Cybersecurity Guidebook For Schools in Hong Kong

Part I :

Ready-to-Use Cybersecurity Policy Templates

Acceptable Use Policy Template

[Your School Name]

Version X.X

Prepared by:	[Name], [Title], [School Name]
Approval /Effective Date:	DD/MM/YYYY

This document is provided as a template for reference only. Schools must review, adapt, and approve the content to reflect their own environment, resources, and needs before implementation. The issuer does not accept liability for any actions taken based on this template.

Version History			
Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

Purpose

The purpose of this Acceptable Use Policy (AUP) is to establish clear guidelines for the responsible, ethical, and secure use of information technology (IT) resources at [School Name]. This policy is designed to protect students, staff, and the school community, ensure compliance with relevant laws and regulations, and support the safe and effective use of digital tools for learning and school administration.

Scope

This policy applies to all users of the school's IT resources, including but not limited to:

- Teaching and non-teaching staff
- Students
- Parents and guardians (where applicable)
- Visitors, contractors, and third parties with access to the school's systems or data
- IT resources include all school-owned computers, mobile devices, network infrastructure, software, cloud services, and any personally owned devices used to access school systems (BYOD).

Definitions

- **IT Systems**: All digital infrastructure, devices, services, and applications managed or used by the school, including networks, servers, computers, and cloud resources.
- **Users:** All individuals with access to the school's IT systems, including staff, students, and authorized third parties.
- **BYOD:** "Bring Your Own Device"; use of personal devices to access school systems.
- **Data Breach**: Unauthorized access, disclosure, or loss of personal or confidential data.
- **Personal Data:** Information relating to an identifiable individual, including students and staff.
- **Cybersecurity Incident:** Any attempted or actual unauthorized access, use, disclosure, disruption, modification, or destruction of information or IT systems.

2. General Policy Principles

Template Note: Summarize prohibited behaviors. Add or remove examples as appropriate for your environment.

Acceptable Use Overview

All users of [School Name]'s IT resources must use these resources responsibly, ethically, and in support of the school's educational and administrative objectives. Acceptable use includes:

- Accessing and using school IT resources for teaching, learning, research, administration, and approved extracurricular activities.
- Respecting the rights, privacy, and property of others, both online and offline.
- Complying with all applicable laws, school policies, and licensing agreements.

Unacceptable Use Overview

Unacceptable use of IT resources includes, but is not limited to:

- Accessing, creating, or sharing illegal, inappropriate, or offensive content.
- Unauthorized access to, or tampering with, the accounts, files, or data of others.
- Engaging in cyberbullying, harassment, or any form of online abuse.
- Downloading or installing unapproved software or applications.
- Using IT resources for personal commercial gain or unauthorized fundraising.
- Any activity that compromises the security, integrity, or availability of school IT systems.

Security and Privacy Principles

[Template Note: Summarize your expectations for protecting IT systems and personal data. Adapt the list to reflect your school's requirements.]

All users are expected to:

- Protect their usernames, passwords, and access credentials; never share them with others.
- Log out or lock devices when not in use.
- Report suspected security incidents, breaches, or suspicious activities to [Insert Responsible Role or Contact].
- Respect the confidentiality and privacy of personal and sensitive information.
- Only collect, access, or share personal data when authorized and necessary for school purposes.

Monitoring and Enforcement

Template Note: Specify your monitoring practices and enforcement mechanisms. Adapt to your school's context and legal requirements.

[School Name] reserves the right to monitor the use of its IT resources to ensure compliance with this policy, support operational needs, and protect users and data. Monitoring may include:

- Reviewing network traffic, email, and internet usage logs.
- Inspecting school-owned devices and storage for policy compliance.

Breaches of this policy may result in disciplinary action, up to and including suspension of IT access, disciplinary procedures, or legal action as appropriate.

3. Roles and Responsibilities

School Management / IT Coordinator

[Template Note: Specify the roles responsible for policy oversight, IT system management, and compliance.]

- Developing, maintaining, and updating the Acceptable Use Policy.
- Communicating policy requirements to all users.
- Providing appropriate IT training and resources.
- Ensuring IT systems and data are protected through technical and procedural controls.
- Monitoring compliance and investigating potential breaches.
- Reporting significant incidents to relevant authorities and stakeholders.
- Reviewing and responding to feedback or incidents relating to IT use.

Teaching and Non-Teaching Staff

[Template Note: Adapt for different staff roles as appropriate.]

All teaching and non-teaching staff are responsible for:

- Using school IT resources in accordance with this policy and modeling responsible digital behavior.
- Supervising student use of IT resources and reporting misuse or concerns to the IT Coordinator or School Management.
- Protecting sensitive information (e.g., student data) and following data protection procedures.
- Completing required IT and cybersecurity training.
- Reporting IT security incidents, suspected breaches, or policy violations promptly.

Students

[Template Note: Customize according to the age group and digital maturity of students.]

All students are responsible for:

- Using IT resources for approved educational purposes.
- Following instructions from teachers and staff regarding IT use.
- Respecting the rights, privacy, and property of others online.
- Keeping personal login credentials confidential.
- Reporting suspicious activity, bullying, or misuse of IT resources.

Note: Younger students may require additional supervision and guidance.

Parents and Guardians

[Template Note: Adjust to reflect parental involvement in your school's context.]

Parents and guardians are responsible for:

- Supporting the school's efforts to promote responsible and safe use of IT resources.
- Reviewing and discussing the Acceptable Use Policy with their children.
- Ensuring consent forms (where required) are reviewed and signed.
- Reporting concerns about student IT use to school staff.

Visitors, Contractors, and Third Parties

[Template Note: Specify requirements for non-regular users of school IT systems.]

Visitors, contractors, and third parties with access to school IT resources are responsible for:

- Using IT resources in accordance with this policy and only for authorized purposes.
- Complying with all relevant confidentiality and security requirements.
- Reporting any security incidents or policy violations to the IT Coordinator or School Management.
- Returning or disabling access credentials upon completion of their engagement.

4. Acceptable and Unacceptable Use

4.1. Staff

[Template Note: Adapt these points to fit your school's expectations for staff.]

Acceptable Use

- Use school IT resources for teaching, administration, professional development, and approved extra-curricular activities.
- Access, create, and share educational materials within school guidelines.
- Communicate with students, parents, and colleagues using approved school platforms.
- Store and handle personal and confidential information in accordance with school policies and privacy laws.
- Use the internet and email for work-related purposes.

Unacceptable Use

- Accessing, creating, or distributing offensive, illegal, or inappropriate content.
- Using IT resources for personal commercial gain, unauthorized fundraising, or political activities.
- Sharing login credentials or allowing unauthorized individuals to access school systems.
- Downloading or installing unapproved software or applications.
- Disclosing confidential or sensitive information without proper authorization.
- Bypassing, disabling, or interfering with security controls or monitoring systems.

Security Responsibilities

[Template Note: Add or remove items to reflect your school's security procedures.]

- Use strong, unique passwords and change them regularly.
    - Do not use your birthday, "123456", "password", or names of family members as your password.
    - Make your password at least 8 characters long, using a mix of letters (upper and lower case), numbers, and symbols.
    - Example: "SchooL2024!" is stronger than "school" or "123456".
    - Do not reuse passwords from other websites or personal accounts.
    - Consider using a passphrase—a short sentence that's easy for you to remember but hard for others to guess, such as "SunnyDays!Read2Learn".
    - Change your password if you think someone else might know it.
    - Never write your password on a sticky note near your computer or share it with anyone.
- Do not share passwords with anyone.
- Lock or log off devices when unattended.

- Promptly report any suspected security breaches, phishing attempts, or suspicious activities to the IT Coordinator.
- Ensure that all data storage and transmission complies with school data protection policies.
- Admit only authorized students into virtual classrooms, and verify student identities when necessary.
- Do not share virtual classroom links or meeting passwords publicly or with unauthorized individuals.
- Use waiting rooms, password protection, and other security features provided by the virtual classroom platform.
- End virtual sessions promptly after class and ensure recordings are stored securely in accordance with school policy.
- Mute participants and disable cameras/microphones for students as needed to prevent disruptions or inappropriate behavior.
- Remind students of online etiquette and privacy expectations during virtual lessons.
- Inform students and parents before recording lessons and obtain consent if required by school policy or local law.
- Store lesson recordings only on approved, secure school platforms—not on personal devices or consumer cloud services.
- Regularly review and delete unnecessary recordings or files containing student information.
- Share assignments, resources, and links only through approved school channels (e.g., secure LMS, school email).
- Never post classroom links, assignments, or student work on public websites or social media.
- Be vigilant for phishing emails or messages pretending to be from students, parents, or school administrators.
- Verify unexpected requests for sensitive information before responding.
- Use official school communication channels for all correspondence with students and parents.
- Monitor student interactions in chat and breakout rooms to prevent bullying, harassment, or sharing of inappropriate material.
- Provide students with clear guidance on how to report any concerns or inappropriate incidents encountered online.
- Do not share your personal contact details or social media with students.
- Avoid discussing or displaying sensitive personal or student information during live sessions or in shared materials.

Use of Personal Devices (BYOD)

[Template Note: Specify your school's BYOD policy. Remove this section if BYOD is not permitted.]

- Staff may use personal devices for work purposes only if they comply with school security requirements.
- Personal devices must have up-to-date antivirus software and use secure passwords.
- Only access school systems via approved applications or secure connections.
- Report any loss or theft of a personal device used for school business immediately.

4.2. Students

Acceptable Use

[Template Note: Adapt language for age group/primary vs. secondary.]

- Use IT resources for learning, research, and school-related activities.
- Follow teacher and staff instructions when using IT devices or platforms.
- Communicate respectfully and responsibly online.
- Access only appropriate websites and content as directed by staff.

Unacceptable Use

- Accessing, creating, or sharing content that is illegal, offensive, or inappropriate.
- Engaging in cyberbullying, harassment, or any form of online abuse.
- Attempting to bypass school security or internet filtering.
- Sharing personal passwords or using someone else's account.
- Damaging or interfering with school devices, software, or network.

Digital Citizenship and Safety

[Template Note: Add guidance relevant to your student body.]

- Students are expected to treat all individuals with respect and courtesy in both online and offline interactions.
- Personal information, including names, addresses, phone numbers, and passwords, must be protected and not disclosed to unknown individuals or posted publicly online.
- Any incidents of cyberbullying, receipt of suspicious messages, or exposure to unsafe or inappropriate online content must be promptly reported to a trusted adult or school staff member.
- Students must respect copyright laws and refrain from plagiarizing, copying, or misusing digital content. All sources must be properly credited.

Security Responsibilities

[Template Note: Add or remove items to reflect your school's security procedures.]

- Students must choose passwords that are not easy to guess (avoid using your name, birthday, or simple words like "password" or "123456").
- Passwords should include a mix of letters, numbers, and symbols whenever possible.
- Never share your password with friends, classmates, or anyone except a trusted adult (such as a parent or teacher, if you need help).
- Do not write your password where others can see it (e.g., on your desk or device).
- Change your password immediately and inform your teacher if you think someone else knows it.
- Use a different password for each school account or platform, if required.

- Never use another person's username or account to log in to school systems or devices.
- Always log out of your accounts and close any school apps or websites when finished, especially on shared or public devices.
- Join virtual classes using your real name and school-provided account, unless otherwise instructed by your teacher.
- Do not share virtual classroom links, meeting passwords, or codes with anyone who is not part of your class.
- Participate in online classes from a safe, appropriate environment and follow all directions from your teacher regarding camera/microphone use.
- Do not record, screenshot, or share virtual classes or classmates without explicit permission from your teacher and the school.
- Only share schoolwork, files, or messages with your teachers or classmates as instructed.
- Do not upload, distribute, or forward inappropriate, offensive, or copyrighted material.
- Always double-check before submitting or posting files to make sure you are sharing the correct information with the right people.
- Do not post or share school-related information, images, or videos on social media without permission.
- Do not create or share content that could embarrass, threaten, or harm others.
- Remember that anything posted online can be permanent and visible to others; think carefully before sharing.
- Never share your address, phone number, student ID, or other personal information online, except as required for school platforms.
- Do not ask classmates for personal information or share other people's information without their consent.
- Respect the privacy of your classmates and teachers at all times, both online and offline.
- Keep your personal devices secure and do not leave them unattended in public places.
- Immediately report to a teacher or IT staff if you see or receive something online that is suspicious, inappropriate, or makes you uncomfortable.
- Tell a trusted adult if you think your account has been hacked or if you suspect someone else is using your account.
- Do not try to hack, disable, or get around any school security settings, filters, or monitoring tools.
- Do not click on suspicious links or download attachments from unknown sources, even if they appear to come from friends.
- Only use school devices, accounts, and networks for learning or other approved activities.
- If you are ever unsure if something is safe or allowed, ask a teacher or IT staff before continuing.

Use of Personal Devices (BYOD)

[Template Note: Specify your school's BYOD policy. Remove this section if BYOD is not permitted.]

- Students may use personal devices at school or for school-related work only with explicit permission from staff.
- All personal devices used on school premises or for school activities must support educational purposes and comply with all applicable school IT and security policies.
- Personal devices must not be used to access, store, or distribute inappropriate content, or to disrupt school activities in any way.
- Any loss, theft, or misuse of a personal device must be reported to school authorities immediately.
- Students are responsible for ensuring the security of their devices, including maintaining up-to-date security settings and not disclosing device passwords to others.

4.3. Parents and Guardians

[Template Note: Adapt these points to reflect your school's approach to home-school partnership and digital citizenship.]

Supporting Responsible Use

- Review and discuss the school's Acceptable Use Policy with your child.
- Encourage your child to follow safe and responsible online practices at home and at school.
- Support the school's efforts to promote digital citizenship, online safety, and respectful online behavior.
- Reinforce the importance of protecting personal information and reporting any concerns about cyberbullying or inappropriate content.

Consent and Supervision

- Complete and return all required consent forms related to your child's use of school IT resources, digital platforms, and online services.
- Supervise your child's use of technology at home, especially for younger students.
- Inform the school of any specific concerns or requirements regarding your child's use of technology.
- Communicate with school staff if you notice any issues or have questions about your child's digital safety or online experiences.

4.4. Visitors and Contractors

Acceptable Use

[Template Note: Specify any restrictions or requirements for external users.]

- Use school IT resources only for authorized business, educational, or support purposes.
- Access only the systems, data, and information required for your role or engagement with the school.
- Follow all school policies and security procedures when using IT resources.
- Maintain confidentiality and protect any personal or sensitive information encountered during your visit or service.

Unacceptable Use

- Attempting to access, modify, or share confidential or sensitive school information without authorization.
- Using school IT resources for personal, commercial, or non-school-related activities.
- Introducing unapproved hardware, software, or data to the school network.
- Engaging in any activity that could compromise the security or integrity of school IT systems.
- Failing to comply with instructions from school staff regarding IT use.

5. Data Protection and Privacy

Handling of Personal and Confidential Data

[Template Note: Customize these points to reflect your school's data handling practices and regulatory requirements (e.g., Hong Kong PDPO).]

- All users must handle personal and confidential data in accordance with school policies and applicable data protection laws.
- Access to personal, sensitive, or confidential information is restricted to authorized individuals and only for legitimate educational or administrative purposes.
- Personal data (such as student records, staff information, or parent contact details) must not be disclosed, shared, or transferred outside the school without proper authorization.
- Electronic and paper records containing confidential data must be stored securely, with appropriate safeguards to prevent unauthorized access, loss, or theft.
- Users must ensure data is only retained for as long as necessary and securely deleted or destroyed when no longer required.
- Any use of external digital platforms or cloud services involving personal data must be approved by school management and comply with privacy and security requirements.

Reporting Security Incidents

[Template Note: Specify your school's incident reporting process and responsible contact(s).]

- All users must promptly report any actual or suspected data breaches, loss of personal/confidential data, or other security incidents to [Insert Responsible Role, e.g., IT Coordinator, Data Protection Officer].
- Examples of incidents include: accidental disclosure of data, loss or theft of devices containing school data, unauthorized access to accounts, or receipt of suspicious emails.
- Reports can be made via [Insert reporting method: email, phone, in-person, or designated online form].
- The school will investigate all reported incidents promptly, take appropriate action to mitigate risks, and notify relevant authorities or affected individuals if required by law.
- Users must cooperate fully during investigations and follow any instructions to help contain or resolve the incident.

6. Policy Exceptions and Violations

Policy Review and Updates

[Template Note: Specify your review schedule and update process.]

- This Acceptable Use Policy will be reviewed at least once every [insert period, e.g., year/academic year] or whenever significant changes in technology, regulations, or school operations occur.
- The review process will be led by [insert responsible role, e.g., IT Coordinator or School Management], with input from staff, students, and other stakeholders as appropriate.
- Updates or amendments to the policy must be approved by [insert approval body, e.g., School Management Committee or Principal].
- All users will be notified of significant policy changes and provided with updated copies as required.

Disciplinary Actions and Enforcement

[Template Note: Customize to reflect your school's disciplinary structure and escalation process.]

- Violations of this Acceptable Use Policy may result in disciplinary action, including but not limited to:
    - Verbal or written warnings
    - Suspension or revocation of IT access privileges
    - Additional training requirements
    - Detention, suspension, or expulsion (for students)
    - Disciplinary proceedings or employment actions (for staff)
    - Termination of service or access (for contractors/visitors)
- In cases involving potential criminal activity or legal violations, the school may refer the matter to law enforcement or regulatory authorities.
- Disciplinary actions will be administered in accordance with [insert relevant school policy, e.g., Student Code of Conduct, Staff Handbook].

Roles and Contacts

[Template Note: Fill in the contact points and responsible persons for your school.]

For questions or to report issues related to this policy, please contact:

- IT Coordinator: [Insert name/email/phone]
- Data Protection Officer: [Insert name/email/phone]
- Principal or School Management Office: [Insert contact details]
- Incident Reporting: [Insert reporting method or link]

All inquiries and reports will be handled confidentially and in accordance with school policy.

7. Acknowledgement

7.1. Student/Parent Acknowledgement Form

Student / Parent Acknowledgement Form

Acceptable Use Policy

School Name: _____

Policy Version/Date: _____

Student Name: _____

Class/Year: _____

Acknowledgement:

We have received, read, and understood the [School Name] Acceptable Use Policy for IT resources.

As a student, I agree to follow the rules and responsibilities outlined in the policy when using school technology and online services.

As a parent/guardian, I agree to support the school in promoting safe and responsible use of technology, to supervise my child's use of digital devices as needed, and to contact the school if I have any questions or concerns about the policy.

Student Signature: _____ Date: _____

Parent/Guardian Name: _____

Parent/Guardian Signature: _____ Date: _____

Contact Number/Email: _____

For Office Use Only:

Received by: _____ **Date:** _____

Contact for Questions

- IT Coordinator: [Insert name/email/phone]
- School Management Office: [Insert contact details]

7.2. Staff Acknowledgement Form

Staff Acknowledgement Form

Acceptable Use Policy

School Name: _____

Policy Version/Date: _____

Staff Name: _____

Position/Department: _____

Email/Contact Number: _____

Acknowledgement:

I acknowledge that I have received, read, and understood the [School Name] Acceptable Use Policy for IT resources. I agree to comply with the requirements, responsibilities, and expectations described in the policy. I understand that breach of the policy may result in disciplinary action, including loss of IT privileges or further action as outlined by school policies.

I understand that it is my responsibility to seek clarification from the IT Coordinator or School Management if I have questions about any aspect of the policy.

Signature: _____ **Date:** _____

For Office Use Only:

Received by: _____ **Date:** _____

Contact for Questions

- IT Coordinator: [Insert name/email/phone]
- School Management Office: [Insert contact details]

7.3. Visitor/Contractor Acknowledgement

Visitor/Contractor Acknowledgement Form

Acceptable Use Policy

School Name: _____

Policy Version/Date: _____

Visitor/Contractor Name: _____

Organization/Company (if applicable): _____

Purpose of Visit/Service: _____

Contact Number/Email: _____

Acknowledgement:

I acknowledge that I have received, read, and understood the [School Name] Acceptable Use Policy for IT resources as it applies to visitors and contractors.

I agree to comply with the policy requirements while accessing or using any school IT resources, systems, or data. I understand that failure to follow the policy may result in revocation of access or termination of my engagement with the school.

I will seek clarification from the school's IT Coordinator or designated contact if I have any questions regarding the policy.

Signature: _____ **Date:** _____

For Office Use Only:

Received by: _____ **Date:** _____

Contact for Questions

- IT Coordinator: [Insert name/email/phone]
- School Management Office: [Insert contact details]

Appendices

A. Glossary of Terms

Term	Definition
Access Control	Processes and technologies used to restrict access to IT systems, data, or locations to authorized users only.
AI (Artificial Intelligence)	Computer systems or software that can perform tasks usually requiring human intelligence, such as learning or problem-solving.
Asset	Any device, software, data, or system owned or managed by the school, including hardware, software, and cloud services.
Backup	A copy of data stored separately to enable recovery in case of loss or corruption.
BYOD (Bring Your Own Device)	The use of personally owned devices (e.g., laptops, smartphones) for school activities or accessing school systems.
Cloud Service	An online service (e.g., storage, application, platform) hosted by a third party and accessed via the Internet.
Confidential Data	Information that must be protected from unauthorized access, such as student records or personal data.
Cybersecurity Incident	Any attempted or actual unauthorized access, use, disclosure, disruption, modification, or destruction of information or IT systems.
Data Encryption	The process of converting data into a coded form to prevent unauthorized access.
Data Loss Prevention (DLP)	Tools or processes designed to prevent the unauthorized sharing or loss of sensitive information.
Data Protection	Measures taken to secure personal, sensitive, or confidential information from unauthorized access, disclosure, alteration, or destruction.
Endpoint	Any device (e.g., computer, tablet, smartphone) that connects to the school network.
Firewall	A security system (hardware or software) that monitors and controls incoming and outgoing network traffic based on predetermined rules.
Incident	Any event that could compromise the confidentiality, integrity, or availability of school information or systems.
IT Coordinator	The person or role responsible for overseeing the school's IT systems, security, and compliance.
Log	A record of events, such as system access or data changes, used for monitoring and accountability.
Mobile Device Management (MDM)	Tools or processes used to monitor, manage, and secure mobile devices used in school operations.
Multi-Factor Authentication (MFA)	A security process that requires users to provide two or more independent credentials to verify their identity.
Network Segmentation	The division of a computer network into sub-networks to improve security and performance.
Patch Management	The process of keeping software up to date by applying fixes (patches) to address vulnerabilities or bugs.
Personal Data	Any information relating to an identified or identifiable individual, such as name, ID number, or contact details.

Term	Definition
Physical Access Control	Measures used to restrict entry to buildings, rooms, or other sensitive areas.
Privilege/Privileged Access	Higher-level system access granted to users who need to perform administrative or sensitive tasks.
Ransomware	Malicious software that locks or encrypts a victim's data and demands payment for its release.
Remote Access	The ability to access school IT systems or data from outside the school's physical premises, typically via VPN or secure connections.
Sensitive Data	Data that, if disclosed, could harm individuals or the school, such as health records or disciplinary reports.
Supplier	Any third-party vendor or service provider that supplies goods or services to the school, especially those with access to data or systems.
User	Any staff, student, or other person authorized to use school IT resources.
Vulnerability	A weakness in a system, software, or process that could be exploited to compromise security.
Wireless Security	Controls and practices implemented to protect wireless (Wi-Fi) networks from unauthorized access or attacks.

End of Document

Category	Checklist Item	Priority	Guidance / Examples	Implementation Status
Governance & Compliance	2.1 Legal and Regulatory Compliance	P1	Comply with Personal Data (Privacy) Ordinance (Cap. 486) and PCPD requirements (collection, use, storage, disclosure of personal data), as required by the Privacy Commissioner for Personal Data (PCPD)	
Governance & Compliance	2.1 Legal and Regulatory Compliance	P2	Adhere to relevant Education Bureau (EDB) circulars/guidelines (e.g., Information Security in Schools – Recommended Practice).	
Governance & Compliance	2.1 Legal and Regulatory Compliance	P2	Comply with other applicable laws and standards (e.g., Copyright Ordinance, Computer Crimes Ordinance, sector codes).	
Governance & Compliance	2.1 Legal and Regulatory Compliance	P2	Monitor changes to laws/guidelines and ensure policies and practices remain compliant.	
Governance & Compliance	2.2 Policy Management and Review	P2	Obtain formal approval of cybersecurity policies/procedures by school management/governing body.	
Governance & Compliance	2.2 Policy Management and Review	P2	Review policies at least annually or upon significant changes (technology, legal, operational).	
Governance & Compliance	2.2 Policy Management and Review	P3	Maintain version control for all policies (approval dates, updates, reviews).	
Governance & Compliance	2.2 Policy Management and Review	P1	Communicate policies to staff/students/third parties; provide training/awareness as needed.	
Governance & Compliance	2.2 Policy Management and Review	P3	Drive continuous improvement using feedback, incidents, and audit findings.	
Governance & Compliance	2.2 Policy Management and Review	P1	Senior leadership is accountable for policy management, compliance, and governance of information security.	
Asset Management	3.1 IT Asset Inventory	P1	Maintain an up-to-date inventory of all IT assets; assign overall responsibility to IT Coordinator/School Secretary.	
Asset Management	3.1 IT Asset Inventory	P2	Establish and maintain a documented secure configuration process for all the IT assets and devices managed by school IT, including hardware, software & network devices.	
Asset Management	3.1 IT Asset Inventory	P2	Ensure inventory includes hardware, software/licenses, and cloud services.	
Asset Management	3.1 IT Asset Inventory	P2	Update inventory when assets are acquired, reassigned, or decommissioned.	
Asset Management	3.1 IT Asset Inventory	P2	Review the asset inventory at least annually, or bi-annually.	
Asset Management	3.1 IT Asset Inventory	P1	Use a defined tracking method/tool [e.g., spreadsheet, asset management system].	
Asset Management	3.1 IT Asset Inventory	P2	Follow procedures for asset return and secure disposla (e.g., secure wipe before disposal).	
Asset Management	3.1 IT Asset Inventory	P1	Maintain a regular (weekly, biweekly) process to remove/deny unauthorized assets in the school network.	
Asset Management	3.1 IT Asset Inventory	P1	Review the software asset inventory monthly, ensure they are being supported actively and remove any unauthorized softwares present on any devices.	
Asset Management	3.2 Data Classification and Handling	P1	Establish and Maintain a Data management Process and Data Inventory. These should cover the following • Data owners • Data retention limits and disposal requirements • Data classification & handling; Classify data at minimum as Confidential, Internal, or Public. • Confidential (e.g., student health records, disciplinary reports) • Internal (e.g., staff memos, draft lesson plans) • Public (e.g., school newsletters, event flyers)	
Asset Management	3.2 Data Classification and Handling	P1	Restrict access to confidential/internal data to authorized personnel/roles, such as teachers, administrative staff, IT administrators, etc. This can be done through data access control lists.	
Asset Management	3.2 Data Classification and Handling	P1	Apply appropriate safeguards for sensitive data (e.g., encryption tools, password protection).	
Asset Management	3.2 Data Classification and Handling	P1	Enforce least-privilege access control lists on shares, restricting student/staff data access.	
Asset Management	3.2 Data Classification and Handling	P3	Review data classifications and handling practices at least semi-annually or annually.	
Asset Management	3.2 Data Classification and Handling	P2	Securely delete/destroy data that is no longer required (e.g., digital shredding; shredding printed lists).	
Access Control	4.1 User Account Management	P1	Establish and maintain an inventory of accounts; including the user, administrator and service accounts. This inventory should contain each person's name, username, start/stop dates, department. The accounts present in this inventory should be authorized on a recurring schedule, every quarter at minimum.	
Access Control	4.1 User Account Management	P1	Securely manage school-owned assets and software, configuring software and device setting configuration through secure network protocols. Additionally, disable default accounts and prevent them from being operated.	
Access Control	4.1 User Account Management	P2	Assign responsibility for user account management to IT Coordinators or Administrators.	
Access Control	4.1 User Account Management	P1	Ensure each user has a unique user ID; enforce individual accountability.	
Access Control	4.1 User Account Management	P2	Provision/modify/revoke accounts via a formal process using an access request system, or an IT ticketing system.	
Access Control	4.1 User Account Management	P2	Review active accounts at least annually/biannually; disable/remove stale accounts (e.g., after 90 days of inactivity).	
Access Control	4.1 User Account Management	P1	Remove access promptly when users leave or change roles. Disable dormant accounts after 45 days of inactivity.	
Access Control	4.2 Privileged Access	P1	Create dedicated admin accounts that utilize admin-only credentials and elevated rights, and are not used for regular day-to-day operations.	
Access Control	4.2 Privileged Access	P2	Maintain a simple request/approval procedure before accounts are created or permissions are granted to a specific user.	
Access Control	4.2 Privileged Access	P1	Use privileged accounts only for administrative tasks; not for routine activities.	
Access Control	4.2 Privileged Access	P2	Avoid local admin rights on endpoints; if required, obtain approval from IT Security Lead/equivalent, document, and review regularly.	
Access Control	4.2 Privileged Access	P1	Require MFA registration for all administrative access accounts, either managed on-site or through a service provider.	
Access Control	4.2 Privileged Access	P2	Require privileged access to be requested and approved by IT Security Lead/IT Administrators.	
Access Control	4.2 Privileged Access	P1	Maintain separate credentials for privileged and non-privileged activities.	
Access Control	4.2 Privileged Access	P2	Log and regularly review privileged actions using a central log platform, such as a SIEM or log server.	
Access Control	4.3 Password Policy	P1	Enforce minimum password length [e.g., 8+ characters] and complexity (mix of letters, numbers, symbols).	
Access Control	4.3 Password Policy	P1	Prevent common or weak passwords, prohibit sharing of passwords, and prohibit password reuse across different school systems.	
Access Control	4.3 Password Policy	P3	Require periodic password changes at least every [e.g., 90 days] or based on risk.	
Access Control	4.3 Password Policy	P1	Implement account lockout after [e.g., 5] failed attempts.	
Access Control	4.3 Password Policy	P2	Store passwords securely (hashed and/or encrypted).	
Access Control	4.3 Password Policy	P1	Enable identity methods, e.g., MFA, for sensitive accounts/systems where possible.	

Access Control	4.4 Remote and Third-Party Access	P1	Require secure channels for remote access (e.g., VPN, encrypted connections).	
Access Control	4.4 Remote and Third-Party Access	P1	Require an MFA service to authenticate and assist users' log-on on all forms of remote access.	
Access Control	4.4 Remote and Third-Party Access	P2	Grant remote/third-party access only with explicit approval from IT Administrators and with a defined scope/duration.	
Access Control	4.4 Remote and Third-Party Access	P2	Log and review all third-party access activities.	
Access Control	4.4 Remote and Third-Party Access	P1	Revoke temporary/emergency access promptly upon task completion.	
Network Security	5.1 Network Segmentation	P1	Segment internal networks (e.g., admin, student, guest) using segmentation methods, such as VLANs, separate Wi-Fi SSIDs.	
Network Security	5.1 Network Segmentation	P1	Use private IPs; prevent direct Internet access to internal systems.	
Network Security	5.1 Network Segmentation	P1	Allow only authorized devices on each segment; block unmanaged/personal devices from staff/admin networks.	
Network Security	5.1 Network Segmentation	P3	Review segmentation and access controls at least annually/biannually.	
Network Security	5.2 Firewall and Perimeter Security	P1	Deploy and maintain firewalls at Internet gateway and between critical segments using different firewall types, such as hardware firewall, cloud-based firewall solutions. Additionally, consider implementing firewall solutions on end-user devices.	
Network Security	5.2 Firewall and Perimeter Security	P1	Default deny all traffic; allow only approved services/ports, such as HTTPS, email (SMTP).	
Network Security	5.2 Firewall and Perimeter Security	P2	Review/update firewall rules and monitor logs (via firewall log server, SIEM where available).	
Network Security	5.2 Firewall and Perimeter Security	P2	Remove/disable unused network services/features on all devices.	
Network Security	5.3 Wireless Security	P1	Use strong Wi-Fi encryption (WPA3; or WPA2 if unavailable).	
Network Security	5.3 Wireless Security	P1	Set and regularly update strong Wi-Fi passwords; avoid wide sharing.	
Network Security	5.3 Wireless Security	P2	Ensure network infrastructure is up-to-date across the school network; run the latest stable versions of software and review regularly (biweekly, monthly) to verify software support.	
Network Security	5.3 Wireless Security	P2	Control Wi-Fi access using authentication methods, e.g., MAC filtering, user auth portal.	
Network Security	5.3 Wireless Security	P1	Provide a separate guest Wi-Fi network with restricted Internet access only.	
Network Security	5.3 Wireless Security	P3	Monitor for unauthorized/rogue APs/devices at least monthly/quarterly.	
Network Security	5.3 Wireless Security	P2	Enforce mobile device security settings (password/PIN, disable unnecessary features).	
Network Security	5.3 Wireless Security	P2	Remind users not to access sensitive school data on public Wi-Fi.	
Endpoint & Device Security	6.1 School-owned Devices	P2	Secure/manage all school-owned devices per policy.	
Endpoint & Device Security	6.1 School-owned Devices	P1	Use up-to-date security controls (e.g., anti-malware, firewall, security updates). Enable DNS filtering services on all end-user devices.	
Endpoint & Device Security	6.1 School-owned Devices	P2	Ensure only fully supported and up-to-date web browsers and email clients are permitted on school-owned devices, removing or blocking outdated versions.	
Endpoint & Device Security	6.1 School-owned Devices	P1	Configure automatic updates for anti-malware signature files on school devices.	
Endpoint & Device Security	6.1 School-owned Devices	P1	Allow only authorized users; prohibit account/password sharing.	
Endpoint & Device Security	6.1 School-owned Devices	P1	Configure auto-lock after inactivity [e.g., 10–15 minutes].	
Endpoint & Device Security	6.1 School-owned Devices	P2	Disable autorun and autoplay for removable media devices.	
Endpoint & Device Security	6.1 School-owned Devices	P1	Apply security updates regularly [e.g., automatically or at least monthly].	
Endpoint & Device Security	6.1 School-owned Devices	P1	Report lost, stolen, or compromised devices immediately to IT Coordinator/Administrator.	
Endpoint & Device Security	6.2 BYOD	P2	Require personal devices used for school to meet security requirements.	
Endpoint & Device Security	6.2 BYOD	P2	Permit access to sensitive data/systems from personal devices only if security controls are in place, such as device passcode, up-to-date OS and security software, enrollments in mobile device management, etc.	
Endpoint & Device Security	6.2 BYOD	P3	Reserve the right to restrict/revoke access for non-compliant devices.	
Endpoint & Device Security	6.2 BYOD	P1	Require users to secure their devices and report incidents promptly to IT Administrators.	
Endpoint & Device Security	6.2 BYOD	P1	Prohibit storing/processing confidential data on personal devices unless authorized.	
Endpoint & Device Security	6.3 Mobile Device Management	P3	Implement reasonable measures to manage/secure mobile devices accessing school data.	
Endpoint & Device Security	6.3 Mobile Device Management	P3	Use an MDM solution [e.g., Intune, Apple School Manager] to enforce controls where possible.	
Endpoint & Device Security	6.3 Mobile Device Management	P2	If no MDM, establish alternative procedures (strong passwords, encryption, remote wipe ability).	
Endpoint & Device Security	6.3 Mobile Device Management	P3	Restrict or revoke access for non-compliant devices.	
Endpoint & Device Security	6.3 Mobile Device Management	P3	Review device security controls and compliance at least annually or bi-annually.	
Data Protection	7.1 Data Encryption	P1	Protect data at rest and in transit using appropriate encryption (e.g., full disk, encrypted shares, SSL/TLS) where feasible.	
Data Protection	7.1 Data Encryption	P3	If encryption not feasible, implement alternative risk-reducing measures.	
Data Protection	7.1 Data Encryption	P2	Do not store sensitive data on non-encryptable devices unless exception is approved with mitigations.	
Data Protection	7.1 Data Encryption	P2	Securely manage encryption keys; limit access to authorized personnel.	
Data Protection	7.2 Data Backup and Recovery	P1	Back up critical data regularly at least daily/weekly, using backup method (automated backup software, cloud backup service) where possible.	
Data Protection	7.2 Data Backup and Recovery	P1	Ensure there is at least one offline/isolated backup copy, this may be updated every month or at a time interval as deemed necessary by the school.	
Data Protection	7.2 Data Backup and Recovery	P2	If no automated/cloud backup, use manual procedures; keep backup media secure.	
Data Protection	7.2 Data Backup and Recovery	P1	Protect backup copies (e.g., encryption, offsite/cloud storage, restricted access).	
Data Protection	7.2 Data Backup and Recovery	P2	Conduct periodic backup restoration tests annually/biannually.	
Data Protection	7.2 Data Backup and Recovery	P2	Review and update backup/recovery procedures as necessary.	
Data Protection	7.3 Data Loss Prevention (DLP)	P3	Implement measures to reduce risk of accidental/unauthorized data loss/disclosure.	
Data Protection	7.3 Data Loss Prevention (DLP)	P3	Use technical DLP controls (e.g., DLP software, email filtering, access restrictions) where possible.	
Data Protection	7.3 Data Loss Prevention (DLP)	P2	If no technical DLP, rely on awareness/training and clear handling/sharing policies.	
Data Protection	7.3 Data Loss Prevention (DLP)	P1	Prohibit sending sensitive info via insecure channels (e.g., personal email, unencrypted USBs).	
Data Protection	7.3 Data Loss Prevention (DLP)	P1	Report any actual/suspected data loss immediately to IT Administrators.	

Supplier & Third-Party Management	8.1 Supplier Security Requirements	P1	Establish and maintain an inventory of third-party service providers, including their classifications (service provided, priority, etc.). Review and update the inventory annually, and/or when significant change occurs.	
Supplier & Third-Party Management	8.1 Supplier Security Requirements	P2	Ensure suppliers comply with school information security and data protection requirements.	
Supplier & Third-Party Management	8.1 Supplier Security Requirements	P2	Tailor supplier security requirements to sensitivity of data/systems/services.	
Supplier & Third-Party Management	8.1 Supplier Security Requirements	P3	Where feasible, require suppliers to demonstrate security controls (e.g., ISO 27001, access controls, secure handling).	
Supplier & Third-Party Management	8.1 Supplier Security Requirements	P3	If suppliers can't meet standards, assess risk and apply compensating controls.	
Supplier & Third-Party Management	8.1 Supplier Security Requirements	P2	Assign responsibility for managing supplier security to a specified role, such as Data Protection Officer, IT Coordinator or School Business Manager.	
Supplier & Third-Party Management	8.2 Due Diligence and Contracts	P1	Assess supplier security capability before engagement/renewal (e.g., questionnaire, references, certifications).	
Supplier & Third-Party Management	8.2 Due Diligence and Contracts	P2	Include data protection/security clauses in contracts where possible (confidentiality, breach notification, audit, data return/deletion).	
Supplier & Third-Party Management	8.2 Due Diligence and Contracts	P2	If detailed clauses not feasible, document risk and establish alternative safeguards.	
Supplier & Third-Party Management	8.2 Due Diligence and Contracts	P2	Require suppliers to promptly report actual/suspected security incidents to a specified role, such as Data Protection Officer, IT Coordinator.	
Cloud Services Security	9.1 Approved Cloud Services List	P2	Use only cloud services approved by IT Coordinators and support staff.	
Cloud Services Security	9.1 Approved Cloud Services List	P2	Maintain an up-to-date list of approved cloud services. [Google Workspace for Education, Microsoft 365, approved learning platforms]	
Cloud Services Security	9.1 Approved Cloud Services List	P1	Prohibit storing/sharing school data on unapproved cloud services.	
Cloud Services Security	9.1 Approved Cloud Services List	P3	Review/update the approved services list at least annually/biannually.	
Cloud Services Security	9.2 Cloud Data Protection	P1	Protect sensitive/confidential cloud data (encryption at rest/in transit, strong access controls, classification).	
Cloud Services Security	9.2 Cloud Data Protection	P1	Enable MFA for cloud service access where available.	
Cloud Services Security	9.2 Cloud Data Protection	P3	If a service lacks sufficient protection, avoid storing sensitive data or apply alternative safeguards (limit access, anonymize, password-protected files).	
Cloud Services Security	9.2 Cloud Data Protection	P2	Assign responsibility for cloud data security to IT Coordinator/equivalent roles.	
Cloud Services Security	9.3 Cloud Access and Monitoring	P1	Restrict cloud access to authorized users/roles and review regularly annually/biannually.	
Cloud Services Security	9.3 Cloud Access and Monitoring	P2	Monitor cloud usage for unauthorized activity where possible (e.g., suspicious logins, data downloads, external sharing).	
Cloud Services Security	9.3 Cloud Access and Monitoring	P3	If technical monitoring unavailable, implement alternative measures (awareness, manual reviews, clear reporting).	
Cloud Services Security	9.3 Cloud Access and Monitoring	P1	Report suspected/actual cloud security incidents immediately to IT Coordinator.	
Use of Generative AI	10.1 Approved AI Tools	P2	Use only generative AI tools approved by IT Coordinator, updated with relevant security patches as needed.	
Use of Generative AI	10.1 Approved AI Tools	P2	Maintain a list of approved AI tools., such as Microsoft Copilot, Google Gemini, OpenAI ChatGPT, other approved platforms.	
Use of Generative AI	10.1 Approved AI Tools	P1	Do not use unapproved AI tools for processing/storing/generating school data or to provide school network access.	
Use of Generative AI	10.1 Approved AI Tools	P3	Review/update the approved AI tools list at least annually/biannually.	
Use of Generative AI	10.2 Data Protection in AI Use	P1	Do not enter sensitive/personal data into AI tools unless tool is approved and provider has adequate data protection.	
Use of Generative AI	10.2 Data Protection in AI Use	P2	Ensure users protect data privacy when using AI tools.	
Use of Generative AI	10.3 Monitoring and Control	P3	Monitor use of generative AI tools for policy compliance and inappropriate/unauthorized use.	
Use of Generative AI	10.3 Monitoring and Control	P3	Implement technical controls (usage logs, access restrictions, content filtering) to monitor/control AI use where possible.	
Use of Generative AI	10.3 Monitoring and Control	P3	If technical monitoring unavailable, use alternative measures (awareness, manual checks, clear reporting).	
Use of Generative AI	10.3 Monitoring and Control	P1	Report suspected misuse of AI tools or AI-related data breaches immediately to IT Coordinator.	
User Awareness & Training	11.1 Security Awareness Programs	P1	Provide regular information security awareness for all users in resource-appropriate formats.	
User Awareness & Training	11.1 Security Awareness Programs	P2	Train staff and students on how to recognize and report if their device is missing security updates or if automated patching tools appear to be failing.	
User Awareness & Training	11.1 Security Awareness Programs	P1	Cover key topics (data protection, passwords, phishing, dangers of insecure public networks, and incident reporting).	
User Awareness & Training	11.1 Security Awareness Programs	P2	Use alternative approaches if formal/automated training not feasible (posters, meetings, newsletters).	
User Awareness & Training	11.1 Security Awareness Programs	P3	Review/update awareness materials/sessions at least annually/biannually.	
User Awareness & Training	11.1 Security Awareness Programs	P1	Assign responsibility for coordinating awareness to IT Coordinator.	
User Awareness & Training	11.2 Acceptable Use Policy	P1	Require all users to comply with the Acceptable Use Policy (AUP).	
User Awareness & Training	11.2 Acceptable Use Policy	P1	Communicate AUP at enrollment/induction and via regular reminders; obtain acknowledgement where feasible.	
User Awareness & Training	11.2 Acceptable Use Policy	P2	Use alternative communication for very young students (e.g., classroom discussions, teacher reminders).	
User Awareness & Training	11.2 Acceptable Use Policy	P1	Address AUP breaches via school disciplinary procedures.	
User Awareness & Training	11.3 External Training Channels	P3	Leverage external resources where feasible: Digital Policy Office (DPO) initiatives.	
User Awareness & Training	11.3 External Training Channels	P3	Leverage external resources where feasible: Hong Kong Education Bureau (EDB) guidance/training.	
User Awareness & Training	11.3 External Training Channels	P3	Leverage external resources where feasible: HKCERT alerts/resources/workshops.	
User Awareness & Training	11.3 External Training Channels	P3	Leverage external resources where feasible: HKIRC resources (Cybersec Training Hub, Healthy Web, phishing drills).	
Incident Management	12.1 Incident Reporting	P1	Require prompt reporting of actual/suspected incidents to IT Coordinator using various report methods including email, phone, incident report forms.	
Incident Management	12.1 Incident Reporting	P1	Provide clear guidance on recognizing and reporting incidents, through the use of posters, staff meetings, online resources.	
Incident Management	12.1 Incident Reporting	P1	If no formal system, allow reporting to teacher/supervisor for escalation.	
Incident Management	12.2 Incident Response and Recovery	P1	Respond promptly to incidents to contain, investigate, and remediate.	
Incident Management	12.2 Incident Response and Recovery	P2	Use documented procedures/checklists for response/recovery where possible (e.g., isolate devices, reset passwords, restore backups).	
Incident Management	12.2 Incident Response and Recovery	P2	If no formal procedures/tools, take reasonable steps to contain/protect/recover quickly.	
Incident Management	12.2 Incident Response and Recovery	P2	Coordinate communications with affected parties/parents/authorities via IT Coordinator.	
Incident Management	12.2 Incident Response and Recovery	P2	Maintain process/contact info to report to HKCERT as appropriate.	
Incident Management	12.2 Incident Response and Recovery	P1	Maintain process/contact info to report to Hong Kong Police for suspected crimes/solely affected cases.	
Incident Management	12.2 Incident Response and Recovery	P1	Maintain process/contact info to notify PCPD for personal data breaches where harm/distress may result.	
Incident Management	12.2 Incident Response and Recovery	P2	Seek qualified external expertise if internal resources are insufficient to manage/recover from incidents.	

Incident Management	12.3 Post-Incident Review	P3	Conduct post-incident reviews after significant incidents to determine causes and improvements.	
Incident Management	12.3 Post-Incident Review	P3	Document and share findings/lessons learned with relevant staff where possible.	
Incident Management	12.3 Post-Incident Review	P3	Discuss incidents in staff meetings at minimum and implement basic corrective actions.	
Incident Management	12.3 Post-Incident Review	P3	Update policies/procedures based on review outcomes.	
Monitoring & Logging	13.1 System and Network Monitoring	P2	Monitor key systems/network activity for unauthorized access/misuse/incidents using different monitoring methods, built-in alerts, security softwares and firewall logs, where feasible.	
Monitoring & Logging	13.1 System and Network Monitoring	P2	Focus monitoring on critical assets and sensitive data (e.g., admin servers, SIS, cloud platforms).	
Monitoring & Logging	13.1 System and Network Monitoring	P3	If no automated tools, perform regular manual checks/reviews of usage reports and user activity.	
Monitoring & Logging	13.1 System and Network Monitoring	P2	Assign monitoring responsibility to IT Coordinator or System Administrators.	
Monitoring & Logging	13.2 Log Management and Review	P1	Maintain logs of key activities (logins, file access, changes to sensitive data) using logging tools, such as server logs, firewall logs and cloud audit trails, where possible.	
Monitoring & Logging	13.2 Log Management and Review	P2	Establish and maintain a documented audit log management process defining the logging requirements for the school, with regular review and/or when significant changes occur.	
Monitoring & Logging	13.2 Log Management and Review	P2	Protect logs from unauthorized access, modification, or deletion.	
Monitoring & Logging	13.2 Log Management and Review	P2	Retain logs for a defined retention period, such as quarterly/annually, to support investigations/audits/regulatory needs.	
Monitoring & Logging	13.2 Log Management and Review	P3	Securely delete logs after retention period unless needed for ongoing investigations.	
Monitoring & Logging	13.2 Log Management and Review	P2	Review logs regularly monthly/quarterly to detect suspicious activity/policy violations.	
Monitoring & Logging	13.2 Log Management and Review	P3	If no automated log tools, conduct manual reviews and record security-relevant events.	
Monitoring & Logging	13.2 Log Management and Review	P1	Report significant findings/incidents from log reviews promptly to IT Coordinator.	
Physical & Environmental Security	14.1 Physical Access Control	P1	Restrict access to sensitive areas (server rooms, staff workspaces, records storage) to authorized personnel.	
Physical & Environmental Security	14.1 Physical Access Control	P1	Clearly mark areas as public, staff-only, or restricted; control access accordingly.	
Physical & Environmental Security	14.1 Physical Access Control	P1	Use physical access controls (locks, access cards, sign-in/out logs) where possible.	
Physical & Environmental Security	14.1 Physical Access Control	P2	If advanced controls not available, use alternatives (manual supervision, locked cabinets, staff presence).	
Physical & Environmental Security	14.1 Physical Access Control	P2	Supervise and record visitor access to sensitive areas (e.g., visitor log).	
Physical & Environmental Security	14.1 Physical Access Control	P1	Assign responsibility for physical access to IT Coordinator/Administrators.	
Physical & Environmental Security	14.2 Equipment Security	P1	Protect equipment with sensitive information against theft/loss/damage.	
Physical & Environmental Security	14.2 Equipment Security	P1	Securely locate equipment (locked rooms, out of public areas) and physically secure where feasible (cable locks, locked cabinets).	
Physical & Environmental Security	14.2 Equipment Security	P2	Use practical alternatives if advanced measures unavailable (regular checks, locked storage after hours).	
Physical & Environmental Security	14.2 Equipment Security	P1	Report lost/stolen/damaged equipment promptly to IT Administrators.	
Physical & Environmental Security	14.2 Equipment Security	P2	Ensure secure data removal before disposal/transfer of equipment.	
Maintenance & Patch Management	15.1 Software Updates	P1	Keep all systems/software up to date with latest security updates/patches.	
Maintenance & Patch Management	15.1 Software Updates	P1	Enable automatic updates for OS, applications, and security tools where possible.	
Maintenance & Patch Management	15.1 Software Updates	P2	If no auto-updates, implement manual process (scheduled checks, update logs).	
Maintenance & Patch Management	15.1 Software Updates	P1	Apply critical security updates as soon as possible after release.	
Maintenance & Patch Management	15.1 Software Updates	P2	Avoid using end-of-life systems/software unless risk assessed and compensating controls applied.	
Maintenance & Patch Management	15.1 Software Updates	P2	Include third-party cloud/SaaS platforms in update/vulnerability management (verify provider practices or via contract).	
Maintenance & Patch Management	15.1 Software Updates	P2	Assign responsibility for software updates to IT Administrators.	
Maintenance & Patch Management	15.2 Vulnerability Management	P1	Regularly review systems/software for known vulnerabilities (scanning tools, manual checks, vendor notifications).	
Maintenance & Patch Management	15.2 Vulnerability Management	P3	Use vulnerability management tools to identify/prioritize risks where available.	
Maintenance & Patch Management	15.2 Vulnerability Management	P2	If no automated tools, monitor trusted sources (vendor sites, government advisories) and act as needed.	
Maintenance & Patch Management	15.2 Vulnerability Management	P2	Assess/address identified vulnerabilities in a timely manner, prioritizing highest risks.	
Maintenance & Patch Management	15.2 Vulnerability Management	P2	Report significant risks/unresolved issues to IT Coordinators.	
Maintenance & Patch Management	15.2 Vulnerability Management	P3	Assess potential impacts and test major updates where feasible before deployment.	
Maintenance & Patch Management	15.3 Change Management	P3	Review/approve significant IT changes by IT Coordinators before implementation.	
Maintenance & Patch Management	15.3 Change Management	P3	Document significant changes (date, nature, responsible person).	
Maintenance & Patch Management	15.3 Change Management	P3	Test changes where possible to minimize disruption.	
Maintenance & Patch Management	15.3 Change Management	P1	Require staff to report problems arising from changes promptly.	
Policy Exceptions & Violations	16.1 Exception Process	P2	Submit exception requests in writing to IT Coordinators with reasons and compensating controls.	
Policy Exceptions & Violations	16.1 Exception Process	P2	p	
Policy Exceptions & Violations	16.1 Exception Process	P2	Document approved exceptions (scope, duration, conditions).	
Policy Exceptions & Violations	16.1 Exception Process	P3	Review exceptions periodically such as annually, or as needed, to confirm ongoing need.	
Policy Exceptions & Violations	16.2 Disciplinary Actions	P2	Apply disciplinary action for policy violations/unauthorized exceptions per school procedures.	
Policy Exceptions & Violations	16.2 Disciplinary Actions	P2	Consider intent, severity, and impact when determining actions.	
Policy Exceptions & Violations	16.2 Disciplinary Actions	P3	Report potential legal/regulatory breaches to appropriate authorities as required.	
Document Control	17.1 Policy Review and Update History	N/A	Review/update this policy at least annually/biannually or upon significant changes.	
Document Control	17.1 Policy Review and Update History	N/A	Assign responsibility for reviews/updates to IT Coordinator.	
Document Control	17.1 Policy Review and Update History	N/A	Record all policy versions (effective date, summary of changes, responsible person).	
Document Control	17.1 Policy Review and Update History	N/A	Retain previous policy versions for a defined retention period, such as for 3 years.	
Document Control	17.1 Policy Review and Update History	N/A	Make the current approved policy available to staff and, as appropriate, students/parents.	

***Note** : The priority rankings (P1–P4) are general recommendations based on common security practices and limited information about the school's environment. They are not legal, regulatory, or professional advice, and they do not guarantee prevention of incidents or compliance. The school remains responsible for assessing its own risks, legal obligations, resources, and technical context, and for determining the final order, scope, and implementation of controls.*

Implementation Summary	Total Count	Implemented Count	% Implementation
P1 - Do Now Highest priority to implement and encorporate as a baseline level of security, deemed to be vital to uphold a secure environment	84	0	0%
P2 - Next Important protective measures that are beneficial to maintaining security, not very high effort but still closes gaps	83	0	0%
P3 - Later Additional protective measures for enhanced protection, these provide maturity and operational cadence and have a medium strain on resources/time to be implemented	42	0	0%

Cybersecurity Policy Template

[Your School Name]

Version X.X

Prepared by:	[Name], [Title], [School Name]
Approval /Effective Date:	DD/MM/YYYY

This document is provided as a template for reference only. Schools must review, adapt, and approve the content to reflect their own environment, resources, and needs before implementation. The issuer does not accept liability for any actions taken based on this template.

Version History

Version Date	Version Number	Description of Changes	Author

Table of Contents

1. Introduction

1.1. Purpose

[Template Note: Customize this section to reflect your school's IT security goals.]

The purpose of this cybersecurity policy template is to assist schools in developing, formalizing, and maintaining effective IT security policies and practices. Schools should adapt this template to align with their unique context and operational needs.

1.2. Scope

[Template Note: Update the scope according to your school's environment and user groups.]

This policy applies to all IT resources, data, and users at [Insert School Name], including:

- All staff (teaching and non-teaching)
- Students
- Third-party service providers
- Visitors and contractors with access to school-managed IT systems

1.3. Definitions

[Template Note: Adjust/add definitions as relevant to your school.]

- **IT Systems**: All digital infrastructure, devices, services, and applications managed or used by the school, including networks, servers, computers, and cloud resources.
- **Data Protection**: Measures and controls implemented to secure personal, sensitive, or confidential information from unauthorized access, disclosure, alteration, or destruction.
- **Users:** All individuals with access to the school's IT systems, including staff, students, and authorized third parties.
- **Cybersecurity Incident:** Any attempted or actual unauthorized access, use, disclosure, disruption, modification, or destruction of information or IT systems.

1.4. Roles and Responsibilities

[Template Note: Assign responsibility for each bullet as appropriate for your school.]

Each school is responsible for:

- Customizing the Policy: [Insert Responsible Role] will tailor the template to fit the school's environment.
- Approval and Implementation: [Insert Responsible Role/Committee] will approve and ensure implementation of the policy.
- Training: [Insert Responsible Role] will provide necessary training for staff and students.
- Continuous Review: [Insert Responsible Role] will review and update the policy regularly.
- Policy Governance: [Insert Responsible Role] will be accountable for policy compliance.

xNote: Where examples reference specific tools or controls, they are illustrative only and do not constitute endorsements. Each school retains full responsibility for its IT environment and compliance.

2. Governance and Compliance

2.1. Legal and Regulatory Compliance

Schools must comply with all applicable laws, regulations, and guidelines governing information security and data protection in Hong Kong. Key requirements include:

- Personal Data (Privacy) Ordinance (Cap. 486): Schools are required to protect personal data of students, staff, and other stakeholders in accordance with the requirements of the Privacy Commissioner for Personal Data (PCPD). This includes proper collection, use, storage, and disclosure of personal data.
- Education Bureau Circulars and Guidelines: Schools should adhere to relevant EDB circulars, such as the Information Security in Schools – Recommended Practice, and any updates or sector-specific advisories issued.
- Other Applicable Laws and Standards: Schools should be aware of and comply with any other relevant legal or regulatory requirements, such as the Copyright Ordinance, Computer Crimes Ordinance, and sector-specific codes of practice.

The school is responsible for monitoring changes to relevant laws and guidelines, and ensuring all IT policies and practices remain compliant.

2.2. Policy Management and Review

- **Policy Approval:** All cybersecurity policies and procedures must be formally approved by the school's management or governing body prior to implementation.
- **Periodic Review:** Policies should be reviewed at least annually, or whenever there are significant changes in technology, legal requirements, or operational needs.
- **Version Control:** Schools should maintain records of all policy versions, including dates of approval, updates, and reviews.
- **Communication and Awareness:** All staff, students, and relevant third parties should be informed about the policies, with appropriate training and awareness activities conducted as necessary.
- **Continuous Improvement:** Feedback from staff, incident reports, and audit findings should be used to identify areas for improvement. Updates should be implemented proactively to address new risks or compliance requirements.

Note: The school's senior leadership is ultimately accountable for ensuring effective policy management, legal compliance, and ongoing governance of information security.

3. Asset Management

3.1. IT Asset Inventory

The school shall maintain an up-to-date inventory of all information technology assets to support effective security management and compliance.

- The [Information Owner/Role, e.g., IT Coordinator, School Secretary] is responsible for overseeing and maintaining the asset inventory.
- The inventory should include all key school-managed IT assets, such as:
  - **Hardware** (e.g., laptops, desktops, network switches, tablets)
  - **Software and licenses** (e.g., office suites, antivirus subscriptions)
  - **Cloud services** (e.g., SaaS platforms, learning management systems)
- The asset inventory should be updated whenever assets are acquired, reassigned, or decommissioned.
- The inventory shall be reviewed at least [frequency, e.g., annually/biannually].
- The school may use [tool/method, e.g., spreadsheet, asset management system] for inventory tracking.
- Procedures for asset return and secure disposal shall be followed when staff, students, or contractors depart, or when assets are retired (e.g., secure wiping of hard drives before disposal).

3.2. Data Classification and Handling

School data shall be classified and managed based on sensitivity and in accordance with legal and regulatory requirements.

- Data should be categorized, at minimum, as:
  - **Confidential** (e.g., student health records, disciplinary reports)
  - **Internal** (e.g., staff memos, draft lesson plans)
  - **Public** (e.g., school newsletters, event flyers)
- Access to confidential and internal data is restricted to [authorized personnel/roles, e.g., teachers, administrative staff].
- Appropriate safeguards—such as [encryption tools, password protection]—should be applied to protect sensitive data.
- Data classifications and handling practices should be reviewed at least [frequency, e.g., annually].
- Secure deletion or destruction methods (e.g., digital shredding software, shredding printed lists) shall be used for data that is no longer required.

4. Access Control

4.1. User Account Management

- Assign responsibility for user account management to [role, e.g., IT Coordinator/Administrator].
- Each user must have a unique user ID; individual accountability is required for all actions taken under that ID.
- User accounts are provisioned, modified, and revoked through a formal process using [access_request_system, e.g., access request form or IT ticketing system].
- Conduct regular reviews of active accounts at least [frequency, e.g., annually/biannually] to remove or disable accounts that are no longer needed (e.g., after [inactivity_days, e.g., 90 days] of inactivity).
- Remove access promptly when staff, students, or contractors leave the school or change roles.

4.2. Privileged Access

- Privileged accounts (e.g., administrators) must only be used for administrative tasks—never for routine activities.
- Local administrator rights on endpoint devices (e.g., staff or student computers) should be avoided wherever possible. If local admin access is required for specific purposes, it must be approved by [approval_roles, e.g., IT Security Lead, Principal], formally documented, and regularly reviewed.
- Privileged access must be requested and approved by [approval_roles, e.g., IT Security Lead, Principal].
- Maintain a separate set of credentials for privileged and non-privileged activities.
- All privileged actions should be logged and regularly reviewed using [central_log_platform, e.g., SIEM or log server].

4.3. Password Policy

Apply a password policy to all systems, reflecting security best practices:

- Minimum length: [e.g., 8 characters], mix of letters, numbers, and symbols.
- Prevent use of common or weak passwords, and prohibit sharing of passwords.
- Require password changes at least every [e.g., 90 days] or as dictated by risk.
- Implement account lockout after [e.g., 5] failed attempts.
- Store passwords securely (e.g., hashed and/or encrypted).
- Where possible, enable [identity_methods, e.g., multi-factor authentication (MFA)] for sensitive accounts and systems.

4.4. Remote and Third-Party Access

- Remote access to school systems must use secure channels (e.g., VPN, encrypted connections).
- Grant remote or third-party access (e.g., vendors, contractors) only with explicit approval from [approval_roles] and clearly defined scope and duration.
- All third-party access activities must be logged and reviewed.
- Temporary or emergency access must be revoked promptly upon completion of the task.

5. Network Security

The school shall implement controls to protect school networks and data from unauthorized access, disruption, and cyber threats. These controls apply to all network segments, devices, and users on school-managed infrastructure.

5.1. Network Segmentation

- Internal networks must be segmented to separate sensitive areas (such as administration, student, and guest networks) using [segmentation methods, e.g., VLANs, separate Wi-Fi SSIDs].
- Design internal networks with private (non-public) IP addresses; ensure that no internal system is directly accessible from the Internet.
- Only allow authorized devices to connect to each network segment; unmanaged or personal devices must not connect to staff/admin networks.
- Review network segmentation and access controls at least [frequency, e.g., annually, biannually].

5.2. Firewall and Perimeter Security

- Deploy and maintain network firewalls at the school's Internet gateway and between critical network segments using [firewall type, e.g., hardware firewall, cloud-based firewall solution].
- Block all incoming and outgoing network traffic by default, except for [approved services/ports, e.g., HTTPS, email (SMTP)].
- Regularly review and update firewall rules and monitor logs for unauthorized activity using [central_log_platform, e.g., firewall log server, SIEM].
- Remove or disable unused network services and features on all devices.

5.3. Wireless Security

- All school wireless networks must use strong encryption [encryption standard, e.g., WPA3; if unavailable, WPA2].
- Set and regularly update strong Wi-Fi passwords; avoid wide sharing of passwords.
- Control Wi-Fi access using [authentication method, e.g., MAC address filtering, user authentication portal].
- Provide a separate guest Wi-Fi network for visitors with restricted Internet access only.
- Monitor for unauthorized or rogue access points and devices at least [frequency, e.g., monthly, quarterly].
- Enforce security settings for mobile devices (e.g., require password/PIN, disable unnecessary features such as Bluetooth, NFC, location services unless needed).
- Remind users not to access sensitive school data on public Wi-Fi networks.

6. Endpoint and Device Security

The school shall protect all devices that access school data or systems from security threats and unauthorized access.

6.1. School-owned Devices

- All school-owned devices (e.g., computers, tablets, servers) must be secured and managed according to school policy.
- Devices must use up-to-date security controls [e.g., anti-malware, firewalls, security updates] as appropriate.
- Only authorized users may access school-owned devices; sharing accounts or passwords is not permitted.
- Devices must be configured to lock automatically after a period of inactivity [e.g., 10–15 minutes].
- Security updates must be applied regularly [frequency, e.g., automatically or at least monthly].
- Lost, stolen, or compromised devices must be reported immediately to [role, e.g., IT Coordinator/Administrator].

6.2. BYOD (Bring Your Own Device)

- Personal devices (e.g., laptops, tablets, smartphones) used for school purposes must comply with the school's security requirements.
- Access to sensitive school data or systems from personal devices is permitted only if [security controls, e.g., device passcode, up-to-date OS and security software, enrollment in mobile device management] are in place.
- The school reserves the right to restrict or revoke access for non-compliant devices.
- Users are responsible for the security of their own devices and must report any security incidents promptly to [role, e.g., IT Coordinator/Administrator].
- Personal devices must not be used to store or process confidential school data unless specifically authorized.

6.3. Mobile Device Management

- The school shall implement reasonable measures to manage and secure mobile devices that access school systems or data.
- Where possible, the school may use a mobile device management (MDM) solution [e.g., Microsoft Intune, Apple School Manager] to enforce security settings (e.g., screen lock, encryption, remote wipe).
- If a dedicated MDM solution is not available, the school will establish alternative procedures to ensure essential security settings are applied to devices (e.g., requiring strong passwords, enabling device encryption, and ensuring the ability to remotely wipe devices if lost or stolen).
- Devices accessing school systems or data must comply with the school's security requirements and may have access restricted or revoked if non-compliant.
- Security controls and device compliance will be reviewed at least [frequency, e.g., annually, biannually].

7. Data Protection

The school shall protect all personal, confidential, and sensitive data against loss, unauthorized access, or misuse, in line with legal and regulatory requirements.

7.1. Data Encryption

- Data stored on school systems and devices ("data at rest") and data transmitted over networks ("data in transit") should be protected using appropriate encryption methods [e.g., full disk encryption, encrypted file shares, SSL/TLS for email and web traffic] where feasible.
- If encryption is not technically or financially feasible, alternative risk-reducing measures must be implemented [e.g., restrict physical access, limit data storage to secure locations, provide staff training on safe handling].
- Sensitive data may not be stored on devices or media that cannot support encryption unless [exception process, e.g., approved by IT Coordinator/Principal, with mitigation steps in place].
- Encryption keys must be securely managed and access limited to authorized personnel.

7.2. Data Backup and Recovery

- Critical school data must be backed up regularly [frequency, e.g., daily, weekly] using [backup method, e.g., automated backup software, cloud backup service], where possible.
- If automated or cloud backup solutions are not available, manual backup procedures must be established and followed, and backup media kept secure (e.g., locked storage, access control).
- Backup copies must be protected from unauthorized access (e.g., encrypted, stored offsite or in the cloud, with access restricted).
- Periodic tests of backup restoration must be conducted [frequency, e.g., annually, biannually] to ensure data can be recovered in the event of loss or system failure.
- Backup and recovery procedures must be reviewed and updated as necessary.

7.3. Data Loss Prevention (DLP)

- The school shall implement measures to reduce the risk of accidental or unauthorized loss, disclosure, or sharing of sensitive data.
- Where possible, technical controls [e.g., DLP software, email filtering, access restrictions] should be used to detect and prevent unauthorized data transfers.
- If technical DLP solutions are not available, the school will rely on awareness, staff/student training, and clear policies on appropriate data handling and sharing.
- Staff and students must be made aware of their responsibilities for protecting data, including not sending sensitive information via insecure channels (e.g., personal email, unencrypted USBs).
- Any actual or suspected data loss incidents must be reported immediately to [role, e.g., Data Protection Officer, IT Coordinator].

8. Supplier and Third-Party Management

The school shall ensure that suppliers, contractors, and third-party service providers who may have access to school data, systems, or facilities meet appropriate security standards.

8.1. Supplier Security Requirements

- Suppliers and third parties providing goods or services to the school must comply with the school's information security and data protection requirements.
- Security requirements for suppliers should be proportionate to the sensitivity of the data, systems, or services involved [e.g., cloud storage provider vs. cleaning contractor].
- Where feasible, suppliers must demonstrate security controls in place (e.g., ISO 27001 certification, appropriate access controls, secure data handling).
- If suppliers cannot meet formal security standards due to practical or budget constraints, the school must assess risk and apply compensating controls [e.g., limit data shared, restrict access, increase monitoring].
- Responsibility for managing supplier security rests with [role, e.g., Data Protection Officer, IT Coordinator, School Business Manager].

8.2. Due Diligence and Contract Requirements

- Before engaging a new supplier or renewing a contract, the school must assess the supplier's ability to protect school data and systems [e.g., through a security questionnaire, reference checks, public certifications].
- Contracts with suppliers handling sensitive data or systems should, where possible, include specific data protection and information security clauses [e.g., confidentiality, breach notification, right to audit, data return or deletion].
- If it is not feasible to include detailed security clauses (e.g., for minor suppliers), the school must document the risk and establish alternative safeguards [e.g., minimize the data shared, use short-term agreements, or apply technical restrictions].
- Suppliers must promptly report any actual or suspected security incidents involving school data to [role, e.g., Data Protection Officer, IT Coordinator].

9. Cloud Services Security

The school shall ensure that the use of cloud services for storing, processing, or sharing school data meets appropriate security and data protection standards.

9.1. Approved Cloud Services List

- Only cloud services that are approved by [role, e.g., IT Coordinator, Data Protection Officer, Principal] may be used for school data and operations.
- The school will maintain an up-to-date list of approved cloud services [e.g., Google Workspace for Education, Microsoft 365, approved learning platforms].
- Staff and students are not permitted to use unapproved cloud services for storing or sharing school data.
- The approved services list will be reviewed and updated at least [frequency, e.g., annually, biannually].

9.2. Cloud Data Protection

- All sensitive or confidential school data stored in the cloud must be protected using appropriate security measures [e.g., encryption at rest and in transit, strong access controls, data classification].
- Where available, multi-factor authentication (MFA) should be enabled for cloud service access.
- If a cloud service cannot provide sufficient data protection features, the school will assess the risk and either (a) avoid storing sensitive data in that service, or (b) apply alternative safeguards [e.g., limit access to trusted users, anonymize data, use password-protected files].
- Responsibility for managing cloud data security rests with [role, e.g., IT Coordinator, Data Protection Officer].

9.3. Cloud Access and Monitoring

- Access to cloud services must be restricted to authorized users and roles [e.g., staff, students, approved contractors] and be reviewed regularly [frequency, e.g., annually, biannually].
- Where possible, cloud service usage should be monitored for unauthorized activity [e.g., suspicious logins, data downloads, sharing outside the school domain].
- If technical monitoring is not available, the school will implement alternative measures [e.g., user awareness training, regular manual reviews of account activity, clear reporting channels for incidents].
- Any suspected or actual security incidents involving cloud services must be reported immediately to [role, e.g., IT Coordinator, Data Protection Officer].

10. Use of Generative AI

The school shall ensure that the use of generative AI tools (e.g., chatbots, text/image generators, automated marking) supports teaching and learning while protecting privacy, data security, and ethical use.

10.1. Approved AI Tools

- Only generative AI tools approved by [role, e.g., IT Coordinator, Data Protection Officer, Principal, AI Committee] may be used for school-related activities.
- The school will maintain a list of approved AI tools [e.g., Microsoft Copilot, Google Gemini, OpenAI ChatGPT, approved education platforms].
- Staff and students must not use unapproved AI tools for processing, storing, or generating school data.
- The approved AI tools list will be reviewed and updated at least [frequency, e.g., annually, biannually].

10.2. Data Protection in AI Use

- Sensitive or personal school data must not be entered into generative AI tools unless the tool is formally approved for such use and the provider demonstrates adequate data protection [e.g., privacy policy, contract terms, trusted reputation].
- Staff and students are responsible for protecting data privacy when using AI tools.

10.3. Monitoring and Control

- The use of generative AI tools must be monitored for compliance with school policies and for inappropriate or unauthorized use.
- Where possible, technical controls [e.g., usage logs, access restrictions, content filtering] should be implemented to monitor and control AI use.
- If technical monitoring is not available, the school will rely on alternative measures [e.g., user awareness training, regular manual checks, clear procedures for reporting misuse].
- Any actual or suspected misuse of AI tools, or data breaches involving AI, must be reported immediately to [role, e.g., IT Coordinator, Data Protection Officer].

11. User Awareness and Training

The school shall ensure that all staff, students, and relevant stakeholders are aware of their responsibilities for information security and understand how to use school systems and data safely and appropriately.

11.1. Security Awareness Programs

- The school will provide regular information security awareness to all users [e.g., staff, students, contractors] in a format appropriate to available resources [e.g., online training, workshops, printed guides, briefings].
- Awareness programs will cover key topics such as data protection, password security, phishing, safe internet use, and incident reporting.
- Where formal or automated training is not feasible, the school will use alternative approaches [e.g., posters, staff meetings, newsletters, classroom discussions].
- Security awareness materials and sessions will be reviewed and updated at least [frequency, e.g., annually, biannually].
- Responsibility for coordinating security awareness rests with [role, e.g., IT Coordinator, Data Protection Officer, Principal].

11.2. Acceptable Use Policy

- All users must comply with the school's Acceptable Use Policy (AUP), which sets out required and prohibited behaviours for the use of school devices, networks, and data.
- The AUP will be communicated to all users [e.g., at enrollment, new staff induction, regular reminders], and users may be required to acknowledge their understanding and agreement [e.g., via signed form, online acknowledgment].
- Where it is not feasible to obtain formal acknowledgment (e.g., for very young students), the school will ensure that expectations are communicated through alternative means [e.g., classroom discussions, teacher reminders].
- Breaches of the Acceptable Use Policy will be addressed in accordance with school disciplinary procedures.

11.3. External Training Channels

The school should consider using external channels and resources to enhance information security awareness for staff, students, and stakeholders.

- **Government & Public Sector Initiatives**:
  - **Digital Policy Office (DPO):** Offers resources and programs under the "Smart City Blueprint" and Cyber Security Campaigns (e.g., seminars, workshops, awareness campaigns).
  - **Hong Kong Education Bureau (EDB)**: Provides guidelines and training materials on e-learning safety, data privacy, and cyber ethics. Schools can request support or professional development.
- **Non-Governmental Organizations (NGOs) & Associations:**
  - **Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT):** Offers free resources, alerts, training sessions, and tailored workshops.
  - **Hong Kong Internet Registration Corporation (HKIRC):** Offers free resources, such as staff training platform (Cybersec Training Hub), website security check (Healthy Web), phishing drill campaign, etc

12. Incident Management

The school shall ensure that all information security incidents, including data breaches, cyber attacks, and loss or theft of devices, are managed in a timely and effective manner to minimize impact and support recovery.

12.1. Incident Reporting

- All users must promptly report actual or suspected information security incidents to [role, e.g., IT Coordinator, Data Protection Officer, Principal] using [reporting method, e.g., email, phone, incident form].
- The school will provide clear guidance to staff and students on how to recognize and report incidents [e.g., posters, staff meetings, online resources].
- If a formal reporting system is not available, users may report incidents directly to their teacher or supervisor, who will escalate to the appropriate contact.

12.2. Incident Response and Recovery

- The school will respond to security incidents in a timely manner, taking steps to contain, investigate, and remediate the situation.
- Where possible, the school will use documented procedures or checklists to guide response and recovery [e.g., isolating affected devices, resetting passwords, restoring backups].
- If formal procedures or technical tools are not available, the school will use reasonable efforts to contain the incident, protect affected data, and resume normal operations as quickly as possible.
- Communication with affected parties, parents, or authorities will be coordinated by [role, e.g., Principal, IT Coordinator] as appropriate.
    - **Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT):**
        - To report multiple-point cyber attacks or seek advice.
        - Tel: 8105 6060 | hkcert@hkcert.org | Incident report form
    - **Hong Kong Police Force:**
        - To report suspected criminal activity or when the school is the only affected party.
        - Tel: 2860 5012 | e-Report Centre
    - **Privacy Commissioner for Personal Data (PCPD):**
    - If personal data (students, staff, parents) is compromised, especially if harm or distress may result. Use the PCPD data breach notification form or online form.
- If the school's available staff do not have the knowledge, experience, or resources required to effectively manage, investigate, or recover from a security incident, the school should seek help from qualified external experts.

12.3. Post-Incident Review

- After a significant security incident, the school will conduct a post-incident review to identify causes, assess the effectiveness of the response, and recommend improvements.
- Where possible, findings and lessons learned will be documented and shared with relevant staff to reduce the risk of recurrence.
- At minimum, the incident will be discussed in staff meetings and basic corrective actions will be implemented.
- The school will update policies and procedures as necessary based on review outcomes.

13. Monitoring and Logging

The school shall monitor its systems and networks to detect, investigate, and respond to security threats or policy violations, and keep relevant logs to support security and accountability.

13.1. System and Network Monitoring

- The school will monitor key systems and network activity for signs of unauthorized access, misuse, or security incidents using [monitoring methods, e.g., built-in alerts, security software, firewall logs], where feasible.
- Monitoring efforts should focus on critical assets and sensitive data [e.g., administrative servers, student information systems, cloud platforms].
- Where automated monitoring tools are not available, the school will use alternative approaches [e.g., regular manual checks, reviewing system usage reports, spot-checking user activity].
- Responsibility for monitoring rests with [role, e.g., IT Coordinator, System Administrator].

13.2. Log Management and Review

- The school will keep logs of key system and network activities [e.g., logins, file access, changes to sensitive data], using [logging tools, e.g., server logs, firewall logs, cloud audit trails] where possible.
- Logs must be protected against unauthorized access, modification, or deletion.
- Logs should be retained for at least [retention period, e.g., 3 months, 1 year] to support possible investigations, audits, or regulatory requirements.
- After the retention period, logs should be securely deleted unless required for ongoing investigations.
- Logs will be reviewed regularly [frequency, e.g., monthly, quarterly] to detect suspicious activity or policy violations.
- If automated log management tools are not available, the school will conduct manual log reviews and keep basic records of security-relevant events.
- Significant findings or incidents identified during log review must be reported promptly to [role, e.g., IT Coordinator, Data Protection Officer].

14. Physical and Environmental Security

The school shall protect its facilities, equipment, and information from physical threats, unauthorized access, loss, or damage.

14.1. Physical Access Control

- Access to areas containing sensitive information or critical systems (e.g., server rooms, staff workspaces, records storage) must be restricted to authorized personnel only.
- Areas within the school should be clearly marked as public, staff-only, or restricted (e.g., server rooms), and access controlled accordingly.
- Physical access controls [e.g., locks, access cards, sign-in/sign-out logs] should be used where possible to prevent unauthorized entry.
- Where advanced controls are not available, the school will use alternative measures [e.g., manual supervision, locked cabinets, staff presence during access].
- Visitor access to sensitive areas must be supervised and recorded, using [methods, e.g., visitor log, sign-in sheet].
- Responsibility for managing physical access rests with [role, e.g., Office Manager, IT Coordinator, Principal].

14.2. Equipment Security

- School equipment containing sensitive information (e.g., computers, servers, backup devices) must be protected against theft, loss, or damage.
- Equipment should be securely located [e.g., in locked rooms, out of public areas] and physically secured [e.g., cable locks, locked cabinets] where feasible.
- Where advanced security measures are not available, the school will use practical alternatives [e.g., regular equipment checks, storing portable devices in locked drawers after hours].
- Lost, stolen, or damaged equipment must be reported promptly to [role, e.g., Office Manager, IT Coordinator].
- Before disposal or transfer, equipment must be checked to ensure all sensitive data is securely deleted or removed.

15. Maintenance and Patch Management

The school shall ensure that all systems and software are regularly maintained and updated to reduce risks from security vulnerabilities and software defects.

15.1. Software Updates

- All school-owned systems and software must be kept up to date with the latest security updates and patches, where available.
- Where possible, enable automatic updates for operating systems, applications, and security tools [e.g., antivirus, browsers].
- If automated updates are not available, the school will establish a manual process [e.g., scheduled checks, update logs] to ensure timely installation of updates.
- Updates that address critical security vulnerabilities should be applied as soon as possible after release.
- Systems and software that are no longer supported by vendors (end-of-life) must not be used for school activities unless a risk assessment and compensating controls are in place.
- Ensure that third-party cloud services and SaaS platforms (e.g., learning management systems, collaboration tools) are included in the update and vulnerability management process, either by verifying provider update practices or ensuring contractually that updates are promptly applied.
- Responsibility for managing software updates rests with [role, e.g., IT Coordinator, System Administrator].

15.2. Vulnerability Management

- The school will regularly review systems and software for known security vulnerabilities, using [methods, e.g., vulnerability scanning tools, manual checks, vendor notifications].
- Where available, use vulnerability management tools to identify and prioritize risks.
- If automated tools are not available, the school will monitor trusted sources [e.g., vendor websites, government advisories] for relevant security alerts and take action as needed.
- Identified vulnerabilities should be assessed and addressed in a timely manner, with priority given to those posing the greatest risk to school operations or data.
- Significant risks, or issues that cannot be resolved internally, must be reported to and reviewed by [role, e.g., IT Coordinator, Principal].
- Before applying major updates, the school will assess potential impacts and, where feasible, test updates in a controlled environment to minimize disruption.

15.3. Change Management

- Significant changes to school IT systems, software, or network settings (e.g., installing new applications, major updates, changing security settings) should be reviewed and approved by [role, e.g., IT Coordinator, Principal] before being implemented.
- All significant changes should be documented, including the date, nature of the change, and the person responsible.
- Where possible, changes should be tested first to avoid disruption.
- Staff should report any problems arising from changes as soon as possible so they can be addressed quickly.

16. Policy Exceptions and Violations

The school recognizes that, under certain circumstances, it may not be possible to fully comply with all information security policies. In such cases, a formal exception process shall be followed. All staff and users are expected to comply with this policy; violations may result in disciplinary action.

16.1. Exception Process

- Requests for exceptions to this policy must be submitted in writing to [role, e.g., Principal, IT Coordinator, Data Protection Officer], explaining the reason for the exception and any compensating controls in place.
- All exceptions will be reviewed and approved by [role, e.g., Principal, IT Committee, Data Protection Officer] before being granted.
- Approved exceptions must be documented, including the scope, duration, and conditions of the exception.
- Exceptions will be reviewed periodically [frequency, e.g., annually, as needed] to determine if they are still necessary.

16.2. Disciplinary Actions

- Violations of this policy, or unauthorized exceptions, may result in disciplinary action, up to and including [consequences, e.g., reprimand, suspension, dismissal], in accordance with the school's staff and student disciplinary procedures.
- The school will consider the intent, severity, and impact of the violation when determining appropriate actions.
- In cases involving possible legal or regulatory breaches, incidents may be reported to [external authorities, e.g., EDB, police, data protection regulator] as required.

17. Document Control

The school will ensure that all information security policies are properly documented, controlled, and kept up to date. This helps maintain consistency, accountability, and ensures that all users refer to the correct version.

17.1. Policy Review and Update History

- This policy shall be reviewed and, if necessary, updated at least [frequency, e.g., annually, every two years], or in response to significant changes in regulations, technology, or school operations.
- Reviews and updates are the responsibility of [role, e.g., Principal, IT Coordinator, Data Protection Officer].
- All versions of this policy must be recorded, including the effective date, summary of changes, and the person responsible for the update.
- Previous versions should be retained for [retention period, e.g., 3 years] for reference and accountability.
- The current and approved version of this policy will be made available to all staff, and, where appropriate, to students and parents.

Appendix

A. Additional References

The following additional references are available to support the effective implementation of this policy:

Mapping of Recommendations to Priority Levels

The recommendations in the above template are mapped according to a priority level in the following table. The priorities are formed in the manner below:

- P1 – Do Now: Highest priority to implement and incorporate as a baseline level of security, deemed to be vital to uphold a secure environment.
- P2 – Next: Important protective measures that are beneficial to maintaining security, not very high effort but still closes gaps
- P3 – Later: Additional protective measures for enhanced protection, these provide maturity and operational cadence and have a medium strain on resources/time to be implemented
- P4 – Defer/Plan: Measures that can be implemented in the longer term when justified by volume or timing, to be addressed independently by each school's available resources

The table of policy templates is mapped against their relative priorities below:

Category	Template Item	Priority	Guidance/Examples
Governance & Compliance	2.1 Legal and Regulatory Compliance	P1	Comply with Personal Data (Privacy) Ordinance (Cap. 486) and PCPD requirements (collection, use, storage, disclosure of personal data), as required by the Privacy Commissioner for Personal Data (PCPD)
Governance & Compliance	2.1 Legal and Regulatory Compliance	P1	Adhere to relevant Education Bureau (EDB) circulars/guidelines (e.g., Information Security in Schools – Recommended Practice).
Governance & Compliance	2.1 Legal and Regulatory Compliance	P2	Comply with other applicable laws and standards (e.g., Copyright Ordinance, Computer Crimes Ordinance, sector codes).
Governance & Compliance	2.1 Legal and Regulatory Compliance	P1	Monitor changes to laws/guidelines and ensure policies and practices remain compliant.
Governance & Compliance	2.2 Policy Management and Review	P1	Obtain formal approval of cybersecurity

			policies/procedures by school management/governing body.
Governance & Compliance	2.2 Policy Management and Review	P2	Review policies at least annually or upon significant changes (technology, legal, operational).
Governance & Compliance	2.2 Policy Management and Review	P2	Maintain version control for all policies (approval dates, updates, reviews).
Governance & Compliance	2.2 Policy Management and Review	P1	Communicate policies to staff/students/third parties; provide training/awareness as needed.
Governance & Compliance	2.2 Policy Management and Review	P2	Drive continuous improvement using feedback, incidents, and audit findings.
Governance & Compliance	2.2 Policy Management and Review	P1	Senior leadership is accountable for policy management, compliance, and governance of information security.
Asset Management	3.1 IT Asset Inventory	P1	Maintain an up-to-date inventory of all IT assets; assign overall responsibility to IT Coordinator/School Secretary.
Asset Management	3.1 IT Asset Inventory	P2	Ensure inventory includes hardware, software/licenses, and cloud services.
Asset Management	3.1 IT Asset Inventory	P2	Update inventory when assets are acquired, reassigned, or decommissioned.
Asset Management	3.1 IT Asset Inventory	P2	Review the asset inventory at least annually, or bi-annually.
Asset Management	3.1 IT Asset Inventory	P1	Use a defined tracking method/tool [e.g., spreadsheet, asset management system].
Asset Management	3.1 IT Asset Inventory	P2	Follow procedures for asset return and secure disposal (e.g., secure wipe before disposal).
Asset Management	3.2 Data Classification and Handling	P1	Classify data at minimum as Confidential, Internal, or Public. • Confidential (e.g., student health records, disciplinary reports) • Internal (e.g., staff memos, draft lesson plans)

			• Public (e.g., school newsletters, event flyers)
Asset Management	3.2 Data Classification and Handling	P2	Restrict access to confidential/internal data to authorized personnel/roles, such as teachers, administrative staff, IT administrators, etc.
Asset Management	3.2 Data Classification and Handling	P1	Apply appropriate safeguards for sensitive data (e.g., encryption tools, password protection).
Asset Management	3.2 Data Classification and Handling	P3	Review data classifications and handling practices at least semi-annually or annually.
Asset Management	3.2 Data Classification and Handling	P4	Securely delete/destroy data that is no longer required (e.g., digital shredding; shredding printed lists).
Access Control	4.1 User Account Management	P3	Assign responsibility for user account management to IT Coordinators or Administrators.
Access Control	4.1 User Account Management	P2	Ensure each user has a unique user ID; enforce individual accountability.
Access Control	4.1 User Account Management	P3	Provision/modify/revoke accounts via a formal process using an access request system, or an IT ticketing system.
Access Control	4.1 User Account Management	P2	Review active accounts at least annually/biannually; disable/remove stale accounts (e.g., after 90 days of inactivity).
Access Control	4.1 User Account Management	P1	Remove access promptly when users leave or change roles.
Access Control	4.2 Privileged Access	P4	Use privileged accounts only for administrative tasks; not for routine activities.
Access Control	4.2 Privileged Access	P2	Avoid local admin rights on endpoints; if required, obtain approval from IT Security Lead/equivalent, document, and review regularly.
Access Control	4.2 Privileged Access	P2	Require privileged access to be requested and approved by IT Security Lead/IT Administrators.

Access Control	4.2 Privileged Access	P2	Maintain separate credentials for privileged and non-privileged activities.
Access Control	4.2 Privileged Access	P2	Log and regularly review privileged actions using a central log platform, such as a SIEM or log server.
Access Control	4.3 Password Policy	P1	Enforce minimum password length [e.g., 8+ characters] and complexity (mix of letters, numbers, symbols).
Access Control	4.3 Password Policy	P1	Prevent common/weak passwords; prohibit password sharing.
Access Control	4.3 Password Policy	P1	Require periodic password changes at least every [e.g., 90 days] or based on risk.
Access Control	4.3 Password Policy	P1	Implement account lockout after [e.g., 5] failed attempts.
Access Control	4.3 Password Policy	P2	Store passwords securely (hashed and/or encrypted).
Access Control	4.3 Password Policy	P1	Enable identity methods, e.g., MFA, for sensitive accounts/systems where possible.
Access Control	4.4 Remote and Third-Party Access	P1	Require secure channels for remote access (e.g., VPN, encrypted connections).
Access Control	4.4 Remote and Third-Party Access	P2	Grant remote/third-party access only with explicit approval from IT Administrators and with a defined scope/duration.
Access Control	4.4 Remote and Third-Party Access	P2	Log and review all third-party access activities.
Access Control	4.4 Remote and Third-Party Access	P1	Revoke temporary/emergency access promptly upon task completion.
Network Security	5.1 Network Segmentation	P2	Segment internal networks (e.g., admin, student, guest) using segmentation methods, such as VLANs, separate Wi-Fi SSIDs.
Network Security	5.1 Network Segmentation	P1	Use private IPs; prevent direct Internet access to internal systems.

Network Security	5.1 Network Segmentation	P1	Allow only authorized devices on each segment; block unmanaged/personal devices from staff/admin networks.
Network Security	5.1 Network Segmentation	P2	Review segmentation and access controls at least annually/biannually.
Network Security	5.2 Firewall and Perimeter Security	P1	Deploy and maintain firewalls at Internet gateway and between critical segments using different firewall types, such as hardware firewall, cloud-based firewall solutions.
Network Security	5.2 Firewall and Perimeter Security	P1	Default deny all traffic; allow only approved services/ports, such as HTTPS, email (SMTP).
Network Security	5.2 Firewall and Perimeter Security	P3	Review/update firewall rules and monitor logs (via firewall log server, SIEM where available).
Network Security	5.2 Firewall and Perimeter Security	P2	Remove/disable unused network services/features on all devices.
Network Security	5.3 Wireless Security	P1	Use strong Wi-Fi encryption (WPA3; or WPA2 if unavailable).
Network Security	5.3 Wireless Security	P1	Set and regularly update strong Wi-Fi passwords; avoid wide sharing.
Network Security	5.3 Wireless Security	P2	Control Wi-Fi access using authentication methods, e.g., MAC filtering, user auth portal.
Network Security	5.3 Wireless Security	P2	Provide a separate guest Wi-Fi network with restricted Internet access only.
Network Security	5.3 Wireless Security	P3	Monitor for unauthorized/rogue APs/devices at least monthly/quarterly.
Network Security	5.3 Wireless Security	P3	Enforce mobile device security settings (password/PIN, disable unnecessary features).
Network Security	5.3 Wireless Security	P2	Remind users not to access sensitive school data on public Wi-Fi.
Endpoint & Device Security	6.1 School-owned Devices	P3	Secure/manage all school-owned devices per policy.
Endpoint & Device Security	6.1 School-owned Devices	P2	Use up-to-date security controls (e.g., anti-malware, firewall, security updates).

Endpoint & Device Security	6.1 School-owned Devices	P1	Allow only authorized users; prohibit account/password sharing.
Endpoint & Device Security	6.1 School-owned Devices	P1	Configure auto-lock after inactivity [e.g., 10–15 minutes].
Endpoint & Device Security	6.1 School-owned Devices	P1	Apply security updates regularly [e.g., automatically or at least monthly].
Endpoint & Device Security	6.1 School-owned Devices	P1	Report lost, stolen, or compromised devices immediately to IT Coordinator/Administrator.
Endpoint & Device Security	6.2 BYOD	P3	Require personal devices used for school to meet security requirements.
Endpoint & Device Security	6.2 BYOD	P2	Permit access to sensitive data/systems from personal devices only if security controls are in place, such as device passcode, up-to-date OS and security software, enrollments in mobile device management, etc.
Endpoint & Device Security	6.2 BYOD	P3	Reserve the right to restrict/revoke access for non-compliant devices.
Endpoint & Device Security	6.2 BYOD	P1	Require users to secure their devices and report incidents promptly to IT Administrators.
Endpoint & Device Security	6.2 BYOD	P1	Prohibit storing/processing confidential data on personal devices unless authorized.
Endpoint & Device Security	6.3 Mobile Device Management	P4	Implement reasonable measures to manage/secure mobile devices accessing school data.
Endpoint & Device Security	6.3 Mobile Device Management	P4	Use an MDM solution [e.g., Intune, Apple School Manager] to enforce controls where possible.
Endpoint & Device Security	6.3 Mobile Device Management	P2	If no MDM, establish alternative procedures (strong passwords, encryption, remote wipe ability).
Endpoint & Device Security	6.3 Mobile Device Management	P3	Restrict or revoke access for non-compliant devices.

Endpoint & Device Security	6.3 Mobile Device Management	P2	Review device security controls and compliance at least annually or bi-annually.
Data Protection	7.1 Data Encryption	P1	Protect data at rest and in transit using appropriate encryption (e.g., full disk, encrypted shares, SSL/TLS) where feasible.
Data Protection	7.1 Data Encryption	P3	If encryption not feasible, implement alternative risk-reducing measures.
Data Protection	7.1 Data Encryption	P3	Do not store sensitive data on non-encryptable devices unless exception is approved with mitigations.
Data Protection	7.1 Data Encryption	P2	Securely manage encryption keys; limit access to authorized personnel.
Data Protection	7.2 Data Backup and Recovery	P1	Back up critical data regularly at least daily/weekly, using backup method (automated backup software, cloud backup service) where possible.
Data Protection	7.2 Data Backup and Recovery	P3	If no automated/cloud backup, use manual procedures; keep backup media secure.
Data Protection	7.2 Data Backup and Recovery	P2	Protect backup copies (e.g., encryption, offsite/cloud storage, restricted access).
Data Protection	7.2 Data Backup and Recovery	P2	Conduct periodic backup restoration tests annually/biannually.
Data Protection	7.2 Data Backup and Recovery	P1	Review and update backup/recovery procedures as necessary.
Data Protection	7.3 Data Loss Prevention (DLP)	P2	Implement measures to reduce risk of accidental/unauthorized data loss/disclosure.
Data Protection	7.3 Data Loss Prevention (DLP)	P2	Use technical DLP controls (e.g., DLP software, email filtering, access restrictions) where possible.
Data Protection	7.3 Data Loss Prevention (DLP)	P3	If no technical DLP, rely on awareness/training and clear handling/sharing policies.
Data Protection	7.3 Data Loss Prevention (DLP)	P1	Prohibit sending sensitive info via insecure channels (e.g.,

			personal email, unencrypted USBs).
Data Protection	7.3 Data Loss Prevention (DLP)	P1	Report any actual/suspected data loss immediately to IT Administrators.
Supplier & Third-Party Management	8.1 Supplier Security Requirements	P3	Ensure suppliers comply with school information security and data protection requirements.
Supplier & Third-Party Management	8.1 Supplier Security Requirements	P1	Tailor supplier security requirements to sensitivity of data/systems/services.
Supplier & Third-Party Management	8.1 Supplier Security Requirements	P2	Where feasible, require suppliers to demonstrate security controls (e.g., ISO 27001, access controls, secure handling).
Supplier & Third-Party Management	8.1 Supplier Security Requirements	P2	If suppliers can't meet standards, assess risk and apply compensating controls.
Supplier & Third-Party Management	8.1 Supplier Security Requirements	P1	Assign responsibility for managing supplier security to a specified role, such as Data Protection Officer, IT Coordinator or School Business Manager.
Supplier & Third-Party Management	8.2 Due Diligence and Contracts	P1	Assess supplier security capability before engagement/renewal (e.g., questionnaire, references, certifications).
Supplier & Third-Party Management	8.2 Due Diligence and Contracts	P2	Include data protection/security clauses in contracts where possible (confidentiality, breach notification, audit, data return/deletion).
Supplier & Third-Party Management	8.2 Due Diligence and Contracts	P2	If detailed clauses not feasible, document risk and establish alternative safeguards.
Supplier & Third-Party Management	8.2 Due Diligence and Contracts	P1	Require suppliers to promptly report actual/suspected security incidents to a specified role, such as Data Protection Officer, IT Coordinator.
Cloud Services Security	9.1 Approved Cloud Services List	P2	Use only cloud services approved by IT Coordinators and support staff.

Cloud Services Security	9.1 Approved Cloud Services List	P2	Maintain an up-to-date list of approved cloud services. [Google Workspace for Education, Microsoft 365, approved learning platforms]
Cloud Services Security	9.1 Approved Cloud Services List	P1	Prohibit storing/sharing school data on unapproved cloud services.
Cloud Services Security	9.1 Approved Cloud Services List	P2	Review/update the approved services list at least annually/biannually.
Cloud Services Security	9.2 Cloud Data Protection	P1	Protect sensitive/confidential cloud data (encryption at rest/in transit, strong access controls, classification).
Cloud Services Security	9.2 Cloud Data Protection	P1	Enable MFA for cloud service access where available.
Cloud Services Security	9.2 Cloud Data Protection	P3	If a service lacks sufficient protection, avoid storing sensitive data or apply alternative safeguards (limit access, anonymize, password-protected files).
Cloud Services Security	9.2 Cloud Data Protection	P3	Assign responsibility for cloud data security to IT Coordinator/equivalent roles.
Cloud Services Security	9.3 Cloud Access and Monitoring	P1	Restrict cloud access to authorized users/roles and review regularly annually/biannually.
Cloud Services Security	9.3 Cloud Access and Monitoring	P2	Monitor cloud usage for unauthorized activity where possible (e.g., suspicious logins, data downloads, external sharing).
Cloud Services Security	9.3 Cloud Access and Monitoring	P4	If technical monitoring unavailable, implement alternative measures (awareness, manual reviews, clear reporting).
Cloud Services Security	9.3 Cloud Access and Monitoring	P1	Report suspected/actual cloud security incidents immediately to IT Coordinator.
Use of Generative AI	10.1 Approved AI Tools	P1	Use only generative AI tools approved by IT Coordinator.
Use of Generative AI	10.1 Approved AI Tools	P1	Maintain a list of approved AI tools., such as Microsoft

			Copilot, Google Gemini, OpenAI ChatGPT, other approved platforms.
Use of Generative AI	10.1 Approved AI Tools	P1	Do not use unapproved AI tools for processing/storing/generating school data.
Use of Generative AI	10.1 Approved AI Tools	P2	Review/update the approved AI tools list at least annually/biannually.
Use of Generative AI	10.2 Data Protection in AI Use	P1	Do not enter sensitive/personal data into AI tools unless tool is approved and provider has adequate data protection.
Use of Generative AI	10.2 Data Protection in AI Use	P2	Ensure users protect data privacy when using AI tools.
Use of Generative AI	10.3 Monitoring and Control	P3	Monitor use of generative AI tools for policy compliance and inappropriate/unauthorized use.
Use of Generative AI	10.3 Monitoring and Control	P3	Implement technical controls (usage logs, access restrictions, content filtering) to monitor/control AI use where possible.
Use of Generative AI	10.3 Monitoring and Control	P3	If technical monitoring unavailable, use alternative measures (awareness, manual checks, clear reporting).
Use of Generative AI	10.3 Monitoring and Control	P1	Report suspected misuse of AI tools or AI-related data breaches immediately to IT Coordinator.
User Awareness & Training	11.1 Security Awareness Programs	P1	Provide regular information security awareness for all users in resource-appropriate formats.
User Awareness & Training	11.1 Security Awareness Programs	P1	Cover key topics (data protection, passwords, phishing, safe Internet use, incident reporting).
User Awareness & Training	11.1 Security Awareness Programs	P2	Use alternative approaches if formal/automated training not feasible (posters, meetings, newsletters).

User Awareness & Training	11.1 Security Awareness Programs	P2	Review/update awareness materials/sessions at least annually/biannually.
User Awareness & Training	11.1 Security Awareness Programs	P1	Assign responsibility for coordinating awareness to IT Coordinator.
User Awareness & Training	11.2 Acceptable Use Policy	P1	Require all users to comply with the Acceptable Use Policy (AUP).
User Awareness & Training	11.2 Acceptable Use Policy	P1	Communicate AUP at enrollment/induction and via regular reminders; obtain acknowledgement where feasible.
User Awareness & Training	11.2 Acceptable Use Policy	P2	Use alternative communication for very young students (e.g., classroom discussions, teacher reminders).
User Awareness & Training	11.2 Acceptable Use Policy	P1	Address AUP breaches via school disciplinary procedures.
User Awareness & Training	11.3 External Training Channels	P3	Leverage external resources where feasible: Digital Policy Office (DPO) initiatives.
User Awareness & Training	11.3 External Training Channels	P3	Leverage external resources where feasible: Hong Kong Education Bureau (EDB) guidance/training.
User Awareness & Training	11.3 External Training Channels	P3	Leverage external resources where feasible: HKCERT alerts/resources/workshops.
User Awareness & Training	11.3 External Training Channels	P3	Leverage external resources where feasible: HKIRC resources (Cybersec Training Hub, Healthy Web, phishing drills).
Incident Management	12.1 Incident Reporting	P1	Require prompt reporting of actual/suspected incidents to IT Coordinator using various report methods including email, phone, incident report forms.
Incident Management	12.1 Incident Reporting	P1	Provide clear guidance on recognizing and reporting incidents, through the use of posters, staff meetings, online resources.

Incident Management	12.1 Incident Reporting	P1	If no formal system, allow reporting to teacher/supervisor for escalation.
Incident Management	12.2 Incident Response and Recovery	P1	Respond promptly to incidents to contain, investigate, and remediate.
Incident Management	12.2 Incident Response and Recovery	P2	Use documented procedures/checklists for response/recovery where possible (e.g., isolate devices, reset passwords, restore backups).
Incident Management	12.2 Incident Response and Recovery	P1	If no formal procedures/tools, take reasonable steps to contain/protect/recover quickly.
Incident Management	12.2 Incident Response and Recovery	P1	Coordinate communications with affected parties/parents/authorities via IT Coordinator.
Incident Management	12.2 Incident Response and Recovery	P1	Maintain process/contact info to report to HKCERT as appropriate.
Incident Management	12.2 Incident Response and Recovery	P1	Maintain process/contact info to report to Hong Kong Police for suspected crimes/solely affected cases.
Incident Management	12.2 Incident Response and Recovery	P1	Maintain process/contact info to notify PCPD for personal data breaches where harm/distress may result.
Incident Management	12.2 Incident Response and Recovery	P2	Seek qualified external expertise if internal resources are insufficient to manage/recover from incidents.
Incident Management	12.3 Post-Incident Review	P3	Conduct post-incident reviews after significant incidents to determine causes and improvements.
Incident Management	12.3 Post-Incident Review	P3	Document and share findings/lessons learned with relevant staff where possible.
Incident Management	12.3 Post-Incident Review	P3	Discuss incidents in staff meetings at minimum and implement basic corrective actions.

Incident Management	12.3 Post-Incident Review	P3	Update policies/procedures based on review outcomes.
Monitoring & Logging	13.1 System and Network Monitoring	P2	Monitor key systems/network activity for unauthorized access/misuse/incidents using different monitoring methods, built-in alerts, security softwares and firewall logs, where feasible.
Monitoring & Logging	13.1 System and Network Monitoring	P2	Focus monitoring on critical assets and sensitive data (e.g., admin servers, SIS, cloud platforms).
Monitoring & Logging	13.1 System and Network Monitoring	P3	If no automated tools, perform regular manual checks/reviews of usage reports and user activity.
Monitoring & Logging	13.1 System and Network Monitoring	P1	Assign monitoring responsibility to IT Coordinator or System Administrators.
Monitoring & Logging	13.2 Log Management and Review	P1	Maintain logs of key activities (logins, file access, changes to sensitive data) using logging tools, such as server logs, firewall logs and cloud audit trails, where possible.
Monitoring & Logging	13.2 Log Management and Review	P1	Protect logs from unauthorized access, modification, or deletion.
Monitoring & Logging	13.2 Log Management and Review	P2	Retain logs for a defined retention period, such as quarterly/annually, to support investigations/audits/regulatory needs.
Monitoring & Logging	13.2 Log Management and Review	P3	Securely delete logs after retention period unless needed for ongoing investigations.
Monitoring & Logging	13.2 Log Management and Review	P1	Review logs regularly monthly/quarterly to detect suspicious activity/policy violations.
Monitoring & Logging	13.2 Log Management and Review	P2	If no automated log tools, conduct manual reviews and record security-relevant events.
Monitoring & Logging	13.2 Log Management and Review	P1	Report significant findings/incidents from log

			reviews promptly to IT Coordinator.
Physical & Environmental Security	14.1 Physical Access Control	P1	Restrict access to sensitive areas (server rooms, staff workspaces, records storage) to authorized personnel.
Physical & Environmental Security	14.1 Physical Access Control	P1	Clearly mark areas as public, staff-only, or restricted; control access accordingly.
Physical & Environmental Security	14.1 Physical Access Control	P2	Use physical access controls (locks, access cards, sign-in/out logs) where possible.
Physical & Environmental Security	14.1 Physical Access Control	P2	If advanced controls not available, use alternatives (manual supervision, locked cabinets, staff presence).
Physical & Environmental Security	14.1 Physical Access Control	P2	Supervise and record visitor access to sensitive areas (e.g., visitor log).
Physical & Environmental Security	14.1 Physical Access Control	P1	Assign responsibility for physical access to IT Coordinator/Administrators.
Physical & Environmental Security	14.2 Equipment Security	P1	Protect equipment with sensitive information against theft/loss/damage.
Physical & Environmental Security	14.2 Equipment Security	P2	Securely locate equipment (locked rooms, out of public areas) and physically secure where feasible (cable locks, locked cabinets).
Physical & Environmental Security	14.2 Equipment Security	P3	Use practical alternatives if advanced measures unavailable (regular checks, locked storage after hours).
Physical & Environmental Security	14.2 Equipment Security	P1	Report lost/stolen/damaged equipment promptly to IT Administrators.
Physical & Environmental Security	14.2 Equipment Security	P3	Ensure secure data removal before disposal/transfer of equipment.
Maintenance & Patch Management	15.1 Software Updates	P1	Keep all systems/software up to date with latest security updates/patches.
Maintenance & Patch Management	15.1 Software Updates	P1	Enable automatic updates for OS, applications, and security tools where possible.

Maintenance & Patch Management	15.1 Software Updates	P2	If no auto-updates, implement manual process (scheduled checks, update logs).
Maintenance & Patch Management	15.1 Software Updates	P1	Apply critical security updates as soon as possible after release.
Maintenance & Patch Management	15.1 Software Updates	P2	Avoid using end-of-life systems/software unless risk assessed and compensating controls applied.
Maintenance & Patch Management	15.1 Software Updates	P2	Include third-party cloud/SaaS platforms in update/vulnerability management (verify provider practices or via contract).
Maintenance & Patch Management	15.1 Software Updates	P1	Assign responsibility for software updates to IT Administrators.
Maintenance & Patch Management	15.2 Vulnerability Management	P2	Regularly review systems/software for known vulnerabilities (scanning tools, manual checks, vendor notifications).
Maintenance & Patch Management	15.2 Vulnerability Management	P3	Use vulnerability management tools to identify/prioritize risks where available.
Maintenance & Patch Management	15.2 Vulnerability Management	P2	If no automated tools, monitor trusted sources (vendor sites, government advisories) and act as needed.
Maintenance & Patch Management	15.2 Vulnerability Management	P2	Assess/address identified vulnerabilities in a timely manner, prioritizing highest risks.
Maintenance & Patch Management	15.2 Vulnerability Management	P1	Report significant risks/unresolved issues to IT Coordinators.
Maintenance & Patch Management	15.2 Vulnerability Management	P3	Assess potential impacts and test major updates where feasible before deployment.
Maintenance & Patch Management	15.3 Change Management	P3	Review/approve significant IT changes by IT Coordinators before implementation.
Maintenance & Patch Management	15.3 Change Management	P3	Document significant changes (date, nature, responsible person).

Maintenance & Patch Management	15.3 Change Management	P3	Test changes where possible to minimize disruption.
Maintenance & Patch Management	15.3 Change Management	P1	Require staff to report problems arising from changes promptly.
Policy Exceptions & Violations	16.1 Exception Process	P1	Submit exception requests in writing to IT Coordinators with reasons and compensating controls.
Policy Exceptions & Violations	16.1 Exception Process	P1	Review and approve exceptions by the person responsible for initiating the exception approval before granting.
Policy Exceptions & Violations	16.1 Exception Process	P2	Document approved exceptions (scope, duration, conditions).
Policy Exceptions & Violations	16.1 Exception Process	P2	Review exceptions periodically such as annually, or as needed, to confirm ongoing need.
Policy Exceptions & Violations	16.2 Disciplinary Actions	P1	Apply disciplinary action for policy violations/unauthorized exceptions per school procedures.
Policy Exceptions & Violations	16.2 Disciplinary Actions	P2	Consider intent, severity, and impact when determining actions.
Policy Exceptions & Violations	16.2 Disciplinary Actions	P3	Report potential legal/regulatory breaches to appropriate authorities as required.
Document Control	17.1 Policy Review and Update History	N/A	Review/update this policy at least annually/biannually or upon significant changes.
Document Control	17.1 Policy Review and Update History	N/A	Assign responsibility for reviews/updates to IT Coordinator.
Document Control	17.1 Policy Review and Update History	N/A	Record all policy versions (effective date, summary of changes, responsible person).
Document Control	17.1 Policy Review and Update History	N/A	Retain previous policy versions for a defined retention period, such as for 3 years.
Document Control	17.1 Policy Review and Update History	N/A	Make the current approved policy available to staff and, as appropriate, students/parents.

Practical Implementation Guides

The practical guides are titled as follows:

- Asset Management – Practical Guide
- Access Control – Practical Guide
- Password Management – Practical Guide
- Maintenance and Patch Management – Practical Guide
- Data Backup and Recovery – Practical Guide
- Data Handling and Protection – Practical Guide
- E-mail Security – Practical Guide
- Mobile Device Management – Practical Guide
- Network Management and Wireless Security – Practical Guide
- Physical and Environmental Security – Practical Guide
- Monitoring and Logging – Practical Guide
- Supplier and Third-Party Relationships – Practical Guide
- Use of Generative AI – Practical Guide

Cybersecurity Incident Response Workflow

Covers the design of the Cyber Incident Response Team (CIRT), roles and responsibilities, reporting and escalation, detailed incident response procedures, and includes scenario-based playbooks for common school security incidents, such as:

- Ransomware Attacks
- Phishing & Malware Infections
- Lost or Stolen Devices
- Accidental Data Disclosure
- Website Defacement
- Denial-of-Service (DoS) Attacks

Security Configuration Checklist

This guide provides step-by-step checklists and practical instructions to help staff configure and secure school devices, systems, and applications in accordance with policy requirements. It covers essential security settings for servers, computers, mobile devices, network equipment, and commonly used software. The checklist includes recommended baseline configurations, hardening steps, and periodic review points to ensure ongoing protection against security threats.

These documents provide step-by-step instructions, checklists, and scenario playbooks for school-specific situations. Users are encouraged to consult these references for practical guidance in daily operations.

B. Glossary of Terms

Term	Definition
Access Control	Processes and technologies used to restrict access to IT systems, data, or locations to authorized users only.
AI (Artificial Intelligence)	Computer systems or software that can perform tasks usually requiring human intelligence, such as learning or problem-solving.
Asset	Any device, software, data, or system owned or managed by the school, including hardware, software, and cloud services.
Backup	A copy of data stored separately to enable recovery in case of loss or corruption.
BYOD (Bring Your Own Device)	The use of personally owned devices (e.g., laptops, smartphones) for school activities or accessing school systems.
Cloud Service	An online service (e.g., storage, application, platform) hosted by a third party and accessed via the Internet.
Confidential Data	Information that must be protected from unauthorized access, such as student records or personal data.
Cybersecurity Incident	Any attempted or actual unauthorized access, use, disclosure, disruption, modification, or destruction of information or IT systems.
Data Encryption	The process of converting data into a coded form to prevent unauthorized access.
Data Loss Prevention (DLP)	Tools or processes designed to prevent the unauthorized sharing or loss of sensitive information.
Data Protection	Measures taken to secure personal, sensitive, or confidential information from unauthorized access, disclosure, alteration, or destruction.
Endpoint	Any device (e.g., computer, tablet, smartphone) that connects to the school network.
Firewall	A security system (hardware or software) that monitors and controls incoming and outgoing network traffic based on predetermined rules.
Incident	Any event that could compromise the confidentiality, integrity, or availability of school information or systems.
IT Coordinator	The person or role responsible for overseeing the school's IT systems, security, and compliance.
Log	A record of events, such as system access or data changes, used for monitoring and accountability.
Mobile Device Management (MDM)	Tools or processes used to monitor, manage, and secure mobile devices used in school operations.
Multi-Factor Authentication (MFA)	A security process that requires users to provide two or more independent credentials to verify their identity.
Network Segmentation	The division of a computer network into sub-networks to improve security and performance.
Patch Management	The process of keeping software up to date by applying fixes (patches) to address vulnerabilities or bugs.
Personal Data	Any information relating to an identified or identifiable individual, such as name, ID number, or contact details.
Physical Access Control	Measures used to restrict entry to buildings, rooms, or other sensitive areas.

Privilege/Privileged Access	Higher-level system access granted to users who need to perform administrative or sensitive tasks.
Ransomware	Malicious software that locks or encrypts a victim's data and demands payment for its release.
Remote Access	The ability to access school IT systems or data from outside the school's physical premises, typically via VPN or secure connections.
Sensitive Data	Data that, if disclosed, could harm individuals or the school, such as health records or disciplinary reports.
Supplier	Any third-party vendor or service provider that supplies goods or services to the school, especially those with access to data or systems.
User	Any staff, student, or other person authorized to use school IT resources.
Vulnerability	A weakness in a system, software, or process that could be exploited to compromise security.
Wireless Security	Controls and practices implemented to protect wireless (Wi-Fi) networks from unauthorized access or attacks.

End of Document

Part II :

Practical Guidelines

Practical Guide to Asset Management

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for asset management in schools across Hong Kong. Its aim is to help educational institutions establish consistent standards that enable effective asset management procedures that ensure the safety and integrity of school systems and sensitive information.

The scope of this guide includes the creation of asset management lists and management procedures, both for hardware assets and software assets. There is also a suggested list of hardware assets to be maintained in inventory, serving as a baseline to meet schools' needs. It is designed to be adaptable for different school sizes, system types, and available resources.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Identify and track the various kinds of assets required for smooth operations of the school IT infrastructure
    - Inclusive of hardware and software assets, generally acquired through licensing
- Maintain records of assets according to their usage status, providing update schedules and status audits
- Conduct regular reviews of IT assets in a timely manner
- Follow standard procedure to replace assets in case of damage/malfunction

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Creating Asset Management Lists

This section outlines the process of creating Asset Management Lists for schools to help with their Asset Management Procedures. Use these recommendations as a foundation and adjust them to suit your school's workflow.

2.1. Hardware Asset List

- Purpose: Tracking the status of every hardware asset on one master list for quick reference.
- Content: All school-owned computer hardware and its relevant information such as hardware serial number, purpose and its location. For all recommended information types, please check the appendix.

Adaptational Tips:

- Assign IT to compile this list. Since the purpose of the list is for easy future reference, it is recommended to use a database or spreadsheet for easy filtering/querying.
- To ensure the correctness of the Hardware Inventory List, establish policies to discourage self-installation and disposal of hardware assets.
- Not all columns have to be filled up for every asset, just the relevant information (e.g., there is no CPU for a monitor, so the CPU model may be filled "N/A").

Practical Examples:

- Make a database or a spreadsheet for their hardware assets. A recommended list of information to be documented has been listed in the appendix.
- If compiling from scratch. consider assigning a guide for end users (other staff) to report their system information (CPU models, ran and disk size, etc) to reduce work needed.

2.2. Software Asset List

- Purpose: Tracking License Information and Installed Software for each Hardware Asset.
- Content: Details of school-owned computer software including license counts, expiry dates, installed devices (e.g., Asset number) and version number.

Adaptational Tips:

- Assign IT to compile this list. Since the purpose of the list is for easy future reference, we recommend using a database or spreadsheet for easy filtering/querying.
- Apart from software versions, we recommend also listing firmware for devices other than workstations, PCs and servers (e.g., networking devices).
- We recommend referencing the Asset number from the Hardware Inventory List, for the purposes of disambiguation and possible table linkage.
- Consider using technical controls to disallow use of unapproved applications.

2.3. Hardware Asset Status Audit Records

- Purpose: Recording any cases of Hardware Asset Status Audit, especially the failures, with their justification. This can then be used as a justification for replacing/disposal of Hardware Assets.
- Content: Asset number, Audit Date and Time, Justification of Success/Failure.

2.4. Disposal Records

- Purpose: Recording any proposals of Hardware Asset Disposal for approval.
- Content: Asset number, Justification of disposal, Status (Pending Approval/Pending Disposal/Disposed).

2.5. Check-Out/Check-in Records

- Purpose: Ensure accountability for borrowed assets by tracking the borrower.
- Content: Asset Number, Borrower, Date and time of Borrow, Date and time of Return.

3. Establishing Hardware Asset Management Procedures

This section explains how a school could establish a proper Hardware Asset Management Procedure, utilizing the Hardware Management Lists. A proper hardware asset management procedure aims to provide up-to-date information of all Hardware assets so that this information can be obtained when in need.

3.1. Updating Hardware Asset List

The Hardware Asset List should be updated in event of:

- Hardware acquisition/replacement
- Hardware retirement
- Repurpose of hardware, including deployment of testing hardware.
- Hardware audits
- Hardware failure
- Any discrepancy found upon Hardware Asset List Review.

3.2. Hardware Asset List Review

A Hardware Asset List Review Consists of two parts, to be conducted together regularly (e.g., annually).

- **Completeness:** Check if all hardware assets are included in the Hardware Asset List.
- **Correctness:** Check if all records in the Hardware Asset List are valid, and that there are no records of disposed assets.

Adaptational Tips:

- The Completeness section will require searching for hardware across the campus, which may require more effort. Consider a procedure that allows all staff to report such assets to lessen the burden on IT.
- The Correctness review should be relatively straightforward, since the Inventory Lists will be readily available, and that the location of the asset will have been documented.

Practical Examples:

- Use sticky labels to label all hardware (e.g., Asset ID, Purpose) for quick future reference. If there is an asset without such label, it may be one that the asset list is missing.
- Ask staff to report any hardware without labels to IT.
- Use scanners or scripts to generate a compiled report of the installed applications in each system. This can then be cross checked with the software inventory list.

3.3. Asset Classification

Classify all assets based on sensitivity (e.g., data stored, impact to operation if brought down) to determine appropriate protection levels for future reference. Put this classification into the records of the Hardware Asset List.

Appendix C in Hong Kong Government IT Security Guidelines (G3) defines a three-tier classification for information systems based on confidentiality, integrity, and availability (CIA):

- **Tier 1 (Low Impact)**: Public or non-sensitive data (e.g., school website content). Loss or compromise has minimal impact.

- **Tier 2 (Medium Impact)**: Sensitive but not highly confidential data (e.g., staff emails, student attendance records). Compromise may cause moderate disruption or privacy concerns.

- **Tier 3 (High/Critical Impact)**: Highly confidential or critical data (e.g., student personal data, exam results, financial records). Compromise could lead to significant legal, reputational, or operational damage.

3.4. Hardware Asset Status Audit

Asset Status Audits are simple checks of the status of the hardware asset for its ability to continue serving its designated task, and should be done regularly (e.g., annually) on all assets on the Hardware Asset List.

Audits on the status of a particular asset can also be done on an ad-hoc basis, e.g., when there is a user report of system malfunction.

If the asset works as intended:

- Update the last audit date of the asset in the Hardware Asset List.

Otherwise:

- Update the last audit date of the asset in the Hardware Asset List.
- Mark the asset as "Status Audit Failed"
- Undergo replacement and disposal procedures for the asset.
- Document the justification of the failure in Asset Status Audit Records.

Adaptational Tips:

- The status of different assets can be left with the professional judgement of the IT staff.

3.5. Replacement of Malfunctioning Assets

When an asset needs malfunctions, consider the following:

- **Check for warranty:** Cross check the asset number against the Hardware Asset List for any warranty service and the contacts.
- **Check for available replacement assets:** Check the Hardware Asset List for any available hardware fit for replacement.

Modify the Hardware Asset List to reflect any changes on the status on any hardware.

Follow Maintenance and Patch Management – Practical Guide for details on replacement when deploying any hardware changes.

3.6. Disposal of Hardware Asset

In event of disposing a Hardware Asset, follow the following procedures:

- Mark the assets to be disposed in the Hardware Asset List as “To Be Disposed”.
- Add the justification of disposal and the assets to be disposed to the Disposal Records.
- After approval, dispose the assets according to the e-waste disposal policies of the Government, or the general asset disposal policy of the school. If the asset contains operational data, follow the Data Handling and Protection – Practical Guide for secure disposal.
- After disposal of asset, update the asset on the Hardware Asset List to reflect that it has been disposed.

3.7. Borrow and Return Procedures

Preparations

- **Asset Eligibility Check**: Verify the asset's availability and condition using the Check-in/Check-out list. Only assets marked as "available" and in good working order can be borrowed.
- **Borrower Verification**: Confirm the borrower's identity (e.g., student ID, staff badge) and eligibility (e.g., no outstanding overdues or restrictions). For students, require parental consent for high-value items.

Check-Out Process

- **Documentation**: Record the transaction in the Check-in/Check-out and/or the Hardware Asset List, noting:
    - Borrower's name, contact info, and affiliation (student/teacher/staff).
    - Asset details (ID/tag number, description, current condition with photos if applicable).
    - Check-out date/time and agreed return date.
- **Agreement Signing**: Have the borrower sign an agreement acknowledging responsibility for the asset, including potential fees for damage or loss.
- **Handover**: Physically hand over the asset and update the status on Hardware Asset List as "checked out."

Check-In Process

- **Return Submission**: Borrowers return the asset to the designated location during specified hours.
- **Inspection**: Staff inspects the asset for condition, comparing it to the check-out record (e.g., note any damage or missing parts).

- **Documentation Update**: Log the return in the Check-in/Check-out list, including:
    - Return date/time.
    - Post-return condition assessment.
    - Any notes on issues or resolutions.
- **Closure**: Mark the asset as "available" in the relevant lists once verified, and notify the borrower if further action (e.g., repairs) is needed.

Record Keeping and Review

- Maintain the Check-in/Check-out list in a secure, accessible format (e.g., shared spreadsheet, database, or asset management software) with backups.
- Conduct regular reviews of the list to identify patterns (e.g., frequent overdues) and audit for accuracy.

Overdue and Dispute Handling

- **Overdue Protocol**: If an asset is not returned by the due date, send escalating notifications (e.g., daily reminders, then alerts to supervisors/parents). After a grace period (e.g., 3 days), apply holds (e.g., restrict future borrowing) or fees as agreed in any signed agreement.
- **Dispute Resolution**: For disputes (e.g., pre-existing damage), refer to the Check-in/Check-out list records as evidence.

Adaptational Tips:

- The Borrowing Agreement should cover borrower's responsibility for the care, return, and potential repair or replacement costs of the asset. It should also specify loan duration, conditions for extensions, and consequences for late returns or damage to ensure accountability and compliance.

4. Establishing Software Asset Management Procedures

This section explains how a school could establish a proper Software Asset Management Procedure, utilizing the Software Management List. A proper software asset management procedure aims to provide up-to-date information of all software assets so that this information can be obtained when in need.

4.1. Updating the Software Asset Management List

The Software Asset List should be updated in event of:

- Software license acquisition
- Software license update
- Software installation
- Software retirement
- Software/firmware changes
- Hardware changes which would result in changes of running software/firmware (e.g., change of network devices)
- Any discrepancy found upon Software Asset List Review.

4.2. Software Asset List Review

A Software Asset List Review Consists of two parts, to be conducted together regularly (e.g., annually).

- **Completeness:** Check if all Software the school is currently using has been included in the Software Asset List.
- **Correctness:** Check if all records in the Software Inventory List are valid, and that there are no records of phased out software.

Adaptation Tips:

- Consider using Software Scanners to scan for installed software on every School owned Workstation.
- Reference the Hardware Asset List to work out the firmware of the devices other than workstations/PCs/Servers (e.g., networking devices)

Appendices

Hardware Inventory List Content Suggestion

Column Name	Description	Data Type	Notes
Asset_ID	Unique identifier for the hardware asset (e.g., auto-generated or school-specific code like SCH-Comp-001).	String or Integer	Primary key for the database table.
Asset_Type	Category of the hardware (e.g., Desktop Computer, Laptop, Printer, Projector, Tablet, Server, Monitor).	String	Use a dropdown list for consistency in a school setting.
Manufacturer	Brand or maker of the device (e.g., Dell, HP, Apple, Epson).	String	
Model	Specific model name or number (e.g., Inspiron 15, iPad Air).	String	
Serial_Number	Manufacturer's serial number for the device.	String	Essential for warranty claims and unique identification.
CPU_Specifications	Details of the processor (e.g., Intel Core i7-10700K 3.8GHz, AMD Ryzen 5).	String	Include speed, cores, generation where applicable.
RAM	Memory capacity and type (e.g., 16GB DDR4).	String	
Storage_Capacity	Hard disk or SSD size and type (e.g., 1TB HDD, 512GB SSD).	String	
Monitor_Size	Screen size in inches (e.g., 15.6", 24") – applicable for desktops, laptops, or standalone monitors.	String	Leave blank for non-display devices like printers.
Operating_System	Installed OS and version (e.g., Windows 11, macOS Ventura, Chrome OS).	String	
IP_Address	Network IP address for connected devices.	String	Optional for networked hardware like computers or printers.
MAC_Address	Hardware MAC address for network interfaces.	String	Useful for IT security and tracking.

Hardware Inventory List Content Suggestion (Cont.)

Location	Current physical location (e.g., Room 101, Library, Admin Office, Building A).	String	Track room, building, or department in a school.
Assigned_To	Person or department the asset is assigned to (e.g., Teacher John Doe, Science Dept, Student ID 12345).	String	Include user ID or name for accountability.
Purchase_Date	Date the asset was purchased.	Date	Format: YYYY-MM-DD.
Purchase_Price	Cost at time of purchase (e.g., $850.00).	Decimal or Currency	Include currency symbol if needed.
Vendor	Supplier or seller (e.g., Best Buy, School District Vendor).	String	
Funding_Source	Source of funds (e.g., School Budget, Grant, Donation).	String	Relevant for schools to track budgets and grants.
Warranty_Expiry_Date	End date of the warranty.	Date	Automate alerts for upcoming expirations.
Service_Contract_Details	Description of any ongoing service agreements (e.g., 3-year on-site repair with ABC Tech).	String	Include contract number or terms.
Support_Contact	Contact info for support (e.g., Vendor phone: 555-1234, Email: support@vendor.com).	String	Multiple contacts can be separated by semicolons.
Insurance_Details	Insurance policy info if applicable (e.g., Covered under school policy #XYZ).	String	For high-value items in schools.
Status	Current operational status (e.g., Active, In Repair, Retired, Lost/Stolen).	String	Use dropdown: Working, Needs Repair, Decommissioned.
Condition	Physical or functional condition (e.g., Excellent, Good, Fair, Poor).	String	Based on audits; include notes on damage.
Last_Audit_Date	Date of the most recent status audit or inspection.	Date	

Hardware Inventory List Content Suggestion (Cont.)

Depreciation_Value (Optional)	Current depreciated value of the asset.	Decimal or Currency	Calculated based on purchase price and age; useful for financial reporting.
Notes	Additional comments or history (e.g., Upgrade history, repair logs).	Text	Free-form field for any other details.

Glossary of Terms

Term	Definition
Asset management	The structured process of identifying, recording, tracking, maintaining, and disposing of school IT assets (hardware, software, and related records) throughout their lifecycle.
Hardware Asset List	The master inventory of school-owned hardware with key fields such as asset number, serial number, specifications, purpose, location, condition, and warranty details.
Software Asset List	The inventory of software titles and licenses, including license counts, expiry dates, installed devices (by asset number), versions, and firmware where applicable.
Asset number / Asset ID	A unique identifier or tag assigned to each asset to enable tracking, auditing, and cross-referencing between lists.
Master list	A single, authoritative inventory (often a spreadsheet or database) used for filtering/querying all asset information.
Appendix fields	The recommended data fields for inventories (e.g., CPU, RAM, storage, serial, location) listed in the guide's appendix.
Completeness review	A check to ensure all assets in use are included in the inventory (no missing items).
Correctness review	A check to ensure asset records are accurate (e.g., status, location) and that disposed or retired assets are not listed as active.
Asset status audit	A periodic or ad-hoc check of whether a device can still serve its intended purpose; results are recorded (pass/fail with justification).
Hardware Asset Status Audit Records	The log of audit dates and outcomes for hardware assets, including justification for failures to support repair/replacement decisions.
Disposal Records	The register of proposed and completed disposals, including asset numbers, justifications, approval status, and final disposition.
Lifecycle management	The end-to-end process of onboarding, deployment, maintenance, repurpose, replacement, and disposal of assets.
Repurpose	Reassigning an asset to a new role or user (e.g., moving a PC from office use to testing).
Testing hardware	Devices set aside for lab/testing that must still appear in the inventory with a clear purpose/status.
Replacement pool	Spare devices recorded in the inventory that can be deployed when an asset fails or is under repair.
Warranty details	Support terms recorded for each asset (coverage period, vendor contacts) to guide repair/replacement decisions.
Condition	Status information such as working, under repair, failed, or to be disposed, used to prioritize actions.

Firmware	Embedded software on devices other than PCs/servers (e.g., network gear) that should be tracked and updated.
License count	The number of rights to install/use a software title recorded in the Software Asset List.
License expiry	The date when a software entitlement ends; used to plan renewals or removals.
Installed device mapping	Linking a software record to the hardware asset number on which it is installed.
Unauthorized applications	Software not approved for school use; should be detected (e.g., by scanners) and removed.
Software scanners	Discovery tools or scripts used to compile reports of installed applications for comparison with the Software Asset List.
Technical controls for software	Configuration or policy settings that prevent installation or execution of unapproved applications.
Status fields	Inventory fields indicating current state (e.g., Active, In storage, To be disposed, Disposed) to support audits and reporting.
Inventory reconciliation	The process of comparing physical checks and scan results with the inventory to resolve discrepancies.
Disposal procedure	The steps to approve and carry out asset disposal, including secure data wiping and e-waste compliance.
Secure data wiping	The use of approved tools/methods to irreversibly erase data from a device prior to disposal or reassignment.
E-waste compliance	Disposal in line with government or school environmental policies, including certified recycling partners.
Cross-reference key	The common field (typically the asset number) used to link hardware and software records.
User/custodian	The person or role currently responsible for an asset; recorded for accountability.
Location	The physical placement of an asset (e.g., Room number); used for audits and recovery.
Purpose/role	The intended function of an asset (e.g., “Room 101 PC,” “Classroom projector”), aiding suitability checks and audits.
N/A (not applicable)	A placeholder value for fields that do not apply to a particular asset (e.g., CPU model for a monitor).
Change trigger	Events that require inventory updates (e.g., acquisition, retirement, failure, audit discrepancy).
Inventory label	A visible sticker or tag on each device (e.g., Asset ID and purpose) to simplify identification and audits.
Audit justification	The explanation recorded when an asset fails a status audit, supporting repair or replacement decisions.
Standard build image	A captured, hardened configuration image used to deploy or reset devices consistently and quickly.
Table linkage	The method of joining hardware and software lists (e.g., via asset number) to enable combined queries and reports.

End of Document

Practical Guide to Access Control

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for data labelling in schools across Hong Kong. Its aim is to help educational institutions maintain a robust access control system, with a detailed access list to track permissions, ensuring that school systems and sensitive data are accessed and handled securely only by the parties that should have access to the information.

The scope of this guide includes the creation of a formal access control policy designed around "Review Triggers", which are specific events that would prompt a systematic review of access rights to ensure the right parties retain access accordingly. This guide will also cover the logging of access changes and performing regular reviews to maintain secure access. It is designed to be adaptable for different school sizes, system types, and available resources. These guidelines have been derived from various accredited sources, including the Education Bureau of Hong Kong (EDB) as well as the Centre for Internet Security, both of whom have provided guidance and resources that are used to form the basis of these guides.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Achieve scalable permission management by implementing Role-Based Access Control (RBAC)
- Implement important principles and technologies such as Principle of Least Privilege, Separation of Roles and multi-factor authentication to regulate access effectively
- Manage passwords securely and use private keys for administrative tasks, with one-time authentication codes

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Maintaining an Access Control Standard

This section describes the creation, and the due diligence required for maintaining proper access control mechanisms aside from the technical controls. Technical controls should merely serve as enforcement of the policies defined in this section.

2.1. Development of Access Control Policy

Outline the creation of a formal policy (Access Control Policy) defining rules for granting, restricting, and revoking access based on business needs. Draft another document (Access List) specifying access to keep track of granted access rights.

Below lists out the things that the IT should consider when doing so:

- **Formal request procedures:** Use a standardized form and ticketing system for access requests that require users to provide justification.
- **Request verification:** How the IT should verify the authenticity of requests, e.g. requests require confirmation from school management.
- **Restricting Access:** Any procedures to work out the least required access rights for the justification/business need provided.
- **Revoking Access:** Any controls needed to revoke access after a certain period of inactivity, or periodic reviews (e.g., annually) to revoke access. Also include any notification mechanisms and the procedures of reacting to such notifications.
- **Onboarding Procedures:** Apart from the request-based procedures, any batch procedures for onboarding (e.g., Giving out a set of basic access rights to a Teacher/Student/Contractor)
- **Define Review Triggers:** Define a list of circumstances to review the access granted to a user.

Adaptation Tips:

- Incorporate this access control review with the preparation for network segregation described in Guide to Network Management and Wireless Security.
- The latter sections of this document will provide concepts that will facilitate processes mentioned in this section.

Practical Examples:

- Incorporate
- Make an access list with the following columns:
  User ID/Name: Any method of identifying staff members.
  Role/Position: e.g., Teachers, Contractors

Asset/System Accessed: Target of granted access.
Access Level: e.g., Admin, Read/Write, Read Only.
Grant Date
Expiry Date
Approver e.g., Principal, IT Admin
Justification

2.2. Review Triggers

Define the circumstances when the access rights of a certain user have to be reviewed. Below is a list for schools to consider and refer to. Schools should adopt to their actual circumstances themselves.

User Lifecycle and Status Changes (Staff/Employees)

- **Employee or Staff Changes**: Review and revoke access immediately upon termination, resignation, retirement, or end of employment contract for teachers, administrative staff, or IT personnel to prevent unauthorized access to school systems (e.g., email, student databases).
- **Role or Position Changes**: Conduct a review when an individual is promoted, demoted, transferred to a different department, or assumes new responsibilities (e.g., a teacher becoming a department head), adjusting access to align with the new role's needs under the least privilege principle.
- **Temporary Assignments or Leaves**: Revoke or suspend access at the end of short-term roles, such as substitute teachers, interns, or staff on sabbatical, maternity leave, or long-term sick leave; reinstate only upon return and verification.
- **User Death or Incapacity**: In rare cases, immediately revoke access upon notification of a user's passing or long-term incapacity, handling data transfer per legal protocols.

Third-Party and External Engagements

- **Contractor or Vendor Engagements**: Review and revoke access upon completion of projects, expiration of contracts, or when third-party services (e.g., IT maintenance vendors) are no longer required, including removal of any temporary accounts or VPN access.
- **Vendor or Service Provider Updates**: Review access if external services (e.g., cloud providers like Google Workspace) change their terms, or if the school switches providers, ensuring no lingering access from old integrations.

Student-Specific Changes

- **Student Status Changes**: For student accounts, review and revoke access upon graduation, transfer to another school, dropout, or suspension/expulsion to protect ongoing data integrity in learning management systems.
- **Age or Eligibility Milestones**: For age-restricted access (e.g., certain educational tools for minors), review and adjust upon students reaching maturity thresholds or changing grade levels.
- **End of Academic Year or Semester**: Systematically review student and temporary staff access at term ends to archive or revoke rights, preparing for the next cycle.

Parent-Specific Account Changes

- **Student Graduation/Withdrawal**: The departure of a student from the school, either by graduation or by student withdrawal, must trigger an automatic and immediate disabling of the parent accounts.
    - In the case that a student's sibling also studies in the school, the parent account is to remain in use until all associated family members have graduated/withdrawn.
- **Change in Custody/Guardianship:** In the case that there are legal changes in custody or guardianship responsibility of the student (possible due to family situations, student reaching 18 years of age), establish a formal process that allows school administrative staff to inform IT to conduct a review of the privileges associated to parent accounts for the student.

Security Incidents and Threats

- **Policy Violations or Security Incidents**: Immediately review and potentially revoke access if a user is involved in a security breach, misuse of systems (e.g., sharing credentials), or violation of acceptable use policies, pending investigation.
- **Insider Threat Indicators**: Proactively review access upon detection of suspicious behavior, such as unusual login patterns or HR-flagged issues like impending disciplinary actions.

Compliance and Regulatory Triggers

- **Legal or Regulatory Requirements**: Revoke access in response to court orders, data protection requests under PDPO, or compliance audits that identify over-privileging or non-compliance with standards like ISO 27002 or G3 guidelines.
- **Audit Findings**: Following internal or external audits, review and revoke access based on recommendations, such as identifying segregation of duties issues or unauthorized escalations.
- **Policy or Guideline Updates**: After revisions to the school's Access Control Policy or adoption of new standards (e.g., updates to EDB recommendations), conduct a full review to align existing access with the changes.

Routine Maintenance and Monitoring

- **Inactivity or Dormant Accounts**: Periodically scan for and revoke access to accounts inactive for a defined period (e.g., 90 days for staff, end of semester for students) to mitigate risks from forgotten or abandoned accounts.
- **Periodic Scheduled Reviews**: Perform routine audits at fixed intervals, such as quarterly for privileged accounts or annually for all users, to verify that access remains justified by current business needs and remove any unnecessary permissions.
- **Training or Certification Expirations**: Revoke specialized access (e.g., to sensitive research tools) if required certifications or training lapses, reinstating only after renewal.

System, Data, and Organizational Changes

- **System or Application Changes**: Review access rights during major updates, migrations to new software (e.g., switching to a new cloud-based grading system), or decommissioning of old systems to ensure compatibility and eliminate obsolete access.
- **Organizational Restructuring**: In cases of school mergers, department reorganizations, or changes in administrative structure, review all affected users' access to realign with the new setup.
- **Merger with External Systems**: When integrating with partner institutions (e.g., shared library systems), review access to prevent unintended cross-access.
- **Data Classification Changes**: If information assets are reclassified (e.g., from public to confidential due to new privacy concerns), review and restrict access accordingly for all users.
- **Technology or Device Changes**: Revoke access tied to specific devices upon loss, theft, or decommissioning of hardware (e.g., school-issued laptops), or when users switch to new devices requiring re-authentication.

Incident Response and Emergencies

- **Emergency or Crisis Situations**: Temporarily review and revoke non-essential access during incidents like cyberattacks, natural disasters, or pandemics to minimize exposure, restoring only as needed post-recovery.
- **Post-Incident Recovery**: After resolving any access-related incident, perform a comprehensive review to confirm all temporary measures (e.g., emergency revocations) are appropriately finalized.

Other Administrative Triggers

- **Management or User Requests**: Act on formal requests from supervisors, HR, or the users themselves to revoke access when it's no longer needed (e.g., after completing a specific task like exam preparation).

2.3. Logs and Audits

Retain logs for every access control change such that it can be later reviewed in regular audits. Perform regular review on granted access rights.

Adaptation Tips:

- Reviews can be more frequent for the privileged accounts and access rights (e.g., admin, read access on sensitive servers) and less frequent for others. A full review at least annually is recommended.

3. Access Control Concepts

This section provides explanation on common access control concepts and describes how a school could integrate these concepts in their access control policy.

3.1. Role-Based Access Control

Role-Based Access Control is a structured access control methodology that assigns permissions based on predefined roles corresponding to job functions, rather than individual user identities. Permissions are associated with roles, and users are assigned to roles, ensuring consistent and scalable access management.

Adaptation Tips:

- Define roles based on operation use cases, e.g., teachers, contractors, IT services, parents, etc.
- When there are changes of personnel and roles, update the roles of the staff instead on individual access rights.
- To accommodate temporary access grants, make roles for temporary access to a specific resource (e.g., make roles like “Web server 1 R/W”, “Backup Server 3 Read”) such that any temporary access rights can be identified by looking at the roles of a user.

3.2. Least Privilege and Need-to-Know Basis

Least Privilege and Need-to-Know Basis are two similar concepts that often come hand in hand,

- **Least Privilege:** The Principle of Least Privilege mandates that users, systems, or processes are granted only the minimum permissions necessary to perform their authorized functions.
- **Need-to-Know Basis:** The Need-to-Know Basis mandates that access to information is restricted only to users who has a need to access such information.

In essence, these two clauses together demand that access is only given to those who need it, and those who are granted access are given the least amount of access they need to perform their jobs.

Practical Examples:

- Assume a case when ICT Teachers has special access to school infrastructure than regular teachers. The IT should establish two roles for this case – "Teacher" and "ICT Teacher". The "Teacher" role is assigned to all teachers for their basic access, and "ICT Teachers" is assigned to ICT Teachers for their special access to school infrastructure.

3.3. Separation of Roles

Separation of Roles is a concept for managing highly elevated privileges. Accounts with highly privileges should be dedicated to only the jobs which needed those elevated privileges. Tasks which do not require elevated privileges should be done on accounts without escalated privileges.

Practical Examples:

- Make two accounts for administrators: One for administrative purposes and the other for day-to-day work.

4. Technical Controls

Application Layer Access Controls are typically done via technical controls. For Physical Access Controls and Network Layer Access Controls, see their respective guides.

This section lists out various technical controls in authenticating users across networks and their relevant facts. Nevertheless, the scope of the controls is limited to controls

which require user interactions. Schools should take note of them when implementing these technical controls to enforce their access control policy.

4.1. Password Authentication

Passwords are by far the most common authentication method. Relevant considerations of implementing a password authentication include:

- Strength: align with Guide to Password Management to enforce strength requirements on users.
- Transmission: Passwords should be transmitted across a securely end-to-end encrypted channel (e.g., TLS 1.3 connections) to limit exposure.
- Authentication Server Management: Passwords should be hashed and salted, limiting damage upon leakage.

Passwords essentially require users to proof their identity via knowledge of the password.

Adaptation Tips:

- A password's strength heavily relies on the length of password and that it has not been reused elsewhere. Follow the Guide to Password Management to enforce strength requirements on users.

4.2. Private Keys

There are two cases when a private key stored at endpoint can be used to authenticate a user: To authenticate with a client certificate, or to authenticate to an SSH session.

- Strength: Private Keys are generally viewed as highly secure providing cryptographic levels of entropy.
- Transmission: Passwords should be transmitted across a securely end-to-end encrypted channel (e.g., TLS 1.3 connections) to limit exposure.
- Authentication Server Management: A set of accepted public keys will be stored on the authentication server.

This essentially requires users to proof their identity via possession of the private key.

Adaptation Tips:

- To authenticate with private keys requires a private key in each endpoint used to log in to a system. This means it also heavily relies on the security of the system with the private key.
- Although secure, this often proves to be difficult to be deployed in scale and is often reserved for administrative tasks.
- Most private key managers enforce encryption with a passphrase on generated private keys. Private keys should be encrypted unless specific constraints (e.g., automation) require otherwise, which would require other remediations (e.g., offline hardware storage in a locked cabinet, Hardware key embedding, etc)

4.3. One-time Authentication Codes

One-time Authentication Codes can be set up with an out of bound challenge code, either from an authenticator or a message or a call.

- Make sure this authentication code is sent out-of-bound (e.g., to someone's mobile phone instead of their work email, which may be compromised).
- Make sure that the authentication code expires within a short time (e.g., 90 seconds).
- Make sure that only the latest authentication code is accepted.

This essentially requires users to proof their identity via access of the pre-established out of bound communication channel, typically by the possession of their phone.

Practical Examples:

- Dedicated authenticators, like Microsoft Authenticator or Google Authenticator, provide more functionality than simple authentication code generations, but they all require a possession of a device.

4.4. Multi-Factor Authentication (MFA)

Multi-Factor Authentication means any authentication of a user should be based on two or more factors described below:

- The things they know: Passwords, Security Questions, etc.
- The things they possess: Phones, private keys on USB, MFA tokens, etc.
- The things they are: Biometrics, etc.

All things considered, what's feasible for mass deployment in schools are listed above, which means implementations of MFA often result in password + authentication code/authenticators.

5. Review and Improvement

5.1. Regular Policy Review

Set a reminder to review your school's data handling and labelling standards at least once a year, or whenever there are changes to your IT systems. Involve both IT staff and teaching/administrative colleagues to gather helpful feedback.

5.2. Adapting to New Threats and Technologies

Stay updated about new cyber threats that can affect schools, such as phishing scams or password leaks. Also, be aware of new technology or software updates that might offer better ways to protect passwords, e.g. two-factor authentication.

5.3. Making Improvements

After each review, update your password policy as needed. Communicate any changes clearly to staff and students, and provide simple instructions or workshops to help everyone follow the new rules.

Appendices

Glossary of Terms

Term	Definition
Access Control Policy	A formal document that defines the rules, procedures, and responsibilities for granting, managing, and revoking access to school systems and data.
Access List	A detailed record or log that tracks who has access to what, including user ID, role, access level, dates, and justification for the access.
Authentication Factors	The different categories of credentials used to verify a user's identity: something you know (password), something you have (phone/token), and something you are (biometrics).
Dormant Accounts	User accounts that have not been accessed for a defined period (e.g., 90 days), posing a security risk if not disabled or removed.
Hashed and Salted	A security method for storing passwords where a password (hash) is combined with a unique random value (salt) before being stored, making it much harder to crack.
Least Privilege (Principle of)	A security concept mandating that users and systems are granted only the absolute minimum permissions required to perform their specific, authorized tasks.
Multi-Factor Authentication (MFA)	A security process that requires users to provide two or more different authentication factors to verify their identity, significantly strengthening security.
Need-to-Know Basis	A security principle that restricts access to information only to those individuals who have a legitimate, job-related reason to view or use it.
Onboarding Procedures	Standardized, pre-defined processes for granting a baseline set of access rights to new users (e.g., teachers, students) when they join the school.
One-Time Authentication Code	A temporary, single-use code sent to a user's device (e.g., via SMS or an authenticator app) to serve as a second factor of authentication.
Out-of-Bound	A communication channel that is separate from the primary channel being used for authentication (e.g., receiving a code on a phone instead of the work email that is being logged into).
Over-privileging	The state of a user account having more access rights and permissions than are necessary for their role, creating a significant security risk.
Private Key	A secret, cryptographic key stored on a user's device that is used in public-key cryptography to prove identity, often for secure SSH sessions or with client certificates.
Public Key	The corresponding cryptographic key to a private key, which is shared openly and used by servers to verify the identity of a user who possesses the matching private key.
Review Triggers	A predefined set of events or circumstances (e.g., a change in role, employee departure, or security incident) that automatically initiates a review of a user's access rights.
Role-Based Access Control (RBAC)	An access management methodology where permissions are assigned to predefined roles (e.g., "Teacher," "Admin") rather than to individual users, simplifying management.

Term	Definition
Segregation of Duties	A security principle aimed at preventing fraud and errors by ensuring that no single individual has control over all aspects of a critical task. Often related to Separation of Roles.
Separation of Roles	The practice of using separate accounts for different functions, especially requiring administrators to use a standard user account for daily tasks and a separate privileged account for administrative duties.
SSH (Secure Shell)	A cryptographic network protocol used for operating network services securely over an unsecured network, often for remote command-line administration.
Ticketing System	A software system used to manage and track user requests, including formal requests for access to systems or data.
TLS (Transport Layer Security)	A cryptographic protocol that provides end-to-end security for data transmitted over a network, such as when a password is sent from a browser to a server.

End of Document

Practical Guide to Password Policy Management

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for password management in schools across Hong Kong. Its aim is to help educational institutions establish secure, consistent, and effective password practices that protect school systems and sensitive information.

The scope of this guide includes password policy development, technical controls, account management procedures, and user support. It is designed to be adaptable for different school sizes, system types, and available resources.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Set and enforce effective password policies,
- Implement secure storage and authentication methods,
- Respond to password-related incidents,
- Support end users with password best practices,
- Maintain compliance with applicable data protection requirements.

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Establishing a Password Policy

This section outlines core components of a strong password policy for schools. Use these recommendations as a foundation and adjust them to suit your school's systems, user groups, and available resources. Strong policies protect both everyday users and critical admin accounts from common threats.

2.1. Minimum Requirements

Set clear, baseline rules that all users must follow for password creation and protection.

Typical minimum requirements include:

- Passwords must be required for all user accounts that have access to school systems or sensitive information.
- Default or temporary passwords must be changed upon first use.
- Passwords should not be written down or stored in plain text where others can access them.

Adaptational Tips:

- Schools can add requirements for specific roles (e.g., stricter rules for staff with access to administrative systems) or adjust according to the sensitivity of different platforms.
- For younger students, consider using memorable passphrases rather than complex passwords, and provide guidance to teachers for classroom account management.

2.2. Password Complexity & Length

Strong passwords are harder to guess or crack. Recommend the following:

- **Length:** Minimum 8–12 characters for general users (longer is better if systems allow).
- **Complexity:** Use a mix of uppercase and lowercase letters, numbers, and symbols.
- **Avoid simple patterns:** No easily guessed words or patterns (e.g., "password," "1234," school names).

Adaptational Tips:

- Consider passphrases (multiple unrelated words) for younger users who struggle with complex passwords. Adjust complexity as appropriate for different age groups or user roles.

2.3. Prohibited Passwords and Sharing

Prevent common password mistakes to reduce risk.

- **Block common/breached passwords:** Avoid passwords known to be weak or compromised (e.g., "123456," "qwerty").
- **No password sharing:** Users must not share passwords, even within staff or student groups.
- **Unique passwords:** Do not use the same password for different school systems.

Adaptational Tips:

- Use tools or directory settings to automatically block common passwords where possible. Reinforce these rules with regular reminders and training.
    - *In Google Workspace for Education, admins can set minimum password length and complexity requirements in the Admin Console under Security > Password Management.*
    - *In Microsoft Active Directory, use Group Policy Objects (GPOs) to enforce password complexity and length.*

2.4. Frequency of Password Changes

Overly frequent password changes can lead to weaker passwords. Best practices suggest:

- **Only require changes when necessary:** Change passwords if there is a suspected compromise or other security incident.
- **Scheduled changes for sensitive accounts:** For critical systems, consider requiring changes every 6–12 months.
- **Mandatory change after breach:** Always require a password reset after any suspected breach or risk event.

Adaptational Tips:

- Tailor change frequency to suit your environment—avoid frequent resets unless absolutely necessary, especially for students.
    - Use your user directory or account management system to flag potentially compromised accounts for required password resets.
    - After a phishing incident, bulk reset passwords for affected users via admin tools (e.g., Google Admin Console, AD Users and Computers).

2.5. Admin and Technical Account Passwords

Accounts with admin or system-level access require stricter controls to protect critical infrastructure and sensitive data.

- **Longer passwords:** Require at least 14–16 characters, preferably using a passphrase (e.g., Sunny!Beach_Chair7Horse).
- **Unique and complex:** Every admin account should have its own unique, strong password—never reused across systems.
- **Use password managers:** Deploy a reputable password manager (such as Bitwarden, LastPass, or KeePass) to generate and store complex passwords securely.
- **Enable Multi-Factor Authentication (MFA):** Always turn on MFA for admin and privileged accounts.
- **No shared admin accounts:** Assign individual admin accounts to each staff member; don't share login details.
- **Regular review:** Periodically audit admin accounts, removing unnecessary or unused accounts.

Adaptational Tips:

- If resources are limited, prioritize longer and more complex passwords for admin accounts and enable MFA for any cloud or critical system accounts at minimum.
    - Require all admin accounts in Google Workspace or Microsoft 365 to use MFA (enforced via the Admin Console or Azure AD).
    - Use password manager vaults with shared access controls for IT teams (e.g., Bitwarden Organizations).
    - Schedule regular reviews of all admin accounts (e.g. quarterly) by exporting user lists from your directory platform and disabling unused accounts.

- **Example strong admin passphrases:**
    - Sunlight$Giraffe!82_Rain
    - Puzzle#Leaf_Train!934
    - Ocean_Cable2!BridgeMoon

2.6. SaaS Solutions and Third-Party Applications

Many schools use online platforms and apps for learning, administration, and communication. Even if you can't control every setting, you can still promote strong password practices and manage risk.

- **Review Password Options:** Whenever possible, set strong password policies for user accounts in SaaS platforms (e.g., Google Workspace, Microsoft 365, learning management systems, library systems).
- **Enforce Multi-Factor Authentication (MFA):** Enable MFA for staff/admin accounts in any SaaS solution that supports it. Encourage staff to turn on MFA for their personal school accounts as well.
- **Unique Passwords Per Platform:** Require users, especially staff, to use unique passwords for each SaaS or third-party application. Example: Staff should not use their school email password as their Zoom, library, or e-learning portal password.
- **Use SSO (Single Sign-On):** Where available, integrate SaaS applications with your school's main directory (e.g., Google, Microsoft Azure AD) using SSO. This centralizes authentication and simplifies password management.
- **Password Managers:** ncourage staff to use password managers for tracking credentials to third-party platforms, especially if they must use many different services.
- **Vendor Communication:** When adopting new SaaS or third-party apps, ask vendors about their password policies, MFA support, and how they protect user credentials.

Adaptational Tips:

- Limited IT Resources: Focus on user education and use SSO wherever possible to minimize the number of passwords staff and students must remember.
- More Advanced IT: Standardize onboarding/offboarding processes for SaaS apps and keep an inventory of platforms in use, including who has admin rights.

3. Implementing Password Practices

This section explains how to put your password policy into everyday practice, with both technical controls and procedures. It includes examples for common school systems, and tips for adapting these measures to your environment.

3.1. Enforcing Policies (General Methods)

Technical Enforcement: Use your directory services or cloud admin consoles to enforce password length, complexity, and change requirements. *Example: In Microsoft Active Directory, use Group Policy Objects (GPOs) for enforcement; in Google Workspace, adjust password settings in the Admin Console.*

- **User Education:** Provide clear instructions and reminders about password rules during onboarding and in periodic security campaigns.
- **Regular Audits:** Periodically review accounts and policy compliance. *Example: Run reports to identify accounts with weak or non-compliant passwords (if your system supports this).*

Adaptational Tips:

- If you lack technical tools, focus on user education and regular reminders.

3.2. Secure Password Storage

- **Never Store in Plain Text:** Do not keep passwords in spreadsheets, emails, or paper notes.
- **Use Password Managers:** Provide or recommend a secure password manager (e.g., Bitwarden, KeePass) for staff and IT admins.
- **System Storage:** Ensure any system that stores passwords (e.g., homegrown applications) uses encrypted, salted hashing—not plain text or simple encryption.

Practical Examples:

- Use Bitwarden or LastPass for staff and admin password storage.
- For applications developed in-house, have your IT vendor confirm that password storage uses strong, industry-standard encryption (e.g., bcrypt).

3.3. Handling Forgotten Passwords and Resets

- **Self-Service Reset:** Enable self-service password reset features with secure identity verification (e.g., secondary email or SMS code).
- **Helpdesk Process:** If users must contact IT for resets, require verification of identity (such as a staff badge or answering security questions).
- **Password Reset Links:** Send password reset links that expire after a short time (e.g., 30–60 minutes).

Adaptational Tips:

- Define simple, secure reset procedures for schools with limited IT staff.

Practical Examples:

- Google Workspace and Microsoft 365 offer self-service password reset options for users with recovery info set up.
- For younger students, password resets may be handled by classroom teachers with verification.

3.4. Account Lockout and Recovery

- **Lockout After Failed Attempts:** Configure systems to lock out accounts after a set number of failed login attempts (e.g., 5–10 tries).
- **Notify Users and Admins:** Alert users and IT staff when accounts are locked to detect possible attacks.
- **Recovery Procedures:** Provide a documented process for verifying identity and unlocking accounts.

Practical Examples:

- In Active Directory, set account lockout policies via Group Policy.
- In Google Workspace, monitor login alerts for suspicious activity.

4. Enhancing Security

Beyond basic password rules, additional security measures greatly reduce the risk of account compromise. This section highlights advanced practices every school should consider to protect both users and sensitive systems.

4.1. Multi-Factor Authentication (MFA)

- Require MFA for staff/admin accounts on all systems that support it. Strongly encourage MFA for all users where practical.

4.2. Monitor for Weak or Compromised Passwords

- Use available tools to check for weak, reused, or breached passwords.

Adaptation Tips:

- Limited IT Resources: Prioritize MFA for admin accounts, use simple but secure reset and recovery procedures, and focus on user education.
- More Advanced IT: Automate policy enforcement, use password managers, and implement regular monitoring and reporting.
-

Practical Examples:

- In Microsoft 365, enforce MFA via Azure AD security defaults.
- Use Google's Password Alert extension to warn users if they enter their school password on non-Google sites.
- Use breach monitoring tools (e.g., Have I Been Pwned) to alert staff if their credentials appear in public breaches.

5. Incident Response

This section describes what to do if a password is compromised or an account breach is suspected. Fast, organized response limits damage and protects school data.

5.1. Responding to Compromised Accounts

1. Immediate Actions

- Disable or Lock Account: Temporarily block access to prevent further misuse.
- Reset Password: Require a new, strong password before restoring access.
- Force Logout: Ensure the compromised account is signed out of all sessions and devices.
- Enable MFA (if not already): Add multi-factor authentication for extra protection.

Practical Examples:

- In Google Workspace, use the Admin Console to reset a user's password and sign them out of all devices.
- In Microsoft 365, use Azure AD to reset credentials and revoke tokens.

2. Investigate the Incident

- Check Account Activity: Review recent logins, password changes, and sent emails for suspicious activity.
- Identify the Method: Determine how the compromise occurred (phishing, weak password, malware, etc.).
- Scan Devices: Run antivirus/antimalware scans on computers where the breach occurred.

3. Contain and Remediate

- Reset Other Affected Credentials: If the same password was used elsewhere, reset those too.
- Update and Patch Systems: Make sure systems are up to date to close any vulnerabilities.

5.2. Communication and Escalation

1. **Notify Key Personnel**

- Report all suspected or confirmed breaches to your school's IT or designated security contact.
- Notify leadership if sensitive data or multiple accounts are affected.

2. **Inform Affected Users**

- Let users know their account has been compromised and provide instructions for next steps (e.g., password reset, device scan).
- Communicate details only to those who need to know, balancing transparency and confidentiality.

5.3. Escalate When Necessary

- If sensitive data was accessed, or if the breach could affect many users, escalate to district IT, legal, or data protection authorities as required by law or policy.
- For major incidents (e.g., student records compromised), follow your school's data breach reporting procedures.

Practical Examples:

- If the compromise involves student personal data, notify your school's data protection officer and follow reporting requirements under the Personal Data (Privacy) Ordinance (PDPO) of Hong Kong.

5.4. Incident Documentation

- Document the details of the incident, actions taken, and lessons learned.
- After resolving the incident, review what happened and strengthen policies, training, or technical controls as needed.

6. Review and Improvement

6.1. Regular Policy Review

Set a reminder to review your school's password policy at least once a year, or whenever there are changes to your IT systems. Involve both IT staff and teaching/administrative colleagues to gather helpful feedback.

6.2. Adapting to New Threats and Technologies

Stay updated about new cyber threats that can affect schools, such as phishing scams or password leaks. Also, be aware of new technology or software updates that might offer better ways to protect passwords, e.g. two-factor authentication.

6.3. Making Improvements

After each review, update your password policy as needed. Communicate any changes clearly to staff and students, and provide simple instructions or workshops to help everyone follow the new rules.

Appendices

Glossary of Terms

Term	Definition
Password Policy	Rules for creating and managing passwords in the school.
Password Manager	A secure tool for storing and managing passwords.
Multi-Factor Authentication (MFA)	Security that requires two or more proofs of identity to log in.
Phishing	Tricks to get people to give away passwords, often by fake emails.
Data Breach	When sensitive information is accessed without permission.
Admin Account	A user account with higher-level control over systems.
Password Reset	Process to change a forgotten or compromised password.
Compromised Account	An account accessed by someone without permission.
Encryption	Converting information into a code to prevent unauthorized access.

End of Document

Practical Guide to Maintenance & Patch Management

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for maintenance and patch management in schools across Hong Kong. Its aim is to help educational institutions manage IT updates and changes, focused on patch management and change management through safe testing and deployment procedures.

The scope of this guide includes a lifecycle for change and patch management that follows a formal process of request, impact assessment and testing with rollback procedures to ensure secure rollout. The lifecycles also account for continuous improvement of the processes through regular review at intervals set by the school. This guide is designed to be adaptable for different school sizes, system types, and available resources. These guidelines have been derived from various accredited sources, including the Education Bureau of Hong Kong (EDB) as well as the Centre for Internet Security, both of whom have provided guidance and resources that are used to form the basis of these guides.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for software and patch management for IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Proactively identify vulnerabilities through scheduled scanning and monitoring threat intelligence, using CVSS scores
- Securely deploy and verify patches, by testing in isolated environments, deploying with rollback procedures to ensure system stability
- Conduct verification scans to confirm that vulnerabilities have been patched/remediated
- Enable continuous improvement and responses to evolving cyber threats, through regular policy reviews

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Establishing a Patch Management Lifecycle

This section details guidelines to establishing a structured lifecycle for acquiring, testing, deploying, and verifying patches to minimize vulnerabilities. Schools should take reference and ensure patches are applied systematically and balance between urgency and system stability.

2.1. Vulnerability Identification and Assessment

The school should consider the following measures to stay informed about vulnerability and patch information:

- **Establish Scanning Schedule**: Perform automated vulnerability scans regularly for systems and general networks/devices. align with academic calendars to avoid disruptions.
- **Monitor Threat Intelligence**: Subscribe to daily alerts from HKCERT/GovCERT.HK and vendors (e.g., Microsoft, Google) to track high-severity issues affecting school software (e.g., browsers, OS).
- **Risk Assessment Process:** Read CVSS scores and metrics on exploitability and impact (e.g., data breach risk); make priority for high-risk items (e.g., score >7) for immediate action.
- **Define Response Time:** Define the timeframe in which the vulnerability has to be patched. This can depend on the criticality of the vulnerability.
- **Documentation and Review**: Log findings in a vulnerability register (e.g., spreadsheet) with affected assets, severity, and owner; review quarterly to identify trends (e.g., recurring unpatched software).

Adaptation Tips:

- When establishing scanning schedules, align with school calendars to avoid potential disruptions.
- Consider having two tiers of response based on the CVSS scores/rating of the vulnerability (e.g., High risk items require immediate action; medium and low vulnerabilities are patched in regular patching routines)

Practical Examples:

- Use Nessus Community to scan for vulnerabilities. Prioritise and rotate between critical systems and network devices if target capped.

2.2. Patch Acquisition and Verification

The school should download patches only from official vendor sources and should verify the integrity of the download. Below lists procedures a school should highly consider when acquiring patches from the internet:

- Contact the vendor of the software/hardware for guidance if the official source for patch distribution is unclear.
- Ensure proper TLS connection when downloading and browsing the official site for the patch.
- Download the patch in a virtual machine in a network segregated from the internal network.
- Verify the checksums of the download. The checksums should come from an official source (e.g., official website).

Practical Examples:

- Confirm the hashing algorithm the website uses in generating the checksum, then calculate the hash of the downloaded file in the virtual machine. Common hashing algorithm includes MD5, SHA-1-384/SHA-2-256/SHA-3 etc.

2.3. Testing

Apply patches in an isolated test environment (e.g., virtual machine or isolated physical machine) to check for functionality issues. Procedures may differ between the nature of the software (software, operating system patches, firmware, etc)

- The testing environment should simulate the production environment as close as possible, and the test cases should mimic actual use cases as close as possible.
- The testing environment should be segregated from the internal network.

Practical Examples:

- Use the dual-boot feature for new firmware for networking devices for easy roll-back if testing fails.
- Conduct testing in a virtual machine for an application update.
- Conduct testing of an OS patch in a physical machine with the same specifications and driver versions as other workstations in the school.

2.4. Deployment and Rollback

Before deployment, be prepared for an emergency rollback. This includes preparations like:

- Communicate about system downtime and changes. This may result in deploying during off-hours to avoid interruption to services.
- Communicate about error reporting methods.
- Determine the triggers for rolling back updates.
- Rollback Procedures should a Rollback is triggered and the relevant prerequisites for the procedures.

Adaptation Tips:

- If the deployment and rollback is laborious, consider deploying in small batches before full-scale deployment.

Practical Examples:

- For changes on critical systems (e.g., web servers), make full disk clones before deployment for easy rollback. E.g., clone all disks with dd. Rollback procedure: turn off the machine, remove all disks, insert all cloned disks, reboot.
- Use the dual-boot feature for new firmware for networking devices for easy roll-back if testing fails.
- Restore from any configuration backups such that the configurations can be aligned for networking devices.

2.5. Verification and Documentation

Rescan the deployed systems to verify that the patch has been applied successfully. See section 2.1 for details. Update the appropriate asset lists after applying patches.

3. Establishing a Change Management Lifecycle

This section details guidelines to establishing a structured lifecycle for reliability apply changes to infrastructure of the school. Schools should take reference and adopt changes to their actual scenarios.

3.1. Change Management Integration

To integrate with possible existing change management procedures, which defines the processes before acquisition of any changes, the following should be considered:

- **Formal Request and Approval**: Request approval change via predetermined communication channels and processes.
- **Impact Assessment:** Evaluate effects on the proposed change on school operations (e.g., downtime, any known risks, etc)
- **Asset Management:** Document any purchase of assets in the asset lists.

3.2. Testing

Like applying patches, the testing should be done in an isolated test environment (e.g., virtual machine or isolated physical machine) to check for functionality/compatibility issues.

- The testing environment should simulate the production environment as close as possible, and the test cases should mimic actual use cases as close as possible.
- The testing environment should be segregated from the internal network.

Adaptation Tips:

- The purpose of all testing is to minimize the risks of some process not working upon deployment, despite unable to completely eradicate such risks. Therefore, a school can should conduct risk judgements on how much resources are to be put into testing setups. E.g., if a system allows for downtime and is not critical, one could argue that testing for basic functionality is all that's needed, whereas for a backup system one may want more exhaustive testing to try to expose any problems before deployment.
- Functionality testing is generally easier than reliability testing.
- For critical assets, consider doing test deployments (e.g., open betas) to simulates real life scenarios.

3.3. Deployment and Rollback

Be prepared for an emergency rollback before deployment, just like when applying patches. All clauses within section 2.4 apply, together with the following considerations:

- We recommend documenting step-by-step rollback procedures before applying changes to critical assets due to the higher complexity.
- There is added complexity of deploying a new service in beta, which will cause data migration issues during rollback if needed.
- There may also be more triggers for rollback, such as bad user feedback.
- For any new system, determine, document, and set up logging services for monitoring.

3.4. Verification and Documentation

Continuously monitor logs for any suspicious behaviour Update the Asset Lists to reflect the recent deployment.

4. Review and Improvement

4.1. Regular Policy Review

Set a reminder to review your school's data handling and labelling standards at least once a year, or whenever there are changes to your IT systems. Involve both IT staff and teaching/administrative colleagues to gather helpful feedback.

4.2. Adapting to New Threats and Technologies

Stay updated about new cyber threats that can affect schools, such as phishing scams or password leaks. Also, be aware of new technology or software updates that might offer better ways to protect passwords, e.g. two-factor authentication.

4.3. Making Improvements

After each review, update your password policy as needed. Communicate any changes clearly to staff and students, and provide simple instructions or workshops to help everyone follow the new rules.

Appendices

Glossary of Terms

Term	Definition
Change Management	A structured process for managing all changes to IT infrastructure, from initial request and approval to deployment and verification, to minimize disruption and risk.
Checksum	A unique digital fingerprint (e.g., MD5, SHA-256) calculated from a file, used to verify the file's integrity and ensure it has not been corrupted or altered during download.
Criticality	The level of importance of a system or vulnerability, which determines the urgency and priority of patching and response efforts.
CVSS (Common Vulnerability Scoring System)	An industry standard for assessing the severity of computer system security vulnerabilities, providing a numerical score to help prioritize responses.
Deployment	The process of installing or rolling out a patch, update, or new system into the live production environment.
Dual-Boot	A feature on some network devices or computers that allows it to store two different versions of its operating system or firmware, enabling a quick rollback to the previous version if an update fails.
Full Disk Clone	An exact, bit-for-bit copy of an entire hard drive, including the operating system, applications, and all data, used as a robust backup for easy system rollback.
Hashing Algorithm	The specific mathematical function (e.g., MD5, SHA-256) used to generate a checksum or hash value from a piece of data.
Impact Assessment	The process of evaluating the potential positive and negative effects that a proposed change or patch will have on school operations, systems, and users.
Isolated Test Environment	A separate, segregated network or system (e.g., a virtual machine) used for testing patches and changes without affecting the live production environment.
Open Beta	A pre-release testing phase where a new system or major change is made available to a wider group of real users to identify issues and gather feedback before full launch.
Patch	A piece of software designed to update a computer program or its supporting data to fix or improve it, including fixing security vulnerabilities and other bugs.
Patch Management	The lifecycle of acquiring, testing, deploying, and verifying patches for operating systems and applications to keep systems secure and stable.
Production Environment	The live IT environment where day-to-day school operations take place, as opposed to a testing or development environment.
Response Time	A predefined timeframe within which a discovered vulnerability must be addressed or patched, typically based on its severity level.
Risk Assessment	The process of identifying, analyzing, and evaluating risks associated with a vulnerability, including its exploitability and potential impact.
Rollback Procedure	A pre-planned set of steps to revert a system to its previous state after a failed or problematic patch or change deployment.

Term	Definition
Test Cases	A set of specific conditions or variables under which a tester will determine whether a system is working correctly, designed to mimic real-world usage.
Threat Intelligence	Organized, analyzed, and refined information about potential or current attacks that threaten an organization, often received from sources like HKCERT.
TLS (Transport Layer Security)	A cryptographic protocol that ensures a secure, encrypted connection when browsing websites or downloading files, protecting data in transit.
Vulnerability Register	A log or document (e.g., a spreadsheet) used to track identified security vulnerabilities, including their severity, affected assets, status, and owner.
Vulnerability Scanning	The automated process of using software tools to scan networks and systems to identify known security weaknesses and unpatched software.

End of Document

Practical Guide to Data Backup and Recovery

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for managing data backups and recovery procedures in schools across Hong Kong. Its aim is to help educational institutions maintain a consistent baseline in backing up data securely and establishing a series of steps in managing recovery steps and procedures for data recovery. labelling and safeguarding their data, ensuring that school systems and sensitive information are handled securely.

The scope of this guide includes data backup standards, technical procedures for backup and lifecycle management. It is designed to be adaptable for different school sizes, system types, and available resources. These guidelines have been derived from various accredited sources, including the Education Bureau of Hong Kong (EDB) as well as the Centre for Internet Security, both of whom have provided guidance and resources that are used to form the basis of these guides.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Establish a standard backup routine, defining a frequency, scope and retention policy
- Operate systematically with a framework for secure data handling; encryption practices and requirements for storage of sensitive data, and restricting data uploads onto third-party services
- Create a data lifecycle and deletion policy to minimize potential data exposure/breach
- Define specific retention roles for various data categories based on operational needs
- Securely delete data to ensure information is permanently irrecoverable

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Establishing a Standard Backup Procedure

This section outlines core components of a Backup Routine which a school should consider when establishing the backup procedures such that the backup procedures can be effective.

2.1. Frequency and Scope of Backup

Define clear backup intervals (e.g., daily, weekly, etc) for all operational data.

If the school decides to perform whole disk backups, document the frequency as part of the Backup Procedure. If the school decides to assign different backup frequencies on different data, the frequency of the backup should bear resemblance to the frequency of changes made to the corresponding data. In that case compile a list documenting the Scope and frequency for each backup task.

Adaptational Tips:

- File-based backups allow flexibility on backup frequencies across different operational data; Whole disk backups require less management at the cost of storage space.
- We highly recommend a daily backup on all operational data that is frequently modified.
- We highly recommend implementing automated software for managing local backups.

Practical Examples:

- Create a list documenting the files to backup and the frequencies. Make sure the list covers all operational data.

2.2. Backup Retention

Retain at least 3 generations of backups locally, such that older versions can be accessed when in need.

When defining the retention policy, we highly encourage schools to consider the following:

- Consider retaining 7 or 5 generations if it helps with administrating (e.g., overwrite Monday's backup the following Monday).
- Consider retaining certain backups for a longer period (e.g., first backup for the week/month/year).

Adaptational Tips:

- Align the Backup Retention Policy with the Data Lifecycle and Deletion Policy.

2.3. Offsite and Redundant Backups

We recommend having multiple backup copies, including one off-site copy if possible. Otherwise, put the redundant backups far away from the original backup or consider cloud options.

Practical Examples:

- Every week, make a full disc copy of the current backup. Store the HDD in a locked cabinet inside school office, far away from the backup server.

2.4. Backup Encryption

Backups should be treated as Data at Rest and should therefore be encrypted in accordance with Data Handling and Protection Guidelines.

The encryption key should be encrypted with a password and stored separately in an isolated device, USB stick or TPM.

Adaptational Tips:

- Make the Password at least 15 characters of length, following the Admin Password Policy.

Practical Examples:

- Store the encryption in a device with TPM-aided full disk encryption, e.g., Bitlocker.
- Use archival tools to create encrypted archives (e.g., 7zip), and then manage the password appropriately.

2.5. Backup Integrity

Store the checksum of every backup in a separate location, used for checking the integrity of the backup should a restoration is needed.

2.6. Backup Storage Media Handling

Store the backups in a secure manner by considering the items below:

- Store the backups in a physically secure place. Refer to Practical Guide to Physical and Environmental Security for details.
- Off-power USBs, SSDs and HDDs should be connected to power at least once a year to prevent data loss due to bit flips. For flash memory like USBs and SSDs, Power them for at least an hour. For HDDs, connect them for a day.

Practical Examples:

- Use SMART reporting tools to check the disk health for Drives that support such functionality.
- If the Drives show signs of old age or meets a defined threshold for replacement, replace the Disks by failing the Hardware Asset Audit, see Guide

3. Establishing Restoration Procedures

This section outlines the core components that schools must consider, in establishing effective restoration procedures. These will ensure a smooth and trackable data restoration procedure, in the case that incidents may arise.

3.1. Define Recovery Time Objectives

Define Recovery Time Objective (RTO) as the maximum acceptable time to restore a particular system after a disruption. Restoration Procedures should be a list of instructions which could be completed under this Recovery Time Objective.

Adaptational Tips:

- Define the Recovery Time Objectives based on data criticality and business impact. i.e., for how long a certain resource (e.g., web server) is allowed to be down in event of an incident.
- If any Restoration Procedures cannot be completed within the RTO timeframe, Schools should consider modifying the Restoration Procedures and if needed, the Backup Procedures.
- Resources can be divided into tiers, and then for each tier define an RTO.
- The RTO can also serve as the recovery priority for the team should there be an incident.

Practical Examples:

- Define RTO for different school resources, such as web servers, file servers, cloud platforms.
- There may be sub-components for each resource, which can be addressed in the Recovery Documentation.

3.2. Recovery Documentation

Create step-by-step recovery guides for every resource. A typical recovery guide for a certain resource (e.g., a particular server) includes the following:

- **Initial Assessment:** Guides on evaluating the scope—e.g., determine affected systems (e.g., student database vs. email), estimate data loss using RPO metrics, and isolate the issue to prevent spread (e.g., disconnect networks for suspected

ransomware). Include checklists for logging the incident timestamp, symptoms, and potential causes.

- **Backup Selection and Preparation:** Instructions for choosing the most recent viable backup (e.g., based on RTO targets like restoring critical systems within 4 hours). Detail verification steps, such as scanning for corruption or malware, and preparing recovery environments (e.g., sandbox servers to avoid overwriting live data).
- **Step-by-Step Restoration Process**: Numbered procedures for data restoration, including:
    - Accessing backups (e.g., from cloud portals or offsite drives, and decryption procedures).
    - Process of Restoration, including any special considerations on the order of restoration across different components.
    - Tools and commands (e.g., specific software used with screenshots for illustration).
- **Verification and Testing**: Guides on conducting post-restoration checks, such as integrity tests to validate data completeness (e.g., sample queries on student records), and functional testing (e.g., ensuring grading software works).
- **Rollback Procedures**: Contingency plans if restoration fails, such as reverting to an earlier backup or switching to a secondary site/DR plan.
- **Documentation and Logging**: Require logging all actions (e.g., who did what, when) for audits. Include forms for recording outcomes.

Adaptational Tips:

- Align these processes with Incident Response Playbook to make sure there are no conflicts.

3.3. Regular Restoration Drills

Restoration Drills serve as test for restorability and test for meeting the Recovery Time Objectives (RTO). Restoration Drills should therefore be conducted regularly.

Adaptational Tips:

- Consider incorporating Restorations Drills as part of Incident Response Drill.
- Two main metrics to measure would be Restoration Success and if the RTO is met.
- After a Drill, work out if there are any processes that can be optimized.
- Do not blindly modify the RTO. Leave some headroom if the RTO is met and only increase the RTO if meeting the RTO is unlikely after optimizations.

Practical Examples:

- Conduct Drills in spare server not connected to systems in production.

4. Review and Improvement

4.1. Regular Policy Review

Set a reminder to review your schools' backup standards at least once a year, or whenever there are changes to your IT systems. Involve both IT staff and teaching/administrative colleagues to gather helpful feedback.

4.2. Adapting to New Threats and Technologies

Stay updated about new cyber threats that can affect schools, such as phishing scams or password leaks. Also, be aware of new technology or software updates that might offer better ways to protect passwords, e.g. two-factor authentication.

4.3. Making Improvements

After each review, update your password policy as needed. Communicate any changes clearly to staff and students, and provide simple instructions or workshops to help everyone follow the new rules.

Appendices

Glossary of Terms

Term	Definition
Backup Encryption	The process of encoding backup data so it can only be accessed with a specific decryption key, protecting it from unauthorized access even if the storage media is stolen.
Backup Integrity	The measure of a backup's completeness and accuracy, ensuring the data has not been corrupted or altered and can be successfully restored.
Backup Retention	A policy that defines how many versions (generations) of a backup are kept and for how long before being deleted.
Backup Routine	A standardized and scheduled procedure for creating, storing, and managing backups of school data.
Bit Flips	A form of data degradation in digital storage where a single bit of data spontaneously changes its state, which can lead to file corruption over time, especially in unpowered media.
Checksum	A unique digital fingerprint generated from a file or backup, used to verify its integrity by checking if the data has been altered or corrupted.
Data at Rest	Data that is not actively moving between networks or devices and is stored on media such as hard drives, SSDs, or backup tapes.
Data Criticality	The measure of how important specific data or systems are to school operations, which helps determine recovery priorities and objectives.
Data Lifecycle	The entire process data goes through from creation to deletion, including its active use, storage, and eventual disposal.
Encryption Key	A secret piece of information (like a password or digital file) used by an algorithm to encrypt and decrypt data.
File-Based Backup	A backup method that copies individual files and folders, offering flexibility in what is backed up and at what frequency.
Generations (of Backups)	Different versions of a backup saved over time (e.g., daily backups from Monday, Tuesday, and Wednesday are three distinct generations).
Incident Response Playbook	A set of documented procedures that guide the response to a security incident, such as a data breach or system failure.
Offsite Backup	A copy of backup data stored in a separate physical location from the primary systems to protect against local disasters like fire, flood, or theft.
Operational Data	The live data required for the day-to-day functioning of the school, such as student records, financial information, and teaching materials.
Recovery Documentation	Step-by-step guides that detail the process for restoring specific systems or data from a backup.
Recovery Point Objective (RPO)	The maximum acceptable amount of data loss, measured in time. It defines how frequently backups must occur (e.g., an RPO of 24 hours requires at least daily backups).
Recovery Time Objective (RTO)	The maximum acceptable amount of time that a system or service can be offline after a disruption before it is restored to operational status.
Redundant Backups	Having multiple copies of backup data, often stored in different locations or on different media, to increase reliability.

Term	Definition
Restoration Drills	Regular, scheduled tests where data and systems are restored from backups in a controlled environment to verify that procedures work and RTOs can be met.
Rollback Procedures	A contingency plan to revert a failed or problematic restoration attempt to a previous stable state.
Sandbox Server	An isolated testing environment that allows IT staff to test software or perform restoration drills without affecting live production systems.
SMART (Self-Monitoring, Analysis, and Reporting Technology)	A monitoring system built into hard drives and SSDs that detects and reports on various indicators of drive health and reliability.
TPM (Trusted Platform Module)	A dedicated hardware chip on a device's motherboard that provides secure, hardware-based security functions, such as storing encryption keys.
Whole Disk Backup	A backup method that creates an exact copy (image) of an entire hard drive, including the operating system, applications, and all data.

End of Document

Practical Guide to Data Handling, Labeling and Data Security

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for data labelling in schools across Hong Kong. Its aim is to help educational institutions maintain a consistent baseline in labelling and safeguarding their data, ensuring that school systems and sensitive information are handled securely.

The scope of this guide includes data labelling standards, technical procedures, secure data storage and sharing, and data lifecycle management. It is designed to be adaptable for different school sizes, system types, and available resources. These guidelines have been derived from various accredited sources, including the Education Bureau of Hong Kong (EDB) as well as the Centre for Internet Security, both of whom have provided guidance and resources that are used to form the basis of these guides.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Classify data according to its importance, sensitivity and level of security required to protect the data
- Follow a uniform labelling procedure that is associated with a file/document's data class
- Securely store and send sensitive data through a simple series of steps that maintain consistent security
- Understand the data lifecycle and how best to remove/dispose of data when no longer required

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Establishing a Data Labelling Standard

This section outlines core components of a Data Labelling standard to be upheld. Such conventions allow grouping data into Data Classes for easier control enforcement. Use these recommendations as a foundation and adjust them to suit your school's use cases, user groups, and available resources.

2.1. Data Classification Rules

Define clear, baseline rules for classifying Data into 3 levels based on the impact of the event of leakage. These data classes can then be used when defining the set of controls applied to the sharing and storage of data of a specified class.

Typical Data Class include:

- Public: Publicly known knowledge, or data that will cause no harm in event of accidental disclosure.
- Internal: Any Data that contains information not in the realm of public knowledge, and of which disclosure would cause external parties to gain information not in line with PR strategy.
- Confidential: Data of which disclosure would risk heavy reputation damage, or compliance or legal implications. A common example of confidential data is Personally Identifiable Information (PII), which is any data that relates to a living individual and can infer their identity.

Adaptational Tips:

- Schools can add extra Data Classes if they serve operational needs.
- The controls may be different for data stored in different mediums (i.e., hardcopies and softcopies), but the data classification rules should be the same.

2.2. Data Labeling Procedures

Develop uniform, simple procedures to label data in files, for softcopies and hardcopies separately. Data is considered labelled if a user can identify the data class of the document, but uniformity is generally preferred. Consider the following when designing such a procedure:

- **Ease of procedures:** Lengthy procedures may result in lower willingness to comply.
- **Ease of Recognition:** The Data Labels should be easily visible to staff, eliminating cases of unknowing incompliance.

Adaptational Tips:

- Ensure that all staff learns the Data Labelling Procedure and the Data Classification Rules. Consider making posters in staff rooms for quick reference.
- DLP solutions may provide automatic classification functionalities. Consult IT to be mindful of the alignment between the manual and automatic process.

Practical Examples:

- Manually add tags for all files and watermarks to documents. Consider stamping for hardcopies if there is no watermark in the digital copy. For instance, include a tag in front of the document name, i.e., [Confidential] Student_Data.txt.
- Consider developing automation tools, such as a tool to label every document as confidential in the same folder.

2.3. Data Labeling Audits

Regularly review data and their labels to detect misalignment of the labelling and Data.

Practical Examples:

- Tools like Data Discovery Scanners will help locate sensitive data and thus provide a quick checklist of data that needs to be labelled confidential. Read their data tags to check for misalignment.

3. Establishing a Data Handling Guideline

This section provides example controls for the three data labels mentioned above. Use these recommendations as a foundation and adjust them to suit your school's use cases, user groups, and available resources.

3.1. Secure Data Transmission

- **Encrypt when Sharing:** Password encrypt all files labelled as confidential when sending to others, and send the password in a separately.
- **Restrict receivers:** Data marked as confidential should not be uploaded into any third party servers, including Generative AI services.

Adaptation Tips:

- DLP solutions may provide real time monitoring functionalities and may act as technical controls.
- Operationalize with simple processes that don't require specialized tools, by setting secure default configurations when sharing sensitive data through file permissions settings, including default link expiry dates within 24 hours of sharing, mandating view-only permissions by organization members when handling confidential files
- Share a simple-to-follow one-pager checklist for staff to securely share confidential documents and data, ensuring compliance with secure data transmission practices

3.2. Secure Data Storage

- **Limit Data Exposure:** Avoid storing confidential data in personal or unapproved devices unless authorized and encrypted. Remove confidential data from devices as soon as it is not needed.
- **Encrypt Data at Rest:** Use state of the art encryption schemes to encrypt sensitive data at rest on top of full disk encryption.

Practical Examples:

- Use Bitlocker for school devices.
- Encrypt any backups with AES256-CBC mode with a key generated from a secure password. For break-glass purpose, write the password down on a piece of paper, and place it in a safe in a physically controlled area.

4. Establishing a Data Lifecyle and Deletion Policy

Data Lifecycle Policies define for how long a specific type of data should be kept and deleted afterwards to minimize exposure.

4.1. Data Retention Rules

Document the categories of data the school contains. For each category define the period of retention based on the use cases or any compliance requirements. Data categories could include but not limited to:

- Student Data (Demographics, Academic Performance, Medical Records, etc)
- School Process Data (Events and Examination Schedules, Departmental Meetings, Meeting Minutes, etc)
- Teaching Materials
- Communication Records (Announcements and communications issued to students and staff, other exchanges among third parties including government departments, school organizations, etc.)

Adaptation Tips:

- Should there be too much data for manual review, such as the lack of technical controls, focus on documents with PII.
- The retention period can be conditional based instead of a static timeframe, e.g, 3 months after a student/staff member leaves the school, 1 year after a supplier agreement has terminated/run out, 1 year of records after asset disposal, etc.

Practical Examples:

- Use programs such as Microsoft Purview that keeps track of the last accessed time of a document and alerts/deletes data.

4.2. Deleting Data

Follow the table from section 6.3.5 Information Security in Schools - Recommended Practice (September 2019).

Media Types	**Reuse (including transfer for reuse)**	**Disposal (including trade-in, and replacement of faulty media)**
Non-volatile magnetic media such as hard disk drives, floppy disks, tapes, etc.	Overwriting	Overwriting or Degaussing or Physical Destruction
Non-volatile solid-state memory such as USB flash drives, memory cards, solid state disks (SSD), etc.	Overwriting	Overwriting or Physical Destruction
Optical media - write once such as CDs, DVDs, Blu-ray discs, etc.	N/A	Physical Destruction
Optical media - write many such as CDs, DVDs, Blu-ray discs, etc.	Overwriting	Physical Destruction
Smart devices such as PDAs, mobile phones, tablets, etc.	Overwriting	Overwriting or Degaussing or Physical Destruction

Practical Examples:

- Use programs such as sdelete in windows to securely delete files by overwriting.
- Consider using forensic tools such as autopsy to check for data traces before reuse.

5. Review and Improvement

5.1. Regular Policy Review

Set a reminder to review your school's data handling and labelling standards at least once a year, or whenever there are changes to your IT systems. Involve both IT staff and teaching/administrative colleagues to gather helpful feedback.

5.2. Adapting to New Threats and Technologies

Stay updated about new cyber threats that can affect schools, such as phishing scams or password leaks. Also, be aware of new technology or software updates that might offer better ways to protect passwords, e.g. two-factor authentication.

5.3. Making Improvements

After each review, update your password policy as needed. Communicate any changes clearly to staff and students, and provide simple instructions or workshops to help everyone follow the new rules.

Appendices

Glossary of Terms

Term	Definition
Access Control	Processes and technologies used to restrict access to IT systems, data, or locations to authorized users only.
AI (Artificial Intelligence)	Computer systems or software that can perform tasks usually requiring human intelligence, such as learning or problem-solving.
Asset	Any device, software, data, or system owned or managed by the school, including hardware, software, and cloud services.
Backup	A copy of data stored separately to enable recovery in case of loss or corruption.
BYOD (Bring Your Own Device)	The use of personally owned devices (e.g., laptops, smartphones) for school activities or accessing school systems.
Cloud Service	An online service (e.g., storage, application, platform) hosted by a third party and accessed via the Internet.
Confidential Data	Information that must be protected from unauthorized access, such as student records or personal data.
Cybersecurity Incident	Any attempted or actual unauthorized access, use, disclosure, disruption, modification, or destruction of information or IT systems.
Data Encryption	The process of converting data into a coded form to prevent unauthorized access.
Data Loss Prevention (DLP)	Tools or processes designed to prevent the unauthorized sharing or loss of sensitive information.
Data Protection	Measures taken to secure personal, sensitive, or confidential information from unauthorized access, disclosure, alteration, or destruction.
Endpoint	Any device (e.g., computer, tablet, smartphone) that connects to the school network.
Firewall	A security system (hardware or software) that monitors and controls incoming and outgoing network traffic based on predetermined rules.
Incident	Any event that could compromise the confidentiality, integrity, or availability of school information or systems.
IT Coordinator	The person or role responsible for overseeing the school's IT systems, security, and compliance.
Log	A record of events, such as system access or data changes, used for monitoring and accountability.
Mobile Device Management (MDM)	Tools or processes used to monitor, manage, and secure mobile devices used in school operations.
Multi-Factor Authentication (MFA)	A security process that requires users to provide two or more independent credentials to verify their identity.
Network Segmentation	The division of a computer network into sub-networks to improve security and performance.
Patch Management	The process of keeping software up to date by applying fixes (patches) to address vulnerabilities or bugs.

Term	Definition
Personal Data/Personally Identifiable Information (PII)	Any information relating to an identified or identifiable individual, such as name, ID number, or contact details.
Physical Access Control	Measures used to restrict entry to buildings, rooms, or other sensitive areas.
Privilege/Privileged Access	Higher-level system access granted to users who need to perform administrative or sensitive tasks.
Ransomware	Malicious software that locks or encrypts a victim's data and demands payment for its release.
Remote Access	The ability to access school IT systems or data from outside the school's physical premises, typically via VPN or secure connections.
Sensitive Data	Data that, if disclosed, could harm individuals or the school, such as health records or disciplinary reports.
Supplier	Any third-party vendor or service provider that supplies goods or services to the school, especially those with access to data or systems.
User	Any staff, student, or other person authorized to use school IT resources.
Vulnerability	A weakness in a system, software, or process that could be exploited to compromise security.
Wireless Security	Controls and practices implemented to protect wireless (Wi-Fi) networks from unauthorized access or attacks.

End of Document

Practical Guide to Email Security

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for email security in schools across Hong Kong. Its aim is to help educational institutions establish secure, consistent, and effective email management practices that reduce the risk of compromise of school systems and sensitive information.

The scope of this guide includes spam and phishing protection measures, mail server management, technical controls for cloud-managed mail services, and user support for reporting and acting upon suspicious emails. It is designed to be adaptable for different school sizes, system types, and available resources.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Enforce stringent email security practices across the school, both when managing incoming and outgoing emails.
- Enable scam and phishing protection measures.
- Maintain security and protection for mail servers, including those hosted on the cloud as well as self-hosted email servers.
- Share common practices and safe procedures for handling emails securely, providing information and training on spotting and acting against suspicious emails.

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Suggestions for IT

General Suggestions

2.1. Concealing Email Addresses

The email address is also part of the password verification. Concealing email addresses means it will be harder for attackers to get hold of login credentials.

- Configure role-based aliases for external emails to minimize personal address exposure.
- Assign complex, non-predictable email names.

Practical Examples:

- Set up role-based aliases, for example “External Communications” that teachers can use instead of their own email when replying to external emails.
- Consider using combinations other than trivial last name first name combinations, e.g., “axc362@mail.com” rather than “alice.chan@mail.com”

2.2. Scam and Phishing Protection

- Prepare training materials on spotting and reporting phishing attempts, and procedures for phishing reports.
- Explore open-source phishing detection/analysis software and configure server filters for scam patterns (e.g., urgent keywords).

Adaptational Tips:

- Consider taking reference from Section 3 when working on training materials.
- Make the phishing report procedure as simple as possible.
- Open-source phishing and spam detection will provide technical controls worth exploring rather than solely relying on end user reports.

Practical Examples:

- Open-source suggestions: Apache SpamAssassin for filtering, ThePhish for automated phishing report analysis.

Suggestions for On-Premises Mail Servers

This section outlines processes to secure an on-premises mail server. Use these recommendations as a foundation and adjust them to suit your school's needs and restrictions.

2.3. Mail Server Protection

The first step to protecting emails is to protect the mail server itself. Below are generic suggestions on how to reduce the attack surface of an on-premises mail server.

- Deploy firewalls to restrict SMTP traffic to trusted School IPs.
- Configure servers to strip internal network details from response headers.
- Perform due diligence for updates/patches. See Guide for Maintenance & Patch Management for more details.

Adaptational Tips:

- If external access is required, use a VPN and whitelist the IP range of the VPN in the firewall.
- If there are use cases in which IP whitelisting is not feasible, consider using blacklists to ban access based on regions.

Practical Examples:

- Blacklist IPs from regions the school has no interactions with, for example North Korea and Iran.

2.4. Anti-Bombing/Spamming Measures

This section suggests measures that aims to detect and filter unwanted email activities, including spam, bombing and malicious emails (e.g., viruses).

- Implement logging/intrusion detection to auto-ban suspicious IPs and set up mobile alerts for such events.
- Restrict relaying for authenticated users only.
- Enforce size and rate limits to prevent resource drain.

- Deploy virus scans for attachments and quarantine emails when flagged positive.

Adaptational Tips:

- Be mindful of traffic patterns when setting thresholds, for there may be email surges during periods such as enrolment periods or events.
- Consider integrating to any existing IT dashboards.

Practical Examples:

- Use tools like Fail2Ban for intrusion detection and banning IP addresses.
- Use a lower threshold during 12nn-6am, when large traffic is not expected because end users should be asleep.

Suggestions for Cloud Mail Services

This section outlines processes to secure emails on a Cloud Mail Service. (e.g., Outlook, Gmail). Use these recommendations as a foundation and adjust them to suit your school's needs and restrictions.

2.5. Anti-Bombing/Spamming Measures (Cloud)

Most Cloud Mail Services have spam filters implemented by default and will allow configurations via admin panel. Check for the following settings:

- Configure logging for anomaly detection.
- Enable sender verification in settings.
- Set size and rate limits with policies.

Adaptational Tips:

- Most of the Cloud Mail Providers has built-in spam/phishing/virus detection.
- Consider checking for APIs that allow logs to be exported to a local machine such that third-party anomaly detections systems can be used.

3. Suggestions for End Users

End Users, including teachers and students should consider the following items to minimize the effectiveness of the email attack vector. Use this guide as a reference for making training materials, or as a template for internal guidelines for all teachers.

3.1. Safe Email Handling

General Precautions

- **Verify Sender Identity**: Always check the sender's email address for authenticity. Spoofed addresses may appear legitimate but contain subtle discrepancies (e.g., unusual domains). If in doubt, give the sender a call according to your own contacts.
- **Avoid Opening Emails from Unknown Senders**: Do not open or respond to unsolicited emails. Mark them as spam to improve filtering.
- **Exercise Caution with Links**: Hover over hyperlinks to inspect the destination URL before clicking. Avoid clicking if the URL seems suspicious or mismatched.
- **Limit Email Address Exposure**: Restrict email to professional use. Avoid using the school email to sign up for any personal service/accounts (e.g., News subscriptions), and avoid posting the email address online (e.g., blogs).

Handling Attachments

- **Download Attachments Only from Trusted Sources**: Restrict downloads to known contacts or verified organizations. Scan all attachments with up-to-date antivirus software before opening.
- **Manage Encrypted Attachments Securely**: Refrain from decrypting attachments if the password is provided in the same email or if the source is unknown. Request the password via an out-of-band channel (e.g., phone call or secure messaging app) to confirm legitimacy.

Responding to Suspicious Activity

- **Delete and Report Suspicious Emails**: Immediately delete emails that appear fraudulent, contain urgent demands, or request sensitive information. Report them to your IT department or email provider for investigation.
- **Do Not Share Sensitive Information**: Never provide personal, financial, or login details in response to an email, even if it claims to be from a trusted entity. Verify requests through official or out-of-band channels (e.g., phone call or secure messaging app).

Adaptational Tips:

- Make the designated reporting channels known to teachers and remind them constantly.
- Consider making posters to give constant reminders to teachers.

3.2. Common Signs of Suspicious Emails

Sender and Header Anomalies

- **Spoofed or Mismatched Sender Address:** The email appears to come from a trusted entity (e.g., a bank or colleague), but the actual address is unfamiliar or contains slight variations (e.g., "support@bankk.com" instead of "support@bank.com").
- **Unexpected or Unsolicited Origin:** Emails from unknown senders or organizations you have no prior relationship with, especially those claiming urgency.

Content and Language Indicators

- **Urgent or Threatening Language:** Phrases demanding immediate action, such as "Your account will be suspended" or "Click now to avoid penalties," to create panic and bypass critical thinking.
- **Requests for Sensitive Information:** Demands for passwords, financial details, or personal data, often under the guise of verification or updates. Legitimate organizations rarely request such information via email.
- **Poor Grammar, Spelling, or Formatting:** Errors, awkward phrasing, or inconsistent branding (e.g., mismatched logos or fonts) that deviate from professional standards.
- **Generic or Impersonal Greetings:** Use of "Dear User" or "Valued Customer" instead of your name, indicating a mass-distributed scam.

Links and Attachments

- **Suspicious Hyperlinks:** Links that do not match the displayed text (e.g., hovering reveals a different URL), lead to unfamiliar domains, or includes variations of familiar domains (e.g., www.gmaiI.com instead of gmail.com).
- **Unexpected Attachments:** Files from unknown sources and with unusual extensions (e.g., .exe, .zip), may contain malware. Encrypted attachments with passwords in the same email are especially suspicious in this regard.

Other Red Flags

- **Promises of Rewards or Prizes:** Offers of money, gifts, or opportunities that seem too good to be true, often requiring clicks or data submission.
- **Inconsistencies in Context:** Emails referencing uninitiated transactions, unknown accounts, or events you did not participate in.

Glossary of Terms

Term	Definition
On-premises mail server	A school-managed email server hosted on the school's own network or data center rather than in a public cloud.
Cloud mail service	An email platform hosted and managed by a cloud provider (e.g., Microsoft 365, Google Workspace) and administered via a web console.
Role-based alias	An address representing a function or team (e.g., admissions@) used to reduce exposure of personal addresses and ease handover.
Non-predictable email address format	A naming convention that avoids easily guessed patterns (e.g., random strings instead of firstname.lastname) to hinder account guessing.
Phishing	A social-engineering email attack attempting to trick recipients into revealing credentials, data, or executing harmful actions.
Email scam	A fraudulent message (e.g., urgent payment, gift-card requests, VIP impersonation) seeking financial gain or data theft.
Spam	Unsolicited or bulk email that clutters inboxes and may contain malicious links or attachments.
Mail bombing	A denial-of-service tactic sending very high volumes of email to overwhelm a mailbox or server.
Sender spoofing	Forging the "From" address or display name so a message appears to come from a trusted sender.
Sender verification	Technical/policy checks to confirm a sender is legitimate, reducing spoofing and impersonation.
Quarantine	A holding area where suspicious emails are isolated for review before release to inboxes.
Attachment malware scanning	Automated analysis of attached files to detect and block malicious code.
Link protection / URL rewriting	A control that scans and rewrites links so destinations are checked at click time to block malicious sites.
Anomaly detection	Monitoring for unusual email or login patterns (e.g., spikes, atypical IPs) that may indicate abuse or compromise.
Firewall	A device/service that filters network traffic by rule, used to restrict SMTP and protect mail systems.
SMTP (Simple Mail Transfer Protocol)	The protocol used for transmitting email between servers and from clients to servers.
IP allowlist (whitelist)	A list of trusted IP addresses permitted to access a service; all others are blocked by default.
IP blocklist (denylist)	A list of IP addresses explicitly blocked due to abuse, threats, or policy violations.
Rate/size limiting	Controls that cap message volume or size over time to prevent resource exhaustion and mailbox bombing.

Fail2Ban	An open-source tool that parses logs and automatically blocks IPs after repeated suspicious activity.
Apache SpamAssassin	An open-source email filtering framework that scores messages for spam indicators and enables filtering actions.
ThePhish	An open-source tool that analyzes reported phishing emails to help triage and classify them automatically.
Sandbox / isolated environment	A controlled VM/container used to open or analyze risky files without endangering production systems.
Header sanitation	Configuration that removes internal routing/system details from outgoing email headers to avoid leaking network information.
Out-of-band verification	Confirmation of a request using a separate trusted channel (e.g., phone call) to reduce phishing risk.
TLS (Transport Layer Security)	Encryption protocol protecting data in transit between email clients/servers when supported and enforced.
Authenticated relay restriction	A rule that permits email relaying only for authenticated users, preventing open-relay abuse.
Admin console / dashboard	The management interface for configuring mail security settings, policies, logs, and alerts.
Phishing simulation	A controlled campaign that sends realistic test emails to train users to recognize and report suspicious messages.
Public Wi-Fi caution	User guidance to avoid accessing sensitive data over open hotspots unless protected (e.g., via VPN or pre-encrypted files).

End of Document

Practical Guide to Mobile Device Management

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for mobile device management in schools across Hong Kong. Its aim is to help educational institutions implement secure management practices that protect mobile devices used at school environments and for educational/administrative purposes for the school.

The scope of this guide covers both cases where the school may/may not have access to a mobile device management (MDM) solution, providing technical controls and guidance on acceptable use for the use of mobile devices. There are also sections on implementing alternative technical controls in the case where an MDM solution is not currently in-use at the school, as well as the best practices to integrate these controls with other security measures – to be read in tandem with other practical guides provided. These guidelines have been derived from various accredited sources, including the Education Bureau of Hong Kong (EDB) as well as the Centre for Internet Security, both of whom have provided guidance and resources that are used to form the basis of these guides.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Implement technical controls on mobile devices through MDM solutions
- Formulate an Acceptable Use Policy that guides the use of mobile devices on school environments
- Support MDM solutions by integrating relevant controls with other procedures
- Administer alternative solutions for mobile device management in the case that no MDM tools are readily available
- Create Bring Your Own Device (BYOD) policies that govern the network segregation of devices
- Log a functional inventory of BYOD devices, along with approval and review policies

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Control Suggestions for School Managed Devices

This section explains how a school would be able to effectively manage the security of shared School-Managed Devices (e.g., student tablets/laptops). This section assumes that the devices are of school property and toward which the school has total control.

N.B.: MDM Enrolment

We highly encourage schools to consider free or low-cost MDM solutions specifically designed for education. MDM provides technical control as an alternative to labor-intensive policy controls, saving a lot of human resources. Some MDM providers offer heavily discounted pricing for schools.

The following sections of the guide will be split into two different scenarios; the first section will cover the use of MDM solution, and the other will cover controls that can be implemented in the absence of an MDM solution.

If MDM Solution is Available

2.1. Technical Controls via MDM Solutions

This section lists the recommended controls that a school can implement for their shared devices with MDM.

2.1.1. Password Policy Enforcement

Enforce passcode policies through the MDM.
For details about the password policy, reference the Security Configuration Checklist.

2.1.2. Application Management

Establish a clear list on allowed and prohibited applications.

Configure the MDM to whitelist or blacklist applications according needs (blacklist if whitelisting is too restrictive)

Adaptational Tips:

- Review the application list and the corresponding MDM control regularly (e.g., annually) such that the list remains appropriate for the requirements

2.1.3. Content Filtering

Configure the MDM to enforce content filtering policies.

Practical Examples:

- Use a whitelist for all the approved education resources. If this proves to be too restrictive, GitHub has a lot of community-maintained domain blacklists for harmful content.

2.1.4. Device Encryption

Enable device encryption via MDM during device setup.

Adaptational Tips:

- Be mindful of the encryption scheme the MDM software is using. Weak ciphers such as DES and 3DES, and Weak Block Cipher Modes such as ECB should be avoided.

2.1.5. Remote Wipe

Implement remote wipe capabilities via MDM in case of device being stolen or lost.

Adaptational Tips:

- Perform tests on the remote wipe functionality before deployment.
- Understand the limitations of the remote wipe function: Some implementations require internet connection of the stolen device.

2.1.6. Regular Updates

Enable device encryption via MDM during device setup.

Adaptational Tips:

- Be mindful of the encryption scheme the MDM software is using. Weak ciphers such as DES and 3DES, and Weak Block Cipher Modes such as ECB should be avoided.

2.1.7. Post Device Use

Wipe the device with the MDM solution when repurposing the device (e.g., assigning to another student). Some MDMs would allow automating data wipe and re-enabling all security controls.

Adaptational Tips:

- Follow proper procedures documented in Practical Guide to Data Handling when repurposing the device.

2.2. Acceptable Use Policy Addendum

MDM solutions may collect user activity for anomaly detection. It is important that the users are informed before device use. The below describes the clauses to add to the Acceptable Use Policy of School Devices if any data is collected by the MDM solution.

- **User Activity Monitoring:** Inform end users about the fact that device activity is monitored.
- **Data Collection and Usage Declaration:** List out the usage data that the MDM solution will collect for monitoring purposes, and state that by agreeing to the Acceptable Use Policy the end user accepts the collection of such data. Common data MDM solutions collect include:
  - **App usage and activities**: Tracking which applications are installed, used, and how much time or data they consume, including blacklisted or unauthorized apps.
  - **Network and data usage**: Monitoring network status, traffic consumption by apps, and overall data patterns to detect anomalies or excessive use.
  - **Location and movement**: Real-time location tracking and geofencing to monitor where devices (and by extension, users) are, often triggering alerts for unauthorized areas.

- **User logs and behavior patterns**: Recording user actions, session logs, and behavioral anomalies, such as attempts to access restricted resources or suspicious activities like unauthorized network access.
- **Compliance and policy violations**: Monitoring adherence to organizational policies, including security settings, software updates, and potential threats from user actions like jailbreaking or non-compliant configurations.
- **Device usage patterns**: Overall patterns of how the device is used, including battery life, storage, and session durations, which can indirectly reflect user habits.

Adaptational Tips:

- Data collected will differ between different MDM solutions. Please adjust the items when drafting the Acceptable Use Policy.

If MDM Solution is Not Available

This section lists the alternative controls that a school can consider implementing without the need of an MDM solution, aside on relying on the Acceptable Use Policy. We will first introduce technical controls and then provide an Acceptable Use Policy as a fallback.

2.3. Alternative Technical Controls Without MDM Solutions

In the absence of Mobile Device Management (MDM) solutions, alternative technical controls can be implemented. Scalability, however, remains a key consideration. While we can leverage Active Directory Group Policies to enforce controls centrally, controls must be applied individually and locally on each standalone or non-domain device.

Adaptational Tips:

- To streamline deployment on standalone devices, configure a single device with the desired settings to serve as a "golden image," which can then be cloned across other similar devices. Note that different sets of controls will require separate golden images.
- Regardless of the approach, always restrict end-user access to administrative privileges to maintain security and prevent unauthorized changes.

2.3.1. Password Policy Enforcement

- **Domain-Joined Windows Devices:** Set Default Domain Policy for establishing the Password Policy. To apply different rules for younger students, use Fine-Grained Password Policies for younger student groups.
- **Standalone Windows Devices:** Set up Password Policy with the Local Security Policy editor.
- **MacOS:** Use Apple Configurator to create .mobileconfig files which define password rules. Transfer and install them during initial setup of the device.

For details about the password policy, reference the Security Configuration Checklist.

2.3.2. Application Management

Establish a clear list on allowed and prohibited applications.

Different Operating Systems have built-in tools for blacklisting and whitelist applications. This includes AppLocker on Windows and Apple Configurator on MacOS.

Adaptational Tips:

- AppLocker rules are based on publisher, path, or hash for specific executables. These may proof challenging for making an exhaustive blacklist. Whitelists are therefore recommended.
- Apple Configurator identifies applications by their bundleID, making blacklists more powerful.

2.3.3. Content Filtering

Implement network-wide content filtering (e.g., DNS proxies and firewall rules) in school premises.

Practical Examples:

- Use a whitelist for all the approved education resources. If this proves to be too restrictive, GitHub has a lot of community-maintained domain blacklists for harmful content.
- Consider OpenDNS or Pi-Hole as the main free options.

2.3.4. Device Encryption

Modern Android and iOS devices encrypt system files as long as there is a password set.

For Windows and MacOS laptops, deploy controls to enforce Bitlocker and FileVault implementation.

- **Domain-Joined Windows Devices:** Create Group Policy for Bitlocker Drive Encryption.
- **Standalone Windows and MacOS Devices:** Configure the encryption one by one. Since this is about full disk encryption with TPM integration, Direct cloning will cause caveats. Consider using automated scripts on an USB to ease the process.

2.3.5. After Use Device Wipe

Manually wipe the devices when repurposing them. Follow Practical Guide to Data Handling for more details.

2.4. Integration with Other Procedures

- Follow Practical Guide for Asset Management for guides for guidance on distributing devices.
- Follow Practical Guide for Physical Security for guidance on Secure Storage of School-owned devices.

3. Suggestions on Handling Bring-your-own-device (BYOD) Devices

Adaptation of BYOD devices pose a unique security threat to schools, for essentially it means allowing external devices to access school resources. Deploying MDM solutions on teacher and student devices will be unfeasible, and few policies will be effective due to lack of willingness to comply.

3.1. Network Segregation and Setup

Treat all BYOD Devices as external. Provide internet access via access points that are either physically or logically segregated from the school infrastructure.

Ensure that the passwords of the access points are secure. Refer to the Security Checklist for definitions of a strong password.

Ensure that the protocols of the school's access points are up to date, e.g., use access points that support WPA3.

If there is a need for access to internal network, consider requiring a certificate to connect to the access point, or consider if an access point is needed to begin with.

Adaptational Tips:

- For groups that need access to internal data with their BYOD devices, make a standalone access point for each group, which are separated from each other and to the internal networks logically (e.g., firewall/gateway). Access controls can then be implemented.

Practical Examples:

- Assuming the teachers do not need access to internal servers with their BYOD machines, use 2 separate internet service providers for internal internet access and BYOD/Guest internet access and ensure no physical links between the subnets are present.
- Assuming that the teachers need access to internal resources, but students do not. Make in total of 3 subnets – Internal network, Teacher BYOD and Student BYOD. Segregate Teacher BYOD and internal network with a gateway/firewall, and use another internet service provider for Student BYOD.

3.2. BYOD Inventory and Approval

Establish an approval process for each BYOD Device that has to connect to the internal network.

BYOD Inventory

Maintain a detailed inventory of all BYOD devices that has been allowed access to internal resources, including user information, device details, and a list of installed applications, date of approval.

Approval

Approval of access should be done by IT, which should assess if the device is compliant by checking the device against the technical controls of the AUP.

If the device is compliant, the IT could grant access to the resources the end user needs after the they sign the Acceptable Use Policy for BYOD Devices.

Practical Examples:

- After end user signs the Acceptable Use Policy, grant access by setting firewall rules based on mac addresses.
- When granting access, grant the only necessary access they need.

3.3. BYOD Inventory Review

Conduct regular (e.g., yearly) reviews on the BYOD Inventory list on the needs of access. Revoke Access if the user does not need access anymore.

Appendix

Glossary of Terms

Term	Definition
School-Managed Devices	Devices owned and fully controlled by the school (e.g., shared student tablets/laptops) where the school can enforce settings, install software, and restrict use.
Mobile Device Management (MDM)	A platform that centrally enrolls, configures, and manages devices, enforces security policies, deploys apps, monitors compliance, and can locate or wipe devices remotely.
MDM Enrollment	The process of registering a device with the MDM so it can receive and enforce school policies and configurations.
Acceptable Use Policy (AUP)	A set of rules that defines acceptable and unacceptable behavior when using school devices, networks, and data.
User Activity Monitoring	The collection and review of device/user activity (e.g., app use, network use, location) to detect misuse, policy violations, or security issues.
Data Collection and Usage Declaration	A statement in the AUP explaining what data the MDM collects, why it is collected, and how it will be used.
Anomaly Detection	The identification of unusual patterns in device or user behavior that may indicate misuse, compromise, or policy violations.
Geofencing	A location-based control that uses virtual boundaries to trigger actions or alerts when a device enters or leaves defined areas.
Usage Logs	Time-stamped records of device and user actions (e.g., logins, app launches, network connections) used for monitoring and investigation.
Compliance Monitoring	Checking devices against required security settings and policies to ensure they remain compliant.
Policy Violation	Any instance where a user or device fails to follow defined school policies or security requirements.
Remote Wipe	A command sent to a device to erase data and restore it to a factory or baseline state, typically used if a device is lost or stolen.
Device Encryption	The process of protecting stored data on a device by converting it into unreadable form unless the correct key or password is provided.
Full Disk Encryption (FDE)	Encryption that protects the entire storage drive, ensuring data remains unreadable if the device is lost or stolen.
BitLocker	Microsoft Windows full disk encryption technology that protects data at rest, often using a TPM.
FileVault	Apple macOS full disk encryption technology that protects data at rest.
Trusted Platform Module (TPM)	A hardware chip that securely stores cryptographic keys and supports device integrity checks and disk encryption.
Password Policy	Rules for creating, changing, and managing passwords (e.g., length, complexity, lockout).

Strong Password	A password that meets or exceeds policy (e.g., long, unique, and hard to guess) to resist brute-force and guessing attacks.
Fine-Grained Password Policies	Active Directory feature allowing different password rules for different user groups (e.g., younger students vs. staff).
Default Domain Policy	The baseline Group Policy Object linked to the domain that typically defines organization-wide settings such as password policy.
Local Security Policy	Windows local configuration (secpol.msc) used to enforce security settings on standalone (non-domain) devices.
Apple Configurator	Apple tool used to create and deploy configuration profiles, supervise devices, and install apps on iOS/iPadOS/macOS devices.
.mobileconfig	Apple configuration profile file used to apply settings (e.g., passcode rules, Wi-Fi) to Apple devices.
Application Management	The control of which applications can be installed or run, and how apps are deployed and updated on devices.
Whitelisting (Allowlisting)	A control approach that permits only approved apps, websites, or domains; everything else is blocked by default.
Blacklisting (Blocklisting)	A control approach that blocks specific apps, websites, or domains while allowing other items by default.
AppLocker	A Windows feature that restricts which executables, scripts, and packaged apps can run based on publisher, path, or hash rules.
BundleID	A unique identifier assigned to an app in Apple ecosystems, used to target or control specific apps.
Content Filtering	Controls that restrict access to web content or domains based on categories, whitelists, or blacklists.
DNS Filtering	Filtering web access by controlling DNS queries to block or allow specific domains before connections are made.
OpenDNS	A cloud-based DNS service (Cisco) that can provide category-based web filtering and security protections.
Pi-hole	An open-source DNS sinkhole that blocks ads and trackers and can be used for basic domain-level content filtering on a network.
Golden Image	A standardized, pre-configured system image used to clone consistent settings and software to many devices.
Cloning (Disk Imaging)	Creating and deploying an image of a configured device to other devices to speed setup and ensure consistency.
Domain-Joined Device	A computer connected to an Active Directory domain, allowing centralized authentication and policy enforcement.
Standalone Device	A device not joined to a domain; managed locally on the device itself.
Active Directory (AD)	Microsoft directory service for managing users, groups, devices, authentication, and policies across an organization.
Group Policy (GPO)	Active Directory mechanism for centrally enforcing configuration and security settings on users and computers.
Network Segregation	The practice of separating networks or user groups into isolated segments to reduce risk and limit access (e.g., internal vs. BYOD).

Subnet	A logical subdivision of a network with its own IP address range, often used to separate traffic and apply different controls.
Firewall	A security device or software that permits or blocks network traffic based on defined rules.
Gateway	A network device (often a router or firewall) that connects different networks and enforces routing and access controls between them.
Access Point (AP)	A device that provides wireless (Wi-Fi) network access to client devices.
WPA3	The current Wi-Fi security protocol that offers stronger encryption and authentication than WPA2.
Certificate-Based Authentication	Using digital certificates to authenticate devices or users to a network or service, often for secure Wi-Fi access.
MAC Address	The unique hardware identifier of a network interface, sometimes used in access control lists or firewall rules.
BYOD (Bring Your Own Device)	A practice allowing users to connect personal devices to school networks or resources under defined conditions.
BYOD Inventory	A record of approved personal devices allowed to access internal resources, including owner, device details, apps, and approval dates.
Approval Process	The steps and criteria used by IT to review, authorize, and grant device access to specific resources.
Compliance Check	The assessment of a device against required technical controls and AUP criteria before granting or retaining access.
Post-Use Device Wipe	The process of erasing user data and restoring the baseline configuration before reassigning a device to another user.
Secure Disposal/Wipe	Permanently erasing data so it cannot be recovered when repurposing or retiring a device.
Practical Guide to Data Handling	An internal reference document that defines procedures for secure data handling, wiping, and repurposing of devices.
Practical Guide for Asset Management	An internal reference for distributing, tracking, and maintaining school-owned devices.
Practical Guide for Physical Security	An internal reference for physically securing devices (e.g., storage, access control).
Cryptographic Cipher	An algorithm used to encrypt and decrypt data; its strength affects overall security.
DES	A legacy symmetric cipher now considered insecure and not suitable for protecting modern data.
3DES	A legacy cipher that applies DES three times; now considered weak and being phased out.
ECB (Electronic Codebook)	An insecure block cipher mode that reveals patterns in data and should be avoided.
Content Whitelist	A list of approved websites or domains that users are allowed to access; all others are blocked.
Domain Blacklist	A list of forbidden websites or domains that users are not allowed to access; others remain allowed.
DNS Proxy	A server or service that forwards DNS queries on behalf of clients and can enforce filtering and logging policies.

Internet Service Provider (ISP)	A company that provides Internet connectivity; separate ISPs can be used to isolate internal and BYOD/guest networks.
Jailbreaking	The act of removing manufacturer or OS restrictions on a device (e.g., iOS), allowing unauthorized apps or settings and weakening security.
Non-Compliant Configuration	A device state that does not meet required security policies (e.g., outdated OS, disabled encryption, or prohibited apps).

School-owned Devices Acceptable Use Policy Template

Acceptable Use Policy (AUP) for School-Owned Devices

Introduction

This Acceptable Use Policy (AUP) outlines the guidelines for using school-owned devices, such as laptops and tablets, for educational purposes. These devices are provided to support learning, teaching, and school-related activities for both students and teachers. All users must use these devices responsibly to protect school data, ensure security, and comply with legal and ethical standards. By using a school-owned device, you agree to follow all rules outlined in this policy. Violations may result in disciplinary action, such as loss of device privileges, detention (for students), or further consequences as determined by school administration.

This policy covers key areas of device usage, security, and maintenance. All users are expected to review and adhere to these guidelines.

Safe Wi-Fi Usage

To protect school information and personal data, it is crucial to connect to secure networks.

- Connect only to secure, school-provided Wi-Fi networks when accessing important school information, such as student records or grades. These networks are designed to keep your information private and safe.
- Avoid using public Wi-Fi hotspots (like those at cafes or malls) for school-related work unless you are using a school-approved Virtual Private Network (VPN). Public networks are often not secure and can expose your information to risks.
- If you are unsure whether a Wi-Fi network is safe or legitimate, please ask the school's IT staff for verification.

Secure Data Processing

Handling school data securely is essential to maintain privacy and prevent unauthorized access.

- Use only applications or platforms approved by the school for managing sensitive information (e.g., student IDs, personal details). These approved tools, such as secure cloud storage, are equipped with end-to-end encryption to protect your data.
- Never enter sensitive information on applications or websites that are not encrypted or approved by the school. Look for "https://" in the website address, which indicates a secure connection.
- If you have any doubts about the security of an application or website connection, please consult the school's IT staff.

Data Backup and Synchronization

Regularly backing up your schoolwork helps prevent loss and ensures your progress is saved.

- Use school-provided tools like Google Drive or OneDrive for saving and syncing all your educational files. Ensure that encryption features are enabled as instructed by the school.
- Regularly save your work to the school-approved cloud storage. This practice is vital to prevent losing your assignments and projects.
- Confirm with the IT staff that your backup settings meet the school's security and encryption requirements.

Device Storage

- Store your device in secure locations when it is not in use, such as in a locked cabinet or your school bag. This is especially important when you are outside school property.
- Avoid leaving devices unattended in public or unsecured areas.

Adherence to Login and Password Policy

Following login and security protocols protects your device, account and the school's network.

- Create and maintain strong passwords as required by the IT department. A strong password is <Reference the Security Configure Checklist>. Never share your passwords with anyone.
- Report any issues with your login or auto-lock settings to the IT staff promptly. This ensures your device remains secure.

Password Management

- Do not save passwords for your school email, network logins, or other accounts directly on the device.
- Disable auto-save password features in web browsers or applications when you first set up your device.
- Memorize your passwords or use a school-approved password manager if available.

Device Return and Data Erasure

- Return devices to the IT staff for data erasure before they are disposed of or given to another student. Do not attempt to erase data from the device yourself.

Inventory Reporting

- Report any changes in your device's status immediately to the IT staff, such as if it is lost, damaged, or reassigned to someone else. This helps the school keep accurate inventory records.

General Usage Guidelines

In addition to the security-focused rules above, the following guidelines ensure responsible and effective use of school-owned devices for both students and teachers:

- **Permitted Use**: Devices are intended for school-related activities, including classwork, homework, lesson planning, grading, research, and professional development. Limited personal use (e.g., checking weather or educational apps) is allowed, provided it does not interfere with school responsibilities or violate this policy.
- **Prohibited Activities**:
    - Installing unauthorized software, apps, or extensions without IT approval, as this may introduce security risks or violate licensing agreements.
    - Accessing, downloading, or distributing inappropriate, illegal, or copyrighted materials, including but not limited to content that is violent, discriminatory, or sexually explicit.
    - Using devices for gaming, social media (unless school-approved for educational purposes), or any activity that distracts from learning or teaching.
    - Modifying device settings, hardware, or software beyond what is explicitly allowed by IT.
    - Bullying, harassing, or sending inappropriate messages via school devices or accounts.
- **Internet and Email Usage**: All internet and email activity on school devices is monitored and logged for security and compliance purposes. Use school email for educational communications only. Respect intellectual property rights and avoid sharing confidential information via unsecured channels.
- **Physical Care and Maintenance**: Handle devices with care to avoid damage. Report any hardware issues (e.g., cracked screens, battery problems) to IT immediately. Do not attempt repairs yourself.
- **Remote Access and Off-Site Use**: When using devices outside school (e.g., at home), ensure they are in a secure environment. Enable all required security features, such as auto-lock after inactivity and full-disk encryption. Students must have parental supervision for home use as appropriate.

- **Monitoring and Privacy**: The school reserves the right to monitor device usage, including files, emails, and browsing history, to ensure compliance. Users have no expectation of privacy on school-owned devices.

Consequences of Violations

Violations of this AUP may result in:

- For students: Loss of device privileges, detention, parental notification, or other school disciplinary measures.
- For teachers: Temporary suspension of device access, required retraining, performance reviews, or other administrative actions up to and including termination.
- Legal action if violations involve illegal activities or data breaches.

The school will investigate all reported violations promptly and fairly.

Acknowledgment of Acceptable Use Policy (AUP)

Understanding and agreeing to the school's rules for device use is a mandatory step.

- Review and sign the acknowledgment form (either a physical paper or a digital form) provided by the IT staff before you begin using the school device. This form confirms your understanding of these guidelines. For students under 18, a parent or guardian must also sign.
- If any part of the Acceptable Use Policy (AUP) or security reminders is unclear, contact the IT staff for clarification.

By signing, you acknowledge that you have read, understood, and agree to comply with this AUP. This policy is subject to updates; users will be notified of changes and required to re-acknowledge as needed.

User Signature: _____ Date: _____

Printed Name: _____ Role (Student/Teacher): _____

Device Assigned: _____

Parent/Guardian Signature (if student under 18): _____ Date: _____

For questions or support, contact the school's IT staff at [insert contact information].

BYOD Devices Acceptable Use Policy Template

Acceptable Use Policy for Bring Your Own Device (BYOD)

Introduction and Purpose

This Acceptable Use Policy (AUP) outlines the guidelines for the use of personal mobile devices (BYOD), such as smartphones, tablets, and laptops, when connecting to the school's network and IT systems. The policy aims to ensure a safe, secure, and productive learning environment while protecting school data, networks, and resources from risks such as unauthorized access, data breaches, malware, and loss of sensitive information.

This policy is developed in reference to the Education Bureau's (EDB) "Information Security in Schools - Recommended Practice (September 2019)," particularly Chapters 5 (Access Control), 7 (Network and Communication Security), and 9 (Mobile Device and Mobile Application Protection). It promotes the principles of least privilege, need-to-know access, and responsible use to comply with relevant laws, including the Personal Data (Privacy) Ordinance.

The school encourages the use of BYOD for educational purposes but reserves the right to restrict or revoke access if the policy is violated.

Scope

This policy applies to:

- All students, staff, and visitors using personal devices to access the school's Wi-Fi network, wired connections, or any school IT resources.
- BYOD includes any personally owned mobile device (e.g., iOS/Android phones/tablets, laptops) capable of connecting to the school network.
- School-owned devices are covered under separate IT policies but must adhere to similar security standards when used alongside BYOD.

Exemptions may be granted for accessibility needs, subject to approval by the IT Head.

Acceptable Use Guidelines

Users may use BYOD for:

- Educational activities, such as accessing learning management systems, school email, or approved online resources.
- Administrative tasks (for staff), including collaboration tools and document sharing.
- Limited personal use during non-instructional time, provided it does not interfere with school activities or violate this policy.

All use must align with the school's mission and values, and users must respect the rights of others (e.g., no harassment, bullying, or infringement of intellectual property).

Prohibited Activities

The following are strictly prohibited on BYOD when connected to the school network:

- Accessing, downloading, or distributing illegal, harmful, or inappropriate content (e.g., pornography, hate speech, copyrighted materials without permission).
- Installing or running unauthorized software, including malware, viruses, or apps from untrusted sources. Only apps from official stores (e.g., Apple App Store, Google Play) or school-approved lists are permitted.
- Sharing school credentials (e.g., usernames, passwords) or using shared/group accounts for BYOD access.
- Jailbreaking/rooting devices or exploiting the operating system.
- Connecting to the school network from untrusted or compromised devices (e.g., without up-to-date security patches).
- Using BYOD for commercial activities, gaming, or streaming media that consume excessive bandwidth.
- Bypassing school security measures, such as using VPNs to circumvent firewalls or accessing restricted sites.
- Unauthorized recording, photographing, or filming of students, staff, or school facilities without consent.

Security Requirements for Devices

To connect to the school network, BYOD must meet the following minimum security standards. The school may use Mobile Device Management (MDM) tools to enforce compliance where feasible:

- **Device Configuration:**
    - Enable a strong lock screen: Minimum 8-character password/PIN with mixed characters (letters, numbers, symbols); auto-lock after 5 minutes of inactivity.
    - Install and maintain up-to-date anti-malware software with real-time scanning.
    - Enable full-device encryption (e.g., FileVault on macOS, BitLocker on Windows, built-in encryption on iOS/Android).
    - Keep the operating system and all apps updated with the latest security patches.

    - Disable auto-save for passwords and do not store school credentials on the device.

- **Network Access:**
    - Connect only via the school's secure Wi-Fi (WPA2/WPA3-Enterprise with authentication). Guest networks are isolated and do not provide access to internal resources.
    - Use school-provided VPN for any access to sensitive internal systems; personal VPNs are not permitted.
    - Avoid connecting to public Wi-Fi while handling school data; if necessary, use cellular data with encryption.
- **Approval and Inventory:**
    - Devices must be registered with the IT department (e.g., via MDM enrollment) and approved before access to internal network is granted.
    - The school will maintain an inventory of connected BYOD, including user details and installed apps.
- **Data Handling:**
    - Minimize storage of sensitive school data (e.g., student records) on personal devices; use school-provided cloud storage with encryption.
    - Enable remote wipe capabilities through MDM for lost/stolen devices.
    - Back up data using encrypted tools; erase all school data before device disposal or reuse.

Users are responsible for physically securing devices (e.g., not leaving them unattended) and reporting loss/theft immediately to the IT Head.

User Responsibilities

- **Monitoring Consent:** Users acknowledge that the school may monitor network traffic, device logs, and activities for security purposes (e.g., detecting unauthorized access or malware).
- **Public Use:** When using BYOD outside school (e.g., for homework), avoid processing sensitive data without secure connections; use caution with Bluetooth/NFC to prevent interception.

Network Protection Measures

The school implements the following to safeguard the network:

- Firewalls, intrusion detection/prevention systems (IDS/IPS), and zoning to isolate BYOD traffic from critical systems.
- Regular audits for rogue access points and vulnerability scans.
- Logging of all access attempts.
- Bandwidth management to prevent abuse.

BYOD traffic is segregated (e.g., in a guest/staff/student domain) and filtered to block malicious sites.

Monitoring, Enforcement, and Consequences

- The IT department will monitor compliance through logs, scans, and random audits. Abnormal activities (e.g., malware detection) may trigger investigations.
- Violations will be handled progressively:
    - First offense: Warning and mandatory retraining.
    - Repeated or serious offenses (e.g., data breach): Temporary or permanent revocation of network access; disciplinary action (e.g., suspension for students, termination for staff).
    - Legal violations: Reported to authorities as required.
- Appeals can be made to the Principal within 7 days.

Acknowledgement

By connecting a BYOD to the school network, users agree to comply with this AUP. Parents/guardians must co-sign for students under 18. Acknowledgement can be via signed form, email confirmation, or MDM enrollment.

Contact: For questions, contact the IT Head at [email/phone]. This policy will be reviewed annually or as needed, in line with EDB guidelines.

End of Document

Practical Guide to Network Management and Wireless Security

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for data labelling in schools across Hong Kong. Its aim is to help educational institutions maintain a consistent baseline in protecting their networks, providing a secure manner in which schools can enable wireless security.

The scope of this guide includes network technical controls, hardening servers and network devices along with wireless network protections. It is designed to be adaptable for different school sizes, system types, and available resources. These guidelines have been derived from various accredited sources, including the Education Bureau of Hong Kong (EDB) as well as the Centre for Internet Security, both of whom have provided guidance and resources that are used to form the basis of these guides.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Enable hardening measures on servers and network devices
- Implement the use of strong protocols such as WPA3, robust authentication methods and strict network separation
- Regularly validate through port and vulnerability scanning to identify and fix weaknesses
- Continuously iterate on and improve these processes, through annual reviews and adaptations to new threats

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Network Security Management

This section describes core components to designing and maintaining secure network architectures for schools should take reference.

2.1. Maintaining Network Inventories

- For all Network Devices and Endpoints that connects to the internal network, document their IP addresses (if applicable) and configurations.
- Network diagrams should be maintained and be updated when new devices are added to the internal network, or when old devices are retired.

Practical Examples:

- Use a spreadsheet or database table for inventory tracking. Using a database would allow merging with existing asset management lists.

2.2. Internal Network Design

- **Non-routable IPs:** Design networks using private IP addressing for internal systems by assigning non-routable IP ranges (e.g., 192.168.x.x) to prevent external access.
- **Network Segregation:** Use subnets as the high-level grouping of resources and machines for easy access control. Deny communication across subnets on default.
- **DMZ:** If there is a need for public access of internal resources (e.g., web servers), put that resource inside a Demilitarized Zone (DMZ).

Practical Examples:

- Use the 192.168.0.0 IP range, set up the gateway to make 3 virtual subnets for external devices, internal devices and file servers.
- Alternatively, use another Internet Service Provider for internet connectivity of external devices to physically separate external devices from internal network.

2.3. Network Access Controls

Map out the access needs of endpoints and resources. Consider a group-based access management, which means the map should list all groups and their access rights, and then all members in each group.

Some examples of groups would include:

- Groups of Machines (e.g., Staff Room PCs, Classroom PCs, etc.)
- Devices connected to a certain group of access points
- Groups of internal resources (e.g., all backup servers)

To accommodate to operational needs, make a policy for requesting, granting and revoking access.

Adaptational Tips:

- Treat all mobile devices as external by default.
- Keep in mind that logical Network Access Controls may be circumvented in some circumstances. To absolutely deny access to internal resources, consider Physical Network Segregation. Despite so, Logical Network Access Controls are nonetheless crucial to Network Security.

3. Network Technical Controls

This section lists technical controls that can be used to enforce controls in a well-designed network. Use the below recommendations as a reference for your school.

3.1. Access Control

- **Access Control Lists (ACLs):** Set ACLs on firewalls and routers to restrict traffic by defining rules that allow only necessary ports and protocols (e.g., block inbound traffic except for approved services). Denied attempts can be sent to an intrusion detection system for review.

Adaptational Tips:

- When used in hand with proper network segregation, schools can implement whitelists based on subnets.
- We highly recommend using a whitelist approach, by adding an explicit deny of all traffic as default.

3.2. Web Filtering

- **Web Proxies:** Web Proxies can be used to block malicious IPs, phishing sites, and non-educational content. Some proxies could Man-in-the-Middle TLS connections and read page contents. Denied attempts can be sent to a logging system.
- **DNS Proxies:** DNS Proxies cannot read page content, but it blocks access to malicious pages by blocking the DNS query.

3.3. Monitoring Tools

Set up Intrusion Detection Systems (IDSs) behind key choke points such as gateways or inside the DMZ, and set up an alert system (e.g., emails, text messages) for suspicious activities.

Practical Examples:

- Repurpose a PC, install a lightweight operating system and then an open-source IDS tool like Wazuh. Create a network Tap or mirror Port at the gateway such that traffic is mirrored into the IDS.
- Tune signatures and patterns to minimize false alarms. Analyse initial logs to identify common false positives; Then adjust thresholds or exclude specific traffic patterns.

4. Hardening Servers and Network Devices

Many applications and network devices come with insecure configurations for compatibility purposes. Schools should take note of the following and revoke insecure configurations on their devices and applications.

4.1. Securing Admin Sessions

- **Encrypted Connection:** A lot of administrative sessions for network devices, such as routers and firewalls use the unencrypted HTTP connection by default. Use HTTPS instead.
- **Certificate Management:** A lot of network devices uses a self-signed certificate. Export this certificate and install in the trust stores of the devices used to access the admin interface such that there will be no TLS errors under normal conditions, but a certificate error if an attacker tries to spoof the admin session.
- **IP Whitelisting:** Restrict access to admin interface by limiting the IPs that can access the admin interface. This should be done with DHCP reservations and/or static IP for devices used to access the admin interfaces.
- **Secure Passwords:** Change default passwords and strictly follow the admin password policy in the Security Configuration Checklist.

4.2. Securing Services and Applications

- **Managing Services:** Disable any unused services on a server. Subscribe to patch notifications to apply patches timely.
- **Application Hardening:** Harden application configurations and install security patches by following vendor or third-party (e.g., CIS) hardening guides (e.g., disabling default features). Use encrypted protocols for application traffic.
- **Administrative Access:** Use certificate verification in SSH sessions. Disable password logins.

5. Wireless Networks

Wireless networks are known to have weaker security than wired networks. As a rule of thumb, all devices connecting to Access Points with the same SSID should be treated as an individual group in the network access control model.

5.1. Wireless Network Authentication

Consider an Access Point as a hub which a user can plug in a cable as long as they can authenticate to the Access Point. Therefore, the authentication method to the Access Point must be strong.

For Access Points used to provide internet access to the public, use strong passwords that align with the password policy.

For Access Points used to provide access the internal resources, implement one of the following:

- Use client-side certificates to authenticate.
- Disable DHCP and use MAC and IP whitelisting.
- Long password that provides cryptographic levels of entropy. (e.g., 25 random alphanumeric digits and symbols) and policies to forbit password sharing.

Otherwise, use VPN for internal access.

5.2. Wireless Network Protocol

Use Access points with WPA2/WPA3 Protocols. Disable WPA/WEP protocols in access points.

Adaptational Tips:

- The security of WPA2 is very sensitive to the strength of the password. New Access points support WPA3, but often also support WPA2 for backwards compatibility, making downgrade attacks possible depending on implementation. Use a strong password.

5.3. Wireless Network Separation

Segregate wireless networks from internal networks, logically or physically. Physical Segregation tends to be more secure and is recommended for wireless access points that does not need to provide access to the internal network.

If running another set of network infrastructure for physical segregation is not desirable (e.g., another DNS proxy for content filtering), use logical access control and apply stringent access control with gateways or firewalls.

Practical Examples:

- Provide Internet access with another Internet plan, preferably from another Internet Service Provider such that the public internet access is completely segregated from the internal network.
- Make different access points for teachers and administrative staff, for they require different access to internal resources.

6. Validation

This section outlines measures to validate the security of the network, and should be performed regularly (e.g., annually).

6.1. Port Scanning

Use port scanning tools to validate the implementation of access controls. Perform port scans at different subnets and cross check the reports with the Access Control Map (see Section 2.3).

If there are any inconsistencies, review the firewall rules.

Practical Examples:

- Use nmap to scan for open ports. Use the -p 0-65535 flag to scan for all open ports.
- Expect to see only the ports allowed in the firewall rules.

6.2. Vulnerability Scanning

Use vulnerability scanning tools to find out any vulnerabilities from missing patches in the running services. Review the report and apply the relevant patches if the vulnerabilities apply to the server/network setup.

Adaptational Tips:

- Place the scanner in a subnet with full network access. Firewalls will affect scanning accuracy due to limitation of scanning scope.

7. Review and Improvement

7.1. Regular Policy Review

Set a reminder to review your school's data handling and labelling standards at least once a year, or whenever there are changes to your IT systems. Involve both IT staff and teaching/administrative colleagues to gather helpful feedback.

7.2. Adapting to New Threats and Technologies

Stay updated about new cyber threats that can affect schools, such as phishing scams or password leaks. Also, be aware of new technology or software updates that might offer better ways to protect passwords, e.g. two-factor authentication.

7.3. Making Improvements

After each review, update your password policy as needed. Communicate any changes clearly to staff and students, and provide simple instructions or workshops to help everyone follow the new rules.

Appendices

Glossary of Terms

Term	Definition
Access Control Lists (ACLs)	A set of rules applied to network devices like firewalls and routers that specifies which traffic is permitted or denied based on factors like IP address, port, and protocol.
Application Hardening	The process of securing an application by applying security patches, disabling unnecessary default features, and following vendor security recommendations (e.g., CIS guides).
DHCP Reservation	A network configuration that instructs a DHCP server to always assign the same specific IP address to a particular device based on its MAC address.
DMZ (Demilitarized Zone)	A separate, isolated network segment that sits between the internal network and the public internet, used to host public-facing services like web servers to protect the internal network.
DNS Proxy	A tool that filters web access by intercepting DNS queries and blocking requests to malicious or prohibited domains before a connection is made.
Downgrade Attack	A type of attack where a hacker forces a system to abandon a secure connection (like WPA3) in favor of an older, less secure one (like WPA2) that is easier to exploit.
Hardening	The process of securing a system by reducing its attack surface, which typically involves disabling unnecessary services, changing default passwords, and applying secure configurations.
Intrusion Detection System (IDS)	A system that monitors network traffic for suspicious activity or policy violations and sends alerts when potential threats are detected.
IP Whitelisting	A security practice where access to a system or interface is restricted to a pre-approved list of IP addresses.
Logical Network Segregation	The practice of dividing a network into smaller, isolated sections (subnets) using software-based controls like VLANs and firewall rules.
MAC and IP Whitelisting	A wireless authentication method where only devices with pre-approved MAC addresses and corresponding static IP addresses are allowed to connect.
Network Access Controls	Policies and technical rules that define which users, devices, or groups are allowed to access specific network resources.
Network Diagrams	Visual representations of the school's network, showing how devices are interconnected and where they are located.
Network Inventories	A comprehensive record of all network devices and endpoints, including their IP addresses, configurations, and their physical/logical layout.
Network Segregation	The practice of dividing a network into smaller, isolated sections (subnets) to control traffic flow and limit the spread of potential security threats.
Network Tap / Mirror Port	A method used on a network switch to copy network traffic from one or more ports to a designated monitoring port, allowing an IDS to analyze the traffic without being in-line.
Non-routable IPs	IP addresses (like the 192.168.x.x range) reserved for use on internal networks that are not directly accessible from the public internet.

Term	Definition
Physical Network Segregation	Isolating networks using physically separate hardware, such as different switches, routers, or even separate internet service providers, to prevent any direct communication.
Port Scanning	The process of probing a server or host for open network ports, used to identify running services and verify that firewall rules are working as intended.
Self-signed Certificate	An SSL/TLS certificate that is not signed by a trusted Certificate Authority (CA), but by the entity that created it (e.g., the network device itself).
SSID (Service Set Identifier)	The public name of a wireless network that users see when searching for Wi-Fi connections.
Subnet	A logical subdivision of a larger network, allowing for more efficient traffic management and the application of granular security policies.
Vulnerability Scanning	The automated process of scanning systems, networks, and applications to identify known security vulnerabilities, such as missing patches or insecure configurations.
Web Proxy	A server that acts as an intermediary for web requests, allowing the school to filter content, block malicious sites, and monitor traffic.
Whitelist Approach	A security strategy where all network traffic is blocked by default, and only specifically approved traffic is explicitly allowed to pass.
WPA2 / WPA3	Modern security protocols for wireless networks that provide strong encryption and authentication. WPA3 is the latest and most secure standard.

End of Document

Practical Guide to Physical and Environmental Security

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for physical and environmental security maintenance in schools across Hong Kong. Its aim is to help educational institutions maintain a consistent baseline in keeping schools safe, protecting the school environment against physical and environmental threats.

The scope of this guide includes environment segregation measures, provisioning security measures and resources at different points in the school environment. It is designed to be adaptable for different school sizes, system types, and available resources. These guidelines have been derived from various accredited sources, including the Education Bureau of Hong Kong (EDB) as well as the Centre for Internet Security, both of whom have provided guidance and resources that are used to form the basis of these guides.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Segregate and secure school premises into public, protected and restricted areas
- Mitigate environmental hazards such as fires, floods, typhoons through guidelines on the installation of specialized protection systems
- Selecting the appropriate access control systems, addressing physical and environmental controls
- Implement physical controls to protect and maintain assets, creating a proactive system that assist in layering defences against physical and environmental risks

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Site Preparation

This section describes core components to preparing a school site against physical and environmental security threats. If this guide is being applied to existing school premises, check if the following considerations have been addressed.

2.1. Campus Segregation and Resource Allocation

Segregate the campus into public, protected, and restricted areas. Examples:

- **Public area:** hallways, canteen, etc.
- **Protected area:** Classrooms, Libraries, etc.
- **Restricted area:** Server Room, Staff Room, etc.

Put the classification on a list and assign adequate resources to securing each protected and restricted area.

Adaptational Tips:

- Resources to securing each area could include staffing (e.g., supervision), Real-Time Monitoring (e.g., CCTV systems), Access Control Systems (e.g., Lock and Key, Badges) and another other appropriate measures and policies.

Practical Examples:

- To secure a server room, a school decides to enforce staff supervision with a policy, install CCTV systems, and a badge-in-badge-out system.

2.2. Hazard Preparation

Implement safeguards against fire, flood and typhoon risks, especially in restricted areas like server rooms.

Measures against fire hazards:

- Install detection systems like VESDA (laser-based smoke detection) and thermal sensors to identify smoke or temperature anomalies before a fire starts.
- Conduct regular testing on the detection and alarm system as per normal fire prevention protocols.
- Use gas-based fire suppression systems or fire extinguishers instead of water to avoid damaging IT equipment.

Measures against flooding:

- Inspect roofs, podiums, flat roofs, basements, and drainage systems regularly to ensure drains and manholes are clear of blockages.
- Locate the server room above flood zones and elevate equipment above ground from potential water entry.

Measures against Typhoons:

- Add weather stripping for server room doors or add a room before the server room.
- Do not add windows to the server room to prevent water entry due to leaky or broken windows.

Measures against Power Cuts:

- Install dedicated circuits for servers so that the power will not be cut by the circuit breaker from a fault in other appliances.
- Install UPS for servers so that there is enough time to gracefully shut down the server upon power cut.

Adaptational Tips:

- Some UPS can send signals to shut down a server via network interface upon power disruptions. In this case, pay extra attention to configuring the remote shutdown service. Use a physically segregated network, and IP whitelist the shutdown signal server side.

2.3. Access Control Systems

Below enlists facts on common access control systems which the school should pay special attention to when choosing.

Doors:

- Use doors with safety hinges which lock the door in place when the hinge is removed.
- Use doors with the dead latch mechanism and use the provided strike plate with the door. Do not use a strike plate with a hole too large for the latch.
- Check for good fitment between the frame and the door and apply weather stripping to make it harder for attackers slipping tools across.

Traditional Locks:

- Use locks with anti-picking features such as security pins, sidebars and restricted keyways.
- Keep keys out of sight so they cannot be replicated by reconstructing from pictures.
- Check if there are any numbers engraved/printed on the keys. If the numbers from the keys are short in length (e.g., 4 digits), the keys may have not enough entropy and may be reused in another batch the same lock model.

RFID Badge Systems:

- Use RFID systems with a secure protocol not prone to unauthorized read and emulation. Dated implementations such as Mifare Classic are often prone to such attacks. Mifare Desfire is currently considered to be secure apart from the UID.

Biometric Locks:

- Biometric Locks can be prone to spoofing. Use Biometric Locks with liveness detection mechanisms such as pulse and heat sensing or multi-modal locks such as combining Biometrics with PIN.

PIN Locks:

- Prolonged use of the same PIN may result in a wear pattern which exposes the PIN combination. Rotate PINs that include different digits regularly.

Magnetic Locks/Electric Door Release Mechanisms:

- Use cabled buttons for door release mechanisms. Such cables should connect from the door release button to the door itself. The door release mechanism should involve no wireless communications.
- Do not expose the cable from the button to the door in public areas.
- Keep in mind that they require electricity to stay locked. Check for the battery life to see for how long the door can stay locked upon a power cut.

2.4. Environmental Controls

- Maintain optimal environmental conditions in IT areas, such as temperatures between 20-25°C and humidity 50-80% to prevent premature hardware failures.
- Add redundancy on the cooling power of the environmental controls such that the servers can run uninterrupted during maintenance.
- Implement a maintenance schedule to ensure regular maintenance while the total cooling power could accommodate the server exhausted heat.

2.5. Surveillance Deployment

- Choose cameras that can record in visible light and infrared when there is insufficient visible light.
- Map out the placements and the dead zones on a school plan before deployment. Make sure that all assets have been covered by surveillance.
- Physically segregate the surveillance network from the internal network and from the internet if possible.

3. Asset Security and Maintenance

This section lists technical controls that can be used to physically secure assets. Use the below recommendations as a reference for your school.

3.1. Asset Physical Controls

- Deploy asset locks, such as Kensington Locks for assets located in public area to prevent from stealing. Confirm that the lock is well attached to some permanent structure and cannot be removed without unlocking.
- Deploy cable locks for network cables in accessible areas to prevent unauthorized network access/tapping.
- Place assets such as access points in places that are physically hard to reach, such as ceilings or inside locked cabinets.

3.2. Human Controls

- Use authorized personnel lists with different colour coded badges for staff, visitors and contractors.
- Make a policy for staff to report any suspicious personnel in secured areas to security.

Adaptational Tips:

- Clearly state the areas authorized for the contractors in the authorized personnel lists so that the Security could monitor them with surveillance.

Practical Examples:

- Use Red for visitors and Yellow for Contractors. Ask Staff to report any people with no badges/Red badges to security.

4. Review and Improvement

4.1. Regular Policy Review

Set a reminder to review your school's data handling and labelling standards at least once a year, or whenever there are changes to your IT systems. Involve both IT staff and teaching/administrative colleagues to gather helpful feedback.

4.2. Adapting to New Threats and Technologies

Stay updated about new cyber threats that can affect schools, such as phishing scams or password leaks. Also, be aware of new technology or software updates that might offer better ways to protect passwords, e.g. two-factor authentication.

4.3. Making Improvements

After each review, update your password policy as needed. Communicate any changes clearly to staff and students, and provide simple instructions or workshops to help everyone follow the new rules.

Appendices

Glossary of Terms

Term	Definition
Access Control Systems	The collection of hardware (locks, badge readers) and policies used to manage and restrict entry to physical areas.
Asset Locks	Physical security devices, like Kensington Locks, that use a cable to secure equipment (e.g., laptops, monitors) to a fixed object to prevent theft.
Authorized Personnel List	A formal record of individuals (staff, visitors, contractors) who are granted access to specific secured areas, often used in conjunction with badges.
Biometric Lock	A type of lock that uses unique biological characteristics, such as fingerprints or facial features, for authentication.
Cable Locks	Physical locks used to secure network cables to a device or port, preventing unauthorized disconnection or network tapping.
Campus Segregation	The practice of dividing a school's physical premises into zones (Public, Protected, Restricted) based on sensitivity and access requirements.
Dead Latch	A type of lock mechanism that prevents the latch from being pushed back with a tool (like a credit card), offering enhanced security against simple bypass techniques.
Dedicated Circuit	An electrical circuit that supplies power to a single appliance or a specific set of equipment (e.g., servers), isolating it from faults on other circuits.
Environmental Controls	Systems and procedures used to maintain optimal conditions (e.g., temperature, humidity, air quality) in areas with sensitive IT equipment to prevent hardware failure.
Gas-based Fire Suppression	A fire extinguishing system that uses chemical agents or inert gases to put out a fire without using water, thus protecting electronic equipment from damage.
Human Controls	Security measures that rely on people and policies, such as using color-coded badges for identification and training staff to report suspicious individuals.
Infrared (Recording)	A camera feature that allows for video recording in low-light or no-light conditions by detecting heat signatures.
Liveness Detection	A security feature in biometric systems that verifies the presence of a live person (e.g., by detecting pulse or heat) to prevent spoofing with fake fingerprints or photos.
Magnetic Lock	An electromagnetic lock that uses a strong magnetic field to keep a door secure, requiring continuous power to remain locked.
Mifare Classic / Desfire	Types of RFID protocols. Mifare Classic is an older, insecure standard, while Mifare Desfire is a modern, more secure protocol recommended for access control systems.
PIN Lock	An access control lock that requires a numeric Personal Identification Number (PIN) for entry.
Protected Area	A designated zone within a school, such as a classroom or library, where access is limited to authorized groups like students and staff.
Public Area	A zone within a school, such as hallways or a canteen, that is generally open to all students, staff, and visitors without special access controls.
Restricted Area	A highly secure zone, such as a server room or main office, where access is strictly limited to a small number of specifically authorized personnel.

Term	Definition
Restricted Keyway	A feature of a lock that uses a unique key design, preventing unauthorized duplication of keys by standard locksmiths.
RFID Badge System	An access control system that uses cards or fobs containing a Radio-Frequency Identification (RFID) chip to grant entry when presented to a reader.
Safety Hinges	Door hinges designed with a security stud that interlocks with the door frame, preventing the door from being removed even if the hinge pins are taken out.
Security Pins	Specialized pins inside a lock cylinder designed to make lock-picking more difficult by catching or jamming picking tools.
Surveillance Dead Zone	An area within a surveillance system's field of view that is not visible to any camera, creating a blind spot.
UPS (Uninterruptible Power Supply)	A battery backup device that provides emergency power to connected equipment during a power outage, allowing for a safe and orderly shutdown.
VESDA (Very Early Smoke Detection Apparatus)	A highly sensitive smoke detection system that uses laser-based technology to identify microscopic smoke particles, providing an early warning before a fire fully develops.
Weather Stripping	A material used to seal gaps around doors and windows to prevent the intrusion of elements like water, wind, and dust.

End of Document

Practical Guide to Monitoring and Logging

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for data labelling in schools across Hong Kong. Its aim is to help educational institutions establish a structured logging and monitoring standard to enhance their cybersecurity records and practices. Guided by a core principle of having centralized secure storage for logs, this guide introduces a tiered logging policy with practical implementation steps.

The scope of this guide includes the implementation of an effective monitoring system that turn collected logs into actionable intelligence. This is achieved by establishing a baseline for normal network and system behaviour during typical operations. This guide is designed to be adaptable for different school sizes, system types, and available resources. The instructions have been derived from various accredited sources, including the Education Bureau of Hong Kong (EDB) as well as the Centre for Internet Security, both of whom have provided guidance and resources that are used to form these guides.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Reference ISO 27002 to cover key events, such as access attempts, privilege use and configuration changes.
- Implement and adapt a tiered log retention policy and implementation practices based on operating system, with specific configurations for Windows, macOS and Linux. Additional steps are provided for software that lacks native logging features.
- Create an illustration of baseline operations, leveraging resource usage and login times, to create a schedule tracking typical runtime of different IT systems.

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Establishing a Logging Standard

This section details guidelines to establishing a structured logging standard to ensure the completeness of logging implementation. Schools should take reference and modify for their scenarios.

2.1. Scope of Logging

The ISO 27002 standard defines 10 key types of activity to be logged to ensure accountability, which the school should take reference for what to log.

- **System Access Attempts:** Successful and failed attempts to access systems, including logins and logouts.
- **Use of Privileges:** Actions performed using elevated or administrative privileges (e.g., modifying user permissions).
- **System Configuration Changes:** Modifications to system settings, such as changes to firewall rules or software configurations.
- **Application Process Start and Stop:** Initiation or termination of applications or services.
- **System Faults and Errors:** System malfunctions, crashes, or error messages that could indicate security issues.
- **Information Security Events:** Security-related incidents, such as malware detections or unauthorized access attempts.
- **Activation and Deactivation of Protection Systems:** Enabling or disabling security tools like antivirus, firewalls, or intrusion detection systems.
- **Access to Information:** Interactions with sensitive data, including reading, modifying, or copying files.
- **Deletion of Information:** Removal or deletion of files or data, especially those classified as sensitive.
- **Changes to User Access Rights:** Modifications to user permissions or access levels, such as granting or revoking access.

Adaptation Tips:

- The default logging behaviour is usually insufficient for logging all the events above. Follow the next sections for implementation examples.
- Schools can consider adding more events for logging, such as custom anomaly detections if they have the technical capabilities and resources.

2.2. Centralized Storage of Logs

Logs stored within the local machines are vulnerable to sabotage after a local privilege escalation. Logs should therefore be stored in a centralized storage in which case the logs are exported and in a centralized server with proper access controls.

Having a centralized storage of logs is also essential for effective monitoring of events and incident detection.

2.3. Log Transmission

Logs should be transmitted under securely encrypted channels to avoid interception.

2.4. Log Classification and Retention

Appendix C in Hong Kong Government IT Security Guidelines (G3) defines a three-tier classification for information systems based on confidentiality, integrity, and availability (CIA):

- **Tier 1 (Low Impact)**: Public or non-sensitive data (e.g., school website content). Loss or compromise has minimal impact.
- **Tier 2 (Medium Impact)**: Sensitive but not highly confidential data (e.g., staff emails, student attendance records). Compromise may cause moderate disruption or privacy concerns.
- **Tier 3 (High/Critical Impact)**: Highly confidential or critical data (e.g., student personal data, exam results, financial records). Compromise could lead to significant legal, reputational, or operational damage.

Logs are classified based on the system or data they pertain to, with retention periods tied to tiers (e.g., 6 months for Tier 1, 12 months for Tier 2/3).

Adaptation Tips:

- The classification of systems should have been done during the acquisition of assets, which would have been recorded on the Asset List.

3. Implementation of Logging

To ensure that actions are logged with sufficient detail, schools must configure systems and applications beyond default settings. This section lists the high-level steps for setting up key school IT components for logging and exporting logs which a school can reference.

N.B. The clocks across all devices should be synchronized. This is usually done with and NTP server.

3.1. Operating Systems

Windows

Enable advanced auditing in Group Policy (e.g., Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration). Enable categories such as:

- Logon/Logoff (for system access attempts).
- Privilege Use (for administrative actions).
- Object Access (for file access/deletion).
- System (for configuration changes and faults).

Set up Event Log forwarding to the centralized server for aggregation.

Linux

Modify /etc/rsyslog.conf or /etc/syslog-ng.conf to include detailed logging for authentication (auth.*), system changes (cron.*), and security events. Use auditd for detailed audit trails (e.g., auditctl -w /path/to/grading_files -p wa to monitor write/access).

Edit the rules in the config files to export logs to the centralized server.

macOS

Enable logging via log config commands (e.g., sudo log config --mode "level:debug").

Edit the rules in the config files to export logs to the centralized server.

3.2. Network Devices

Configure routers and firewalls (e.g., pfSense, Cisco) to log traffic (inbound/outbound), access attempts, and configuration changes. Enable syslog output to a central server (e.g., via logging host <server_ip> on Cisco devices).

3.3. Applications

Local Applications

Configurations for applications differ. Schools should explore logging features for each application. Application logs are usually integrated with system logs, which will have been exported to the central server if set up properly.

Enterprise-Grade Applications typically have robust, configurable logging features. For example, Google Workspace's Admin Console logs user actions, file access, and configuration changes, while Microsoft 365's Audit Log captures similar events. Schools can enable these via settings, but may need to adjust defaults for granularity.

Cloud Applications

Schools should explore the logging features of cloud applications and the export functionality. It is recommended to export logs to the centralized logging server.

Applications Without Native Logging Support

To address applications with insufficient or no logging, schools can adopt the following strategies:

- **Supplement with system-level logging:** Configure OS auditing to watch directories where the app stores data (e.g., student records).
- **Supplement with network-level logging:** Route application traffic through a proxy to log http/https requests.

4. Implementing Monitoring Systems

This section provides a high-level overview of implementation of a effective monitoring system for the school's reference.

4.1. Establishing Monitoring Metrics

Below are elements that could indicate threats like data breaches, malware, or unauthorized access. Consider monitoring them based on the school's use case. Key areas include:

- **Inbound/Outbound Traffic**: Monitor network flows through firewalls or gateways to detect unusual patterns, such as data exfiltration to foreign IPs or incoming scans from known malicious sources.
- **Access to Critical Resources**: Watch logins to sensitive systems like student information systems or learning management systems such as Google Classroom or Canvas.
- **Configuration Files**: Keep an eye on changes to system configs, like firewall rules or user permissions, to prevent tampering. Example: Detect unauthorized edits to /etc/passwd on Linux servers or registry keys in Windows that could enable backdoors.
- **Security Tool Logs**: Aggregate alerts from antivirus, anti-malware, or endpoint detection tools.
- **Resource Usage**: Track CPU, memory, disk, and bandwidth to spot resource-intensive activities.

Practical Examples:

- Track HTTP/HTTPS traffic for spikes in uploads/downloads, which might signal ransomware encrypting and sending student files.
- Monitor failed login attempts and flag IP addresses.
- Monitor access from outside the school's geographic area based on IP.
- Monitor edits or attempts to modify important config files or registry keys.

4.2. Establishing Baselines for Normal Behaviour

Collect data over 2-4 weeks during normal school operations to define baselines. Such baselines can then be compared in real-time monitoring to catch anomalies.

For every metric of measurement there needs to be a baseline, which should form a pattern over time.

Note that there may be heavy fluctuations of data due to prominent events in the school such as exam periods, which may trigger false positives. The baselines should therefore be reviewed and refined appropriately if such events happen.

Practical Examples:

- Regular patterns: From the logs the team observed peak logins at 8AM every day, and decides that this is normal behaviour due to teachers and students arriving at school. This behaviour is then documented, and the threshold for triggering a warning in this period is set higher.
- Spikes: Right before the examination period, printer usage may spike due to the need of printing examination papers.
- Droughts: Access numbers plummet or even drop to zero in the middle of the night.

4.3. Configuring Alerts

Set real time alert rules based on the observed patterns and baseline. Integrate with tools that send email, SMS, or push notifications, or slack/telegram/discord bots.

Adaptation Tips:

- The list of alerts rules can be long and tedious, and takes time to refine, see Triggers For Review.

Practical Examples:

- Alert on sustained CPU spikes above baseline on lab computers during off-hours.
- Alert on sudden network spike from exotic countries, e.g., Iran or North Korea.
- Alert on any automatic countermeasures, e.g., ip blocked due to failed login attempts.

4.4. Triggers For Review

- **False Positives:** An alert should trigger a response procedure. Any incident response procedure contains the verification of the potential incident to

determine the validity of the alert. If the alert is a false positive, investigate the cause of the false positive, and adjust the threshold/baseline pattern to fit any new observations.

- **Underfitted thresholds:** If a threshold seems to be set way above normal use levels, consider lowering it to match use cases. If the headroom is left for time/event-specific spikes, consider implementing different rules for normal and busy periods.

4.5. Monitoring Tools

Here lists a non-exhaustive list of tools a school can consider for real-time monitoring.

- **IDS/IPS (Intrusion Detection/Prevention Systems)**: For network monitoring, Snort is open-sourced, Linux based tool for configuring rules to monitor inbound traffic. Integrate with Barnyard2 for database logging and Snorby for a web interface to view alerts.
- **Host-Based Monitoring**: OSSEC is a free monitoring tool that can be installed on Windows/Linux machines and configured to watch for file integrity (e.g., alert on changes to student database files). Otherwise, one could set up operation system level logs for the directories and monitor with centralized log monitoring.
- **File Integrity Monitoring**: Tripwire (open-source version available) scans critical directories (e.g., /var/www for web apps), and conduct daily checks. If a config file changes unexpectedly, it notifies via syslog, which one could route to your alerting system.
- **Bandwidth and Resource Monitoring**: PRTG Network Monitor is free for up to 100 sensors. One could install on a Windows server, add sensors for CPU on lab PCs and bandwidth on routers and configure SMS notifications.
- **Centralized Log Monitoring:** Greylog is open-source log management platform that collects, indexes, and analyzes logs in real time. It's ideal for schools needing a scalable solution to monitor network traffic, security events, and resource usage.

5. Review and Improvement

5.1. Regular Policy Review

Set a reminder to review your school's data handling and labelling standards at least once a year, or whenever there are changes to your IT systems. Involve both IT staff and teaching/administrative colleagues to gather helpful feedback.

5.2. Adapting to New Threats and Technologies

Stay updated about new cyber threats that can affect schools, such as phishing scams or password leaks. Also, be aware of new technology or software updates that might offer better ways to protect passwords, e.g. two-factor authentication.

5.3. Making Improvements

After each review, update your password policy as needed. Communicate any changes clearly to staff and students, and provide simple instructions or workshops to help everyone follow the new rules.

Appendices

Glossary of Terms

Term	Definition
Advanced Auditing	A feature in Windows Group Policy that allows for the detailed configuration of which specific system events are logged, such as privilege use or object access.
Anomaly Detection	The process of identifying unusual patterns or deviations from an established baseline of normal behavior, which could indicate a security threat.
Auditd	The Linux audit daemon, a system component used for creating detailed, kernel-level audit trails of system calls and file access.
Baseline (of Normal Behaviour)	A standard or pattern of normal system and network activity established over a period of time, used as a reference to detect anomalies and security threats.
Centralized Storage of Logs	The practice of exporting and storing logs from multiple systems and devices onto a single, secure server to prevent tampering and facilitate analysis.
CIA Triad (Confidentiality, Integrity, Availability)	A security model used to classify information systems based on three core principles: protecting data from unauthorized disclosure (Confidentiality), ensuring data accuracy (Integrity), and making sure data is accessible when needed (Availability).
Data Exfiltration	The unauthorized transfer or copying of data from a computer or network to an external location.
False Positive	An alert that incorrectly indicates that a security incident has occurred when it has not, often triggered by legitimate but unusual activity.
File Integrity Monitoring (FIM)	A process or tool that monitors and detects changes to critical system or configuration files, alerting administrators to potential unauthorized modifications.
Group Policy	A feature in Microsoft Windows for managing configurations for users and computers, including enabling advanced security and logging settings across a network.
Host-Based Monitoring	Security monitoring focused on activities and events occurring on an individual device (host), such as file changes, log entries, or process execution.
IDS/IPS (Intrusion Detection/Prevention System)	A system that monitors network traffic for malicious activity or policy violations and can either alert administrators (IDS) or actively block the threat (IPS).
ISO 27002	An international standard that provides a framework and guidelines for information security controls, including best practices for logging and monitoring events.
Log Classification and Retention	The process of categorizing logs based on the sensitivity of the system they relate to and defining a specific period for how long those logs must be kept.
Log Transmission	The process of sending log data from a source system (like a server or firewall) to a centralized storage server, which should be done over a secure, encrypted channel.
Monitoring Metrics	Specific, measurable elements of system or network activity (e.g., CPU usage, login failures) used to track performance and detect potential security threats.

Term	Definition
NTP (Network Time Protocol)	A networking protocol for synchronizing the clocks of computer systems over a network, which is essential for correlating events accurately across different logs.
Proxy (for logging)	An intermediary server that can route application traffic, allowing it to log requests and supplement the native logging capabilities of applications that lack them.
Real-time Alert	An automated notification sent immediately when a monitoring system detects an event that matches a predefined rule indicating a potential security incident.
Resource Usage	A monitoring metric that tracks the consumption of system resources like CPU, memory, disk, and network bandwidth to spot unusual or resource-intensive activities.
Syslog	A standard protocol used to send system log or event messages to a specific server, known as a syslog server, for centralized collection and analysis.
Tiered Classification (of Systems)	A method of categorizing information systems into different levels (e.g., Tier 1, 2, 3) based on their impact on confidentiality, integrity, and availability, which then dictates log retention policies.
Underfitted Threshold	An alert threshold that is set too high or is not sensitive enough, failing to detect subtle but potentially malicious activity that falls below the trigger level.

End of Document

Practical Guide to Supplier Relationships

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides practical recommendations and baseline standards for managing supplier relationships, specifically for schools across Hong Kong. Its aim is to help educational institutions maintain a consistent baseline in third party management, enabling schools to establish secure working relationships with relevant third parties.

The scope of this guide includes best evaluation methods of a supplier's security practices, and embedding clear security requirements into contracts. It is designed to be adaptable for different school sizes, system types, and available resources. These guidelines have been derived from various accredited sources, including the Education Bureau of Hong Kong (EDB) as well as the Centre for Internet Security, both of whom have provided guidance and resources that are used to form the basis of these guides.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Evaluate whether suppliers are in compliance with recognized standards such as ISO 27001
- Define security requirements clearly in supplier contracts, including data handling, ownership, return/deletion upon termination, backup schedules, and incident reporting protocols
- Monitor supplier performance with important metrics which evaluate the use of client-side tools
- Establish clear communication channels and integrate supplier procedures into the school's own incident response plans

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Negotiating with Suppliers

This section describes common items to take notice and worth checking before subscribing to a supplier service. Schools should take this list for reference and adopt to their circumstances.

2.1. Evaluation of Supplier Security Practices

- Perform technical review of supplier security, such as understanding access controls, encryption methods, and vulnerability management.
- Identify risks in supplier systems, like data breach histories, through basic web searches or vendor-provided reports.
- Consider compatibility with school IT infrastructure.

Adaptational Tips:

- Check if the supplier has any compliance to standards such as NIST or ISO 27001.

Review supplier proposals on their uptime and security commitments. Negotiate terms to include penalties for non-compliance and the right to terminate if security standards slip (e.g., security audit fail or a publicly known security incident).

2.2. Security Requirements in Agreements

This section focuses on making sure that provided service reaches a certain security standard to protect the interests of the school.
The agreement should cover the below security clauses:

- How the supplier handles data – how data is stored, transmitted and retained before deletion.
- The ownership, return and deletion of data upon contract end.
- The Supplier's backup schedules and their retention scheme.
- Uptime of the service and compensations upon service disruption.
- The duration, scope and cost of ongoing security updates (e.g., patches)
- Communication protocols upon cyber incidents.

Adaptational Tips:

- Use their agreements to check against the cybersecurity policy to see if any further measures has to be taken, or if the service is suitable.

Practical Examples:

- Assume a cloud storage provider that does not encrypt data stored on their servers. The school can either make a policy of encrypting everything before uploading or ditch the service.

2.3. Exit Strategies and Contract Termination

Plan ahead supplier changes. It would be horrible if there is a need to change the supplier, only to find out that all data has to be exported manually.

- Include exit clauses in agreements to ensure data can be transferred and erased upon contract termination (e.g., export utilities).
- Test the data export functionalities before deployment of the service in production, and make local backups regularly. Define such backup schedules in the backup policy of the school.

Practical Examples:

- Ensure data export functionalities in the agreement with the cloud service, then test its functionality during testing phase.
- Export the data daily to make local backups according to the Backup and Retention Policy.

3. Performance Evaluation

This section describes common metrics to measure the performance of a supplier service. Schools should take this list for reference and adopt to their circumstances. Please note that performance monitoring may be highly dependent on the transparency of the Supplier. (e.g., built-in monitoring tools for their service.

3.1. Metrics of Performance

Not all of the listed metrics can be easily monitored. It depends on the Service Provider.

- **Latency:** Measures the time taken for requests to be processed and responded to, helping identify bottlenecks in response times.

- **Throughput:** Tracks the number of requests or operations handled per unit of time, such as requests per minute.
- **Error Rates:** Monitors the percentage of failed requests or operations, indicating reliability issues.
- **Resource Utilization:** Includes CPU usage, memory consumption, and storage I/O operations per second (IOPS), which reveal if your resources are over- or under-provisioned.
- **Uptime and Availability:** Calculates the percentage of time the service is operational, often tied to SLAs (Service Level Agreements).
- **Cost-Related Metrics:** Compute costs or cost-benefit analysis, to ensure that performance aligns with spending.

3.2. Client-Side Monitoring

Client-Side monitoring removes provide dependency and provides a real-user perspective. Tools for monitoring include:

Basic Command-Line Tools:

- **Ping:** Use the built-in ping command on Windows, macOS, or Linux to send packets to the cloud service's endpoint (e.g., ping api.examplecloud.com). It reports average round-trip time (RTT) in ms. For continuous monitoring, tools like MTR (My Traceroute) combine ping with traceroute to identify hops causing delays.
- **Curl or Wget for Throughput**: Test download speeds with curl or wget.

Centralized Continuous Monitoring:

- **Proxy:** Proxies can be configured to log and measure latency and bandwidth of an endpoint, which would reflect the performance of the Supplier.

4. Incident Management Involving Suppliers

This section lists technical controls that can be used to physically secure assets. Use the below recommendations as a reference for your school.

4.1. Incident Report Procedures

Require suppliers to provide clear incident reporting mechanisms in agreements, reviewing their response plans during evaluations. These mechanisms should include:

- Any detection mechanisms from the supplier (e.g., logs, warnings, etc.)

- Any reporting mechanisms from the school (e.g., help tickets, etc.)

4.2. Incorporating Incident Response Procedures

- Integrate supplier incident reporting into school monitoring, using their dashboards or alerts for quick detection.
- Create procedures for incident response involving suppliers, including escalation paths for school leadership and who to contact.
- Maintain contact lists for supplier support. Test contact channels regularly (e.g., annually) if possible.

5. Review and Improvement

5.1. Regular Policy Review

Set a reminder to review your school's data handling and labelling standards at least once a year, or whenever there are changes to your IT systems. Involve both IT staff and teaching/administrative colleagues to gather helpful feedback.

5.2. Adapting to New Threats and Technologies

Stay updated about new cyber threats that can affect schools, such as phishing scams or password leaks. Also, be aware of new technology or software updates that might offer better ways to protect passwords, e.g. two-factor authentication.

5.3. Making Improvements

After each review, update your password policy as needed. Communicate any changes clearly to staff and students, and provide simple instructions or workshops to help everyone follow the new rules.

Appendices

Glossary of Terms

Term	Definition
Client-Side Monitoring	The practice of measuring a supplier's service performance from the school's own network to get a real-user perspective on metrics like latency and throughput.
Contract Termination	The formal process of ending an agreement with a supplier, which should be governed by pre-defined clauses in the contract.
Error Rate	A performance metric that tracks the percentage of failed requests or operations within a supplier's service, indicating its reliability.
Escalation Path	A predefined procedure that outlines who to contact within the school (e.g., leadership) and the supplier organization when an incident needs to be elevated.
Exit Strategy	A pre-planned process for ending a supplier relationship, ensuring that school data can be securely and completely transferred or erased upon contract termination.
Export Utilities	Tools or features provided by a supplier that allow a school to easily extract its data from the service in a usable format.
Incident Reporting Mechanism	A formal process defined in a supplier agreement that outlines how, when, and to whom security incidents should be reported by either the supplier or the school.
ISO 27001	An international standard for information security management, which can be used as a benchmark to evaluate a supplier's security posture and compliance.
Latency	The time delay between a request being sent to a supplier's service and a response being received, used to measure responsiveness and identify bottlenecks.
NIST	The National Institute of Standards and Technology (USA), which provides cybersecurity frameworks that can be used to assess a supplier's security practices.
Performance Evaluation	The process of measuring and assessing a supplier's service against key metrics to ensure it meets the school's operational and contractual requirements.
Resource Utilization	A performance metric that measures how much of a supplier's computing resources (e.g., CPU, memory) are being consumed, helping to ensure resources are provisioned correctly.
Retention Scheme	A supplier's defined policy on how long they will store a school's data and backups before it is permanently deleted.
Round-Trip Time (RTT)	The total time it takes for a data packet to travel from a source (the school) to a destination (the supplier) and back again; a primary measure of latency.
Security Clause	A specific term within a supplier agreement that defines security obligations related to data handling, storage, return/deletion, backups, and incident response.
Service Level Agreement (SLA)	A part of a contract that formally defines the expected level of service from a supplier, including guarantees for uptime, performance, and penalties for non-compliance.

Term	Definition
Supplier Security Practices	The set of technical controls and policies a supplier uses to protect its systems and client data, including access controls, encryption, and vulnerability management.
Throughput	A performance metric that measures the number of operations or requests a supplier's service can handle in a specific unit of time (e.g., requests per minute).
Uptime and Availability	A metric that calculates the percentage of time a supplier's service is operational and accessible to users, often guaranteed in an SLA.
Vulnerability Management	The supplier's process for identifying, evaluating, and remediating security weaknesses in their systems and software.

End of Document

Practical Guide to Use of Generative AI

Version 1.0

This document is intended as a practical guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Introduction

1.1. Purpose and Scope

This guide provides guidelines on the use of generative AI (GenAI) at schools, covering the various tools that may be used and a high-level approach to incorporating the tools into the school environment. The guide will also provide adaptational tips that empower schools to identify and counteract against the potential pitfalls and risks of generative AI, grounding its use in healthy practices that allow responsible and efficient use of AI.

The scope of this guide includes the strengths and weaknesses of generative AI, its potential privacy and data management risks that must be managed for safe use of generative AI, along with steps to mitigate common risks when handling data intended for AI use. It is designed to be adaptable for different school sizes, system types, and available resources. These guidelines have been derived from various accredited sources, including the Education Bureau of Hong Kong (EDB) as well as the Centre for Internet Security, both of whom have provided guidance and resources that are used to form the basis of these guides.

1.2. Audience (IT Administrators & Tech Staff)

This guide is intended for IT administrators, technical staff, and anyone responsible for managing user accounts or IT systems within the school environment. It assumes a basic understanding of information technology operations.

By following the guidance in this document, IT teams will be better equipped to:

- Establish a series of guidelines for approval of GenAI tools in the school environment
- Implement mitigation strategies for risks and problems arising through GenAI
- Share steps for anonymizing data and protecting data privacy for confidential internal documents that are not to be shared publicly
- Identify the strengths and weaknesses of different GenAI service providers
- Establishing best practices for responsible use across the school

Schools are encouraged to adapt these recommendations to fit their own technical environments and operational needs.

2. Privacy and Data Security

Almost all generative AI services are running in the cloud, which is a fancy way of saying computers that belong to a third party. This section describes controls a school could instantiate to ensure Privacy and Data Security.

2.1. Establishing Guidelines for Approved and Restricted GenAI Tools

- **Vendor Evaluation**: Assess vendors based on security certifications and data privacy terms to ensure only tools with clear privacy guarantees are approved.
- **Network Restrictions**: Block unapproved GenAI tools from being accessed on the school network to maintain security and compliance.
- **Streamlined Approval Process**: Implement a simple process, such as a form for staff to submit tool details (e.g., URL), for efficient review and approval of new tools.
- **Regular Policy Reviews**: Conduct annual reviews of vendor policies to update the approval status of GenAI tools and ensure ongoing compliance.

Adaptational Tips:

- Check for Security Compliance reports such as SOC 2 (Type II), ISO/IEC27001, and Privacy Compliance reports such as GDPR Compliance.
- Although there are GenAI tools embedded inside Operating systems, such as Copilot and Gemini, they only collect data when users actively use their features as of the date of writing.

Practical Examples:

- Block all Restricted GenAI Tools with DNS filtering in school premises.
- In case of banning copilot, use the “Turn off Windows Copilot” policy in GPO or Intune.

2.2. Explore Data Loss Protection (DLP) Solutions

Consider using various Data Loss Protection Solutions for real time monitoring of user inputs. For instance, endpoint Data Loss Protection solutions in form of browser extensions are capable of redacting PII during clipboard paste to specific websites; Network level DLP solutions such as proxies would be able to scan http requests and filter/drop flagged requests.

3. Education on the Matter

Many use GenAI services, but few know the risks. The below provides a framework that IT can reference for making training materials for staff on the matter. Schools should modify this list based on their own circumstances to make more tailored materials.

3.1. Introduction to Generative AI

- Definition and overview: Explain what generative AI is (e.g., tools like ChatGPT, DALL-E, or Midjourney that create text, images, or other content based on prompts).
- Real-world examples relevant to education (e.g., generating lesson plans, summarizing articles, or creating study aids).
- Purpose of the training: Emphasize responsible use to maximize benefits while minimizing risks in a school environment.

3.2. Strengths of Generative AI

- Efficiency and productivity: Speeds up tasks like brainstorming ideas, drafting emails, or creating educational content.
- Creativity and innovation: Assists in generating diverse perspectives, visual aids, or personalized learning materials.
- Accessibility: Supports diverse learners (e.g., language translation, simplified explanations for students with varying needs).
- Scalability: Handles repetitive tasks, freeing up time for educators and staff.

3.3. Weaknesses of Generative AI

- Inaccuracy and hallucinations: AI can produce plausible but false information; Users should always verify outputs.
- Lack of understanding: AI doesn't truly comprehend context or nuances, leading to superficial or biased responses.
- Dependency risks: Over-reliance can hinder critical thinking or skill development in users.
- Resource-intensive: Requires internet access and can be computationally demanding.

3.4. Common Risks and Problems When Using Generative AI

- Misinformation and fact-checking challenges: Outputs may spread errors if not cross-verified.

- Bias and fairness issues: AI trained on imperfect data can perpetuate bias or certain opinions.
- Plagiarism and intellectual property concerns: Generated content might infringe on copyrights or fail to credit sources.
- Security vulnerabilities: Potential for data leaks or exposure when inputting sensitive information.
- Ethical dilemmas: Such as using AI for cheating in academic settings or generating harmful content.

3.5. Identifying and Handling Sensitive Data

- Definitions: Explain confidential (e.g., student records), internal (e.g., school policies), and sensitive data (e.g., personal identifiers like names, addresses, or health info).
- Reference to Data Handling Guidelines: Direct users to school-specific policies for detailed classifications and compliance (e.g., FERPA in the US).
- Red flags: How to spot sensitive data in documents, emails, or prompts (e.g., PII, financial details, or proprietary school info).

3.6. Steps for Anonymizing Data from Internal Documents

- Preparation: Review documents for sensitive elements before inputting into AI tools.
- Basic techniques: Use find/replace in word processors to swap names, dates, or locations with placeholders (e.g., replace "John Doe" with "Student A").
- Advanced methods: Redact images or tables, aggregate data (e.g., use averages instead of specifics), or use anonymization software/tools.
- Verification: Double-check anonymized versions to ensure no identifiable info remains; test with sample prompts.
- Best practices: Avoid uploading full documents; extract only necessary excerpts.

Practical Examples:

- Even with DLP protections in place, it is worthwhile to educate staff on this matter and use DLP as last line of defence.
- Remind staff not to use GenAI tools when Anonymizing Data for GenAI use, which defeats the purpose.

3.7. Identifying Services That Use Generative AI

- Common examples: AI helpers in operating systems (e.g., Microsoft Copilot in Windows, Siri enhancements in iOS).
- Productivity tools: Features in Google Workspace (e.g., AI summaries in Docs), Microsoft Office (e.g., AI writing assistants in Word).
- Educational platforms: Tools like Khan Academy's AI tutor or Duolingo's generative features.
- Web-based services: Chatbots on websites, image generators like Canva's Magic Studio.
- How to check: Look for labels like "AI-powered" or review privacy policies; enable/disable AI features in settings.

Adaptational Tips:

- If applicable, consider extending this to any other third-party cloud services with data input. Promote the idea that the cloud is just someone else's computer.

3.8. Best Practices for Responsible Use

- Prompt engineering: Craft clear, specific prompts to improve output quality and reduce risks.
- Verification and citation: Always cross-check AI-generated content with reliable sources and cite appropriately.
- Privacy protection: Use school-approved tools with strong data safeguards; avoid free/public AI for sensitive tasks.
- Collaboration and oversight: Encourage peer reviews of AI outputs and consider integrating into school workflows.

3.9. Legal and Policy Considerations

- Copyright and ownership: Understand that AI-generated content may not be fully original; respect intellectual property laws.
- School-specific rules: Overview of institutional policies on AI use (e.g., acceptable use in assignments, prohibitions on certain tools).
- Regulatory compliance: Brief on relevant laws (e.g., data protection regulations like GDPR or COPPA for minors).

- Reporting issues: How to flag AI-related problems, such as biases or errors, to school IT/admin.

Practical Examples:

- Suggest staff tools for checking for copyright infringement possibilities, such as Grammarly Plagiarism Checker.

3.10. Case Studies and Interactive Exercises

- Real-life scenarios: Examples of AI misuse in education (e.g., a teacher inputting student data leading to a breach) and successful responsible applications.
- Hands-on activities: Role-playing anonymization, identifying AI in tools, or critiquing AI outputs for accuracy/bias.
- Quizzes or discussions: To reinforce key concepts and encourage reflection.

3.11. Conclusion and Resources

- Key takeaways: Summarize the balance of benefits and responsibilities.
- Ongoing learning: Encourage staying updated on AI developments through school updates or reputable sources.
- Support resources: Links to school guidelines, external tutorials (e.g., from UNESCO on AI ethics in education), or contact info for questions.

4. Miscellaneous

4.1. Establishing Age Controls

General recommendations

The UNESCO Guidance for generative AI in education and research (2023) suggests an age control of minimum 13 years of age for generative AI services.

GenAI providers typically mention the age requirement of 13 for their services, while others require 18 years of age in their Terms of Service to avoid liability to potentially mature content.

Our Recommendation

We recommend using network wide content filtering on student networks such as DNS proxies or firewalls for primary schools.

For Secondary Schools however, we believe it is up for the schools to decide whether or not such controls should be implemented.

Adaptational Tips:

- By applying the concepts of network segragation, different sets of controls can be implemented on networks for student internet access and networks for staff access.

4.2. Review of Policy and Teaching Materials

Due to the rapidly evolving nature of generative AI technologies, including advancements in models, tools, and associated regulations, policies and training materials must be regularly reviewed and updated to ensure accuracy and relevance. New features, ethical considerations, legal requirements, and best practices may emerge, potentially affecting the procedures of handling generative AI.

We recommend revisiting these materials regularly (e.g., annually) or whenever significant updates in AI technology, school policies, or applicable laws (e.g., data protection or copyright regulations) are announced. Always consult the latest terms of service for specific AI tools and your institution's guidelines to stay compliant and informed.

Glossary of Terms

Term	Definition
Generative AI (GenAI)	AI systems that create new content (text, images, code, audio, etc.) in response to user prompts using learned patterns from training data.
Prompt	The text or instructions provided to a GenAI tool to guide the content it generates.
Prompt Engineering	The practice of crafting clear, specific, and structured prompts to improve GenAI output quality and reduce risks.
Approved GenAI Tools	GenAI services that have passed the school's security, privacy, and compliance review and are authorized for use.
Restricted GenAI Tools	GenAI services that are blocked or prohibited due to security, privacy, compliance, or policy concerns.
Vendor Evaluation	The assessment of a GenAI provider's security, privacy, compliance, reliability, and contract terms before approval.
Streamlined Approval Process	A lightweight submission and review workflow (e.g., staff form with tool URL) used to evaluate and authorize new GenAI tools efficiently.
Regular Policy Reviews	Scheduled re-evaluations (e.g., annually) of approved/restricted tools and vendor policies to maintain ongoing compliance.
Network Restrictions	Controls that prevent access to unapproved GenAI services on school networks (e.g., DNS blocks, firewall rules).
DNS Filtering	A control that uses domain name system policies to block or allow access to specific sites or categories (e.g., blocking restricted GenAI tools).
Group Policy Object (GPO)	A Windows/Active Directory mechanism to centrally enforce settings (e.g., "Turn off Windows Copilot") across domain-joined devices.
Microsoft Intune	A cloud-based device and application management platform that can enforce policies (e.g., disable Copilot) on managed devices.
Windows Copilot	Microsoft's AI assistant integrated into Windows that provides AI-driven help and content generation features.
Google Gemini	Google's generative AI suite available across Google products and services to assist with content creation and summaries.
Security Certifications	Independent attestations of a vendor's security controls (e.g., SOC 2 Type II, ISO/IEC 27001).
SOC 2 Type II	An audit report that evaluates the design and operating effectiveness of a service organization's controls over a period of time.
ISO/IEC 27001	An international standard specifying requirements for an information security management system (ISMS).
GDPR	The European Union's General Data Protection Regulation governing personal data processing and protection.
COPPA	A U.S. law (Children's Online Privacy Protection Act) regulating online data collection from children under 13.

FERPA	A U.S. law (Family Educational Rights and Privacy Act) that protects the privacy of student education records.
Data Loss Protection (DLP)	Also called Data Loss Prevention; technologies and processes that detect and prevent sensitive data from leaving approved boundaries.
Endpoint DLP	DLP controls on user devices (e.g., browser extensions) that monitor and block/redact sensitive data before it is sent.
Network DLP	DLP controls at the network level (e.g., proxies) that inspect web/HTTP traffic and block, quarantine, or flag sensitive data exfiltration.
Proxy	A server that intermediates web requests, allowing inspection, filtering, logging, and policy enforcement (e.g., for DLP).
HTTP Request Inspection	The analysis of outbound web requests to detect sensitive content or policy violations before data leaves the network.
Clipboard Redaction	Automatic masking or removal of sensitive data when users paste content (e.g., into web forms), enforced by DLP tools.
Personally Identifiable Information (PII)	Data that can identify an individual (e.g., name, address, email, phone number, student ID, health information).
Sensitive Data	Data that could cause harm if exposed (e.g., PII, financial data, health data, internal assessments).
Confidential Data	Highly restricted information intended for a limited audience (e.g., student records, staff disciplinary files).
Internal Data	Non-public information intended for internal use but not highly restricted (e.g., draft policies, internal memos).
Anonymization	The process of removing or transforming identifiers so individuals cannot be re-identified from the data.
Redaction	The removal or masking of specific sensitive elements (e.g., names, IDs) from documents before sharing or AI use.
Aggregation	Combining data into summaries (e.g., averages, totals) to reduce identifiability and protect privacy.
Placeholders	Generic labels (e.g., “Student A,” “School X”) used to replace real identifiers in documents or prompts.
Anonymization Verification	The double-check process to ensure no identifiable information remains after anonymization or redaction.
Data Minimization	The practice of sharing only the minimum necessary data (e.g., excerpts instead of full documents) to reduce exposure.
Misinformation	False or inaccurate content that may appear plausible in GenAI outputs and must be fact-checked.
AI Hallucination	GenAI output that is fabricated or incorrect but presented confidently as fact.
Bias and Fairness	Undesirable skews in AI outputs originating from training data or model behavior that can affect equity and accuracy.
Verification and Citation	The practice of cross-checking AI-generated content with reliable sources and citing appropriately.
Ethical Use	The responsible application of GenAI that avoids harm (e.g., cheating, harmful content) and respects rights and policies.
Intellectual Property (IP)	Rights related to creations of the mind (e.g., copyrights); relevant when using or generating content with GenAI.

Copyright	The legal right controlling the use and distribution of creative works; implicated in the use of AI-generated or source content.
Plagiarism	The presentation of someone else's work or ideas as one's own without proper attribution; AI outputs may risk this if not verified.
Privacy Policy	A vendor's statement describing what data is collected, how it is used, and user rights related to that data.
Terms of Service (ToS)	Contractual terms governing how a service may be used, including age limits, usage rights, and restrictions.
Data Privacy Terms	Contractual clauses or policies that define how personal data is handled, protected, and shared by a service provider.
School-Approved Tools	Services vetted and authorized by the school for specific use cases based on risk assessments and compliance checks.
Public/Free AI Tools	Consumer-facing AI services that may lack enterprise privacy guarantees and are not approved for sensitive tasks.
Third-Party Cloud Services	External providers hosting applications or AI tools in their infrastructure ("someone else's computers").
Cloud Service	A service delivered over the Internet from provider-owned infrastructure, often multi-tenant and remotely managed.
Responsible AI Use	Practices that maximize educational benefit while minimizing risks (privacy, accuracy, ethics, compliance).
Training Materials	Curated content used to educate staff on GenAI strengths, weaknesses, risks, and safe practices.
Case Studies and Exercises	Realistic scenarios and hands-on activities used to practice anonymization, risk spotting, and output critique.
Reporting Issues	The process for staff to flag AI-related problems (e.g., bias, errors, suspected breaches) to IT or administrators.
Age Controls	Policies or technical measures that set minimum ages or restrict access to GenAI services for younger students.
UNESCO Guidance (2023)	UNESCO's recommendations on generative AI in education and research, including a suggested minimum age of 13.
Network-Wide Content Filtering	Controls (e.g., DNS filtering, firewalls) applied across student networks to block inappropriate or risky content.
DNS Proxy	A DNS service that forwards queries while applying filtering and logging policies at the domain-resolution layer.
Firewall	A network security device or service that permits or blocks traffic based on rules, used to enforce GenAI access policies.
Network Segregation	The separation of networks (e.g., student vs. staff) to apply different controls and reduce risk.
Policy Review Cadence	The recommended frequency (e.g., annually) to revisit and update AI policies and training as technology and laws evolve.
Approval List	An inventory of GenAI tools categorized as approved or restricted, maintained and updated by the school.
Data Handling Guidelines	Institutional procedures for classifying, anonymizing, and protecting data used with GenAI tools.
Embedded AI Features	AI capabilities integrated into operating systems or productivity suites (e.g., Copilot in Windows, AI in Google Workspace).

Productivity AI Features	GenAI functions in tools like Docs or Word that draft, summarize, or assist with writing and analysis.
Security Vulnerabilities	Weaknesses that could lead to data leaks or misuse when interacting with GenAI or related services.
Real-Time Monitoring	Continuous observation by tools (e.g., DLP) to detect and block sensitive data disclosure as it occurs.
Clipboard Monitoring	The inspection of copied/pasted content to prevent accidental exposure of sensitive information.
Sensitive Task Restrictions	The policy to avoid using public/free AI tools for any task involving sensitive or confidential data.
Compliance	Adherence to legal, regulatory, and policy requirements (e.g., GDPR, COPPA) when using GenAI tools.

End of Document

Part III :

Typical Incident Response Procedures for Schools

Incident Response Workflows

Version 1.0

This document is intended as a guide for reference only. Schools should review the recommendations and adapt them as needed to suit their own environment, resources, and requirements. The author does not accept responsibility for any actions taken based on this guide.

Version History

Version Date	Version Number	Description of changes	Author

Table of Contents

1. Ransomware Attacks

A ransomware attack is a malicious event where an attacker encrypts a school's files, making them inaccessible, and demands a ransom for their release. The response prioritizes immediate isolation of affected systems to prevent the spread and relies on restoring data from secure, offline backups rather than paying the ransom. Post-incident activities focus on identifying the initial vulnerability and assessing whether sensitive data was exfiltrated before encryption.

1.1 Preparation

1. **Establish/Maintain CIRT:** Define a core Cyber Incident Response Team (CIRT) with clear roles.
2. **Backups:** Maintain regular, automated backups of all critical data. Crucially, ensure at least one copy is offline/air-gapped and immutable.
3. **Test Backups:** Regularly test data restoration to ensure backups are viable.
4. **Tools:** Deploy and maintain Endpoint Detection and Response (EDR) or robust antivirus solutions. Use email filtering to block malicious attachments.
5. **Training:** Train staff to identify phishing emails and suspicious links, as these are common entry points.

1.2 Detection

1. **Initial Detection:** Reports of inaccessible files, new file extensions, ransom notes appearing on screens, or antivirus alerts for ransomware activity.
2. **Analysis:** Confirm the incident is ransomware. Identify the scope (which systems/servers are affected?). Use EDR/AV logs to identify the initial point of compromise if possible. **Do not click on any links in the ransom note.**

1.3 Containment

1. **Isolate Immediately:** Disconnect affected devices from the school network (unplug Ethernet cable, disable Wi-Fi). Do not turn them off, as this can lose valuable forensic data.
2. **Segment Network:** If the attack is widespread, consider taking the entire network segment (e.g., student network) or the whole school network offline to prevent further spread.

3. **Disable Accounts:** Disable the user account associated with the initial infection. Change passwords for all administrative and service accounts as a precaution.

1.4 Eradication & Recovery

1. **Consult Experts:** Inform your IT provider or a cybersecurity expert. Do not attempt to pay the ransom (as advised by NCSC/ACSC).
2. **Eradicate:** Wipe and re-image all affected systems from a known-good "golden image". Do not just run an antivirus scan.
3. **Restore:** Restore data from the most recent, tested, and clean offline backup. Ensure the backup predates the initial infection time ("dwell time").
4. **Patch:** Identify and patch the vulnerability that allowed the attack (e.g., unpatched software, weak RDP credentials).

1.5 Post-Incident Activity

1. **Report:** Report the incident to relevant authorities (e.g., Police, UK's Action Fraud/NCSC, Australia's ReportCyber).
2. **Assess Data Breach:** Determine if personal data was accessed or exfiltrated. If so, report to the data protection authority (e.g., UK's ICO, Office of the Australian Information Commissioner - OAIC) and notify affected individuals (parents/staff) as required.
3. **Lessons Learned:** Conduct a post-incident review to identify weaknesses in security controls and improve the response plan.

2. Phishing & Malware Infections

This incident typically begins with a deceptive phishing email that tricks a user into installing malware or revealing their credentials. The response is focused on containing the threat to a single device by isolating it from the network, resetting the compromised user's password, and centrally removing the malicious email from other mailboxes. Recovery involves cleaning or reimaging the device, and post-incident efforts are geared towards user communication and targeted training to prevent recurrence.

2.1 Preparation

1. **Technical Controls:** Implement strong email filtering (anti-spam, anti-phishing). Use up-to-date endpoint antivirus/anti-malware. Block known malicious websites via DNS filtering.
2. **User Training:** Conduct regular, mandatory cybersecurity awareness training for all staff focusing on identifying phishing attempts.
3. **Reporting Process:** Establish a simple, clear process for users to report suspected phishing emails (e.g., forward to a specific IT email address).
4. **Least Privilege:** Ensure users only have the access rights necessary for their roles.

2.2 Detection

1. **Initial Detection:** User reports a suspicious email, clicks a link, or opens an attachment. Antivirus software alerts on a threat. A device begins acting erratically (slow, pop-ups).
2. **Analysis:** The IT team examines the reported email's headers and content without clicking links. They analyse the malware signature from the AV alert to understand its nature (e.g., keylogger, info-stealer, trojan).

2.3 Containment

1. **Isolate Device:** Immediately disconnect the user's device from the network.
2. **Reset Credentials:** Force a password reset for the affected user's account, as their credentials may have been compromised.
3. **Block Indicators:** Block the sender's email address and any malicious domains/IPs found in the phishing email at the network firewall or email gateway.
4. **Scan Mailboxes:** Search all school mailboxes for other instances of the same phishing email and delete them centrally.

2.4 Eradication & Recovery

1. **Eradicate:** Perform a full system scan with reputable antivirus/anti-malware tools. For high-risk infections (like credential stealers), the safest option is to wipe and re-image the device.
2. **Verify Integrity:** Check the device for persistence mechanisms (e.g., scheduled tasks, registry changes) that the malware may have installed.
3. **Recover:** Restore any corrupted or lost user data from a clean backup if necessary. Reconnect the cleaned/rebuilt device to the network.

2.5 Post-Incident Activity

1. **Communication:** Send an alert to all staff with details of the phishing campaign (e.g., subject line, sender) and remind them not to engage with it.
2. **Review:** Analyse why the phishing email bypassed filters and adjust rules if possible.
3. **Targeted Training:** Use the incident as a real-world example in future training. The user who reported it should be acknowledged positively. If a user fell for it, provide them with supportive, remedial training.

3. Lost/Stolen Devices

This incident involves the physical loss or theft of a school-owned device, creating an immediate risk to any sensitive data stored on it. The response is a race against time, centered on using a Mobile Device Management (MDM) solution to remotely lock or wipe the device's data. Containment also involves revoking the user's account access to prevent misuse of credentials. The post-incident assessment is crucial for determining if a notifiable data breach has occurred, which depends heavily on whether the device was encrypted.

3.1 Preparation

1. **Asset Inventory:** Maintain an accurate inventory of all school-owned devices (laptops, tablets).
2. **Technical Controls:** Enforce mandatory full-disk encryption (e.g., BitLocker for Windows, FileVault for macOS) on all portable devices.
3. **MDM:** Enrol all mobile devices in a Mobile Device Management (MDM) solution that allows for remote lock and wipe capabilities.
4. **Policy & Training:** Have a clear policy requiring staff and students to report lost or stolen devices immediately. Train them on this procedure.

3.2 Detection

1. **Initial Detection:** A staff member or student reports that their school-issued device is lost or has been stolen.
2. **Analysis:** Immediately confirm the user's identity and the details of the lost device from the asset inventory. Determine what kind of data was likely on the device (e.g., student records, sensitive emails) and whether it was encrypted.

3.3 Containment

1. **Remote Lock/Wipe:** Immediately use the MDM solution to trigger a remote lock on the device to prevent access. If the device is unlikely to be recovered or contains highly sensitive data, trigger a remote wipe.
2. **Revoke Access:** Disable the user's school account temporarily to prevent access to cloud services (email, shared drives).
3. **Change Passwords:** Force a password reset for the user.

3.4 Eradication & Recovery

1. **Eradicate:** The remote wipe action serves as eradication of the data on the lost device. Mark the device as "lost/stolen" in the asset inventory.

2. **Recover:** Provision a new, secure device for the user. Restore their data from cloud services or backups onto the new device. Re-enable their school account.

3.5 Post-Incident Activity

1. **Report to Police:** If the device was stolen, advise the user to report the theft to the police and obtain a crime reference number.
2. **Assess Data Breach:** This is a physical data breach. If the device was not encrypted and contained personal data, it is a reportable incident. Notify the data protection authority (ICO/OAIC) and affected individuals as required by law.
3. **Review Policy:** Review physical security and device handling policies to see if improvements can be made.

4. Accidental Data Disclosure

This type of incident is typically caused by human error, such as sending an email with sensitive information to the wrong recipient or misconfiguring file sharing permissions. The response is non-technical and focuses on communication: attempting to recall the message, contacting the unintended recipient to request and confirm deletion of the data, and revoking access if the disclosure occurred via a cloud sharing link. Post-incident steps involve assessing the risk of harm to determine if a formal data breach notification is required and providing supportive, remedial training to the individual involved.

4.1 Preparation

1. **Data Classification:** Establish a simple data classification policy (e.g., Public, Internal, Confidential) and train staff on it.
2. **Training:** Train staff on common mistakes, such as using 'Reply All' inappropriately, sending emails to the wrong recipient, or misconfiguring file sharing permissions.
3. **DLP Tools:** If possible, implement basic Data Loss Prevention (DLP) rules in your email system to warn users before they send emails containing sensitive keywords (e.g., "student ID") outside the school.

4.2 Detection

1. **Initial Detection:** A user self-reports that they have sent an email with sensitive data to the wrong person, or a recipient notifies the school they have received data in error.
2. **Analysis:** Quickly verify the incident. Identify exactly what data was disclosed, who it was sent to (internal/external), and the sensitivity of the information.

4.3 Containment

1. **Attempt Recall:** Immediately attempt to recall the email (understanding this is not always effective, especially for external recipients).
2. **Contact Recipient:** Contact the unintended recipient(s) by phone or a separate email, explain the error, and formally request that they delete the information and confirm deletion in writing.
3. **Revoke Access:** If the data was shared via a cloud link (e.g., SharePoint, Google Drive), immediately revoke access to the file or folder.

4.4 Eradication & Recovery

1. **Eradicate:** Eradication is achieved when you receive confirmation that the unintended recipient has deleted the data. Document this confirmation.
2. **Recover:** No technical recovery is needed. The focus is on procedural recovery: ensuring the original data is secured and the user understands the mistake.

4.5 Post-Incident Activity

1. **Assess Breach:** This is a data breach. The Incident Lead must assess the risk of harm to the individuals whose data was disclosed.
2. **Report:** Based on the risk assessment, report the breach to the data protection authority (ICO/OAIC) if it meets the mandatory reporting threshold.
3. **Notify:** Inform the affected individuals (or their parents) about the breach, the potential impact, and the steps taken to mitigate it.
4. **Training:** Provide remedial training to the staff member involved and use the anonymised scenario in wider staff training.

5. Website Defacement

A website defacement is an attack where an unauthorized party gains access and alters the visual content of the school's public website, often for reputational damage. The immediate response is to take the website offline and replace it with a static maintenance page to contain the damage. Recovery is not about fixing the defaced content, but about restoring the entire site from a known-clean backup after identifying and patching the vulnerability that allowed access. Post-incident activities focus on hardening website security to prevent re-entry.

5.1 Preparation

1. **Secure Access:** Enforce strong, unique passwords and Multi-Factor Authentication (MFA) for all website admin accounts. Limit the number of admin accounts.
2. **Patching:** Keep the website's Content Management System (CMS), themes, and plugins fully patched and updated at all times.
3. **Backups:** Maintain regular, automated backups of the website files and database. Store them separately from the web server.
4. **Monitoring:** Use a file integrity monitoring service to alert on unauthorized changes to website files.

5.2 Detection

1. **Initial Detection:** The school is alerted by a staff member, student, parent, or through website monitoring that the website content has been altered with unauthorized messages or images.
2. **Analysis:** Verify the defacement. Take screenshots as evidence. Check server logs to identify suspicious IP addresses or activity around the time of the defacement.

5.3 Containment

1. **Take Site Offline:** Immediately take the website offline and replace it with a static, pre-prepared maintenance page (e.g., "Our website is temporarily unavailable. We are working to restore it soon."). This prevents further reputational damage.
2. **Preserve Evidence:** Take a full backup/snapshot of the defaced site for later investigation before making any changes.

5.4 Eradication & Recovery

1. **Identify Vulnerability:** Analyse logs and files to find the point of entry (e.g., a vulnerable plugin, compromised password).
2. **Eradicate & Recover:** Delete all website files from the server. Restore the website files and database from the most recent known-clean backup. **Do not** just try to edit the defaced pages.
3. **Secure:** Change all administrative, database, and FTP passwords. Apply the patch for the vulnerability that was exploited. Scan the restored site for any remaining backdoors.
4. **Bring Online:** Once secure, bring the restored website back online.

5.5 Post-Incident Activity

1. **Review:** Conduct a review of the incident to confirm the root cause.
2. **Improve Security:** Implement additional security measures based on the review, such as a Web Application Firewall (WAF) or more stringent access controls.
3. **Communication:** Inform the school community (if necessary) that the website issue has been resolved and security has been enhanced.

6. Denial-of-Service (DoS) Attacks

A Denial-of-Service (DoS) attack aims to make critical online services, such as the school's website or internet connection, unavailable by overwhelming them with malicious traffic. Unlike other incidents, the primary response is not technical but procedural: immediately contacting the school's Internet Service Provider (ISP) or hosting provider, as they have the network-level tools to filter and block the attack traffic. The school's role is to monitor the restoration of services and communicate internally about the disruption, while post-incident analysis is conducted with the provider to implement stronger preventative measures.

6.1 Preparation

The Software Asset List should be updated in event of:

1. **Know Your Provider:** Have the 24/7 technical support contact details for your Internet Service Provider (ISP) and website hosting provider readily available.
2. **Use Protection Services:** For critical services like the school website, use a cloud-based DNS/proxy service (e.g., Cloudflare) that includes DDoS mitigation.
3. **Scalable Hosting:** Host critical services on platforms that can scale to absorb minor traffic spikes.
4. **Network Monitoring:** Have basic network traffic monitoring in place to identify unusual spikes.

6.2 Detection

1. **Initial Detection:** Reports that the school website, learning platform, or entire internet connection is offline or unusably slow. Monitoring tools show an extremely high volume of incoming network traffic.
2. **Analysis:** Differentiate between a simple outage and a DoS attack. A DoS is indicated by a massive, sustained flood of traffic from many (DDoS) or few (DoS) sources, overwhelming the server or network link.

6.3 Containment

1. **Contact Provider: This is the most critical step.** Immediately contact your ISP or website hosting provider. Inform them you believe you are under a DoS attack. They have the network-level tools to mitigate it ("blackholing" traffic, rate limiting).
2. **Enable Mitigation:** If you use a service like Cloudflare, enable its "I'm Under Attack" mode.
3. **Communicate Internally:** Inform staff that key services are down due to a suspected network attack and that you are working with the provider to resolve it.

6.4 Eradication & Recovery

1. **Work with Provider:** The provider will perform the eradication by filtering out the malicious traffic. Your role is to monitor the status of your services.
2. **Recovery:** As the provider's mitigation takes effect, services will gradually become available again. Test key services (website, email) to confirm they are operational.

6.5 Post-Incident Activity

1. **Post-Attack Analysis:** Debrief with your provider to understand the nature and scale of the attack.
2. **Implement Recommendations:** Implement any security recommendations from your provider to better withstand future attacks.
3. **Communication:** Inform the school community that services have been restored. It is not always necessary to specify the cause was a DoS attack; "technical difficulties" or a "network disruption" is often sufficient.

Appendices

Glossary of Terms

Term	Definition
Accidental Data Disclosure	An incident where sensitive information is unintentionally exposed to an unauthorized individual, often through human error such as sending an email to the wrong recipient.
Air-Gapped Backup	A backup copy that is physically disconnected from the network, making it immune to online attacks like ransomware.
Asset Inventory	A detailed and up-to-date list of all school-owned technology assets, such as laptops, tablets, and servers, which is crucial for managing and responding to incidents.
Backdoor	A hidden method of bypassing normal authentication or security controls, often left by an attacker to regain access to a system after an initial compromise.
Blackholing	A DoS mitigation technique where an ISP directs all traffic destined for the attacked IP address into a "black hole," effectively dropping it before it reaches the school's network.
Containment	The phase of incident response focused on stopping the spread of an attack and preventing further damage, such as by isolating affected devices from the network.
Content Management System (CMS)	The software platform used to create and manage the content of a website (e.g., WordPress, Joomla). It is a common target for attackers if not kept updated.
Cyber Incident Response Team (CIRT)	A pre-designated group of individuals with defined roles (e.g., Incident Lead, Technical Lead) responsible for managing the response to a cybersecurity incident.
Data Classification	The process of categorizing data based on its sensitivity (e.g., Public, Internal, Confidential) to determine the appropriate level of protection.
Data Exfiltration	The unauthorized act of copying or transferring data from a network. Modern ransomware often exfiltrates data before encrypting it, creating a data breach.
Data Loss Prevention (DLP)	Technology or processes designed to detect and prevent sensitive data from being sent outside the organization's network.
Data Protection Authority	A government agency responsible for enforcing data privacy laws and handling data breach notifications (e.g., the ICO in the UK, the OAIC in Australia).
Denial-of-Service (DoS) / Distributed Denial-of-Service (DDoS)	An attack that aims to make a service (like a website or internet connection) unavailable by overwhelming it with a flood of malicious traffic from a single (DoS) or multiple (DDoS) sources.

DNS Filtering	A security measure that blocks access to known malicious websites by preventing the user's device from resolving the website's domain name to an IP address.
Dwell Time	The period of time from the initial compromise of a network to the moment the attack is detected. Understanding dwell time is critical for ransomware recovery to ensure a backup is restored from a point before the attacker was present.
Endpoint Detection and Response (EDR)	An advanced form of antivirus software that provides real-time monitoring and analysis of endpoint devices to detect, investigate, and respond to threats.
Eradication	The phase of incident response focused on completely removing all traces of the threat from the environment (e.g., deleting malware, patching vulnerabilities).
File Integrity Monitoring (FIM)	A security process or tool that monitors critical system and website files to detect and alert on any unauthorized changes.
Forensic Image	An exact, bit-for-bit copy of a storage drive, created to preserve the state of an affected system for investigation without altering the original evidence.
Full-Disk Encryption	A security control that encrypts all data on a device's hard drive, making the data unreadable without the correct password if the device is lost or stolen.
Golden Image	A pre-configured, secure, and clean template of an operating system and its applications, used to rapidly wipe and rebuild a compromised system.
Immutable Backup	A backup that is stored in a way that it cannot be altered or deleted, even by an administrator, providing a strong defence against ransomware that targets backups.
Indicators of Compromise (IOCs)	Pieces of forensic data, such as malicious IP addresses, file hashes, or domain names, that identify a potential security breach.
Least Privilege (Principle of)	The security concept of ensuring that users are only given the minimum levels of access—or permissions—needed to perform their job functions.
Malware	Malicious software designed to disrupt operations or gain unauthorized access to computer systems, including viruses, trojans, spyware, and keyloggers.
Mobile Device Management (MDM)	A software solution that allows IT administrators to centrally control, secure, and enforce policies on mobile devices like tablets and smartphones.
Multi-Factor Authentication (MFA)	A security measure that requires users to provide two or more verification factors to gain access, such as a password and a code from their phone.
Offline Backup	A backup copy stored on a device or media that is not connected to the network, protecting it from being encrypted or deleted during a ransomware attack.
Persistence Mechanism	A technique used by malware to automatically restart itself or maintain access after a system reboot (e.g., creating a scheduled task or a registry entry).

Phishing	A type of social engineering attack where an attacker sends a fraudulent message, often an email, designed to trick a person into revealing sensitive information or deploying malware.
Physical Data Breach	A security incident resulting from the loss or theft of a physical device (like a laptop) that contains sensitive or personal data.
Ransomware	A type of malware that encrypts files on a device, making them inaccessible, and then demands a ransom payment to restore access.
Rate Limiting	A DoS mitigation technique that controls the amount of incoming traffic from a source in a given period, helping to reduce the impact of a flood attack.
Recovery	The phase of incident response focused on restoring systems and data to normal operation after a threat has been eradicated.
Remedial Training	Targeted, supportive training provided to a user after a security incident to reinforce best practices and prevent a recurrence.
Remote Lock / Wipe	Functions within an MDM system that allow an administrator to remotely lock a lost device to prevent access or permanently erase all data from it.
Static Maintenance Page	A simple, pre-prepared web page that is displayed to visitors when a website is taken offline for maintenance or during an incident like a defacement.
Web Application Firewall (WAF)	A security tool that filters and monitors HTTP traffic between a web application and the internet, helping to protect against common web-based attacks.
Website Defacement	An attack on a website that illegally changes its visual appearance, typically by replacing the original content with the attacker's own messages or images.

1. Roles and Responsibilities

1. Cyber Incident Response Team (CIRT)

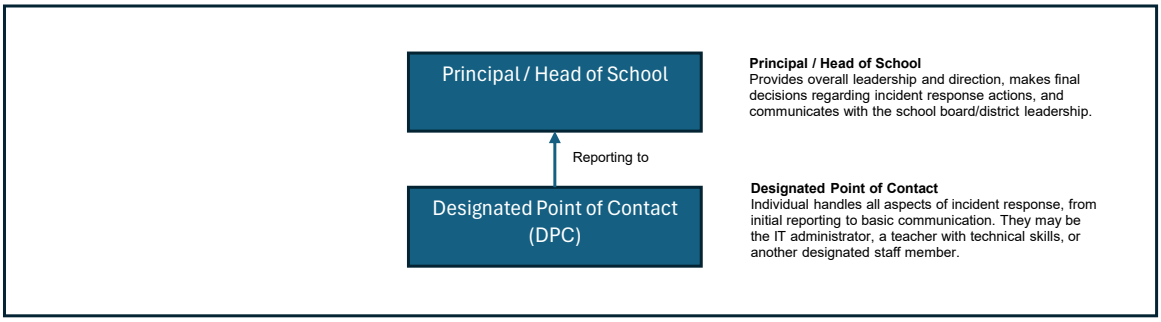
What is a CIRT?
A Cyber Incident Response Team (CIRT) is a group of individuals responsible for handling and responding to cybersecurity incidents. In a school setting, this includes events like data breaches, malware infections, phishing attacks, denial-of-service attacks, and other cyber threats. A CIRT's primary goal is to minimize the impact of these incidents, protect student and staff data, and ensure the continuity of learning.

Why is a CIRT Important for Schools?
Schools are increasingly reliant on technology, making them vulnerable to cyberattacks. A well-defined CIRT structure ensures a coordinated and effective response to incidents, minimizing disruption and damage. It also demonstrates a commitment to data security and builds trust with the school community.

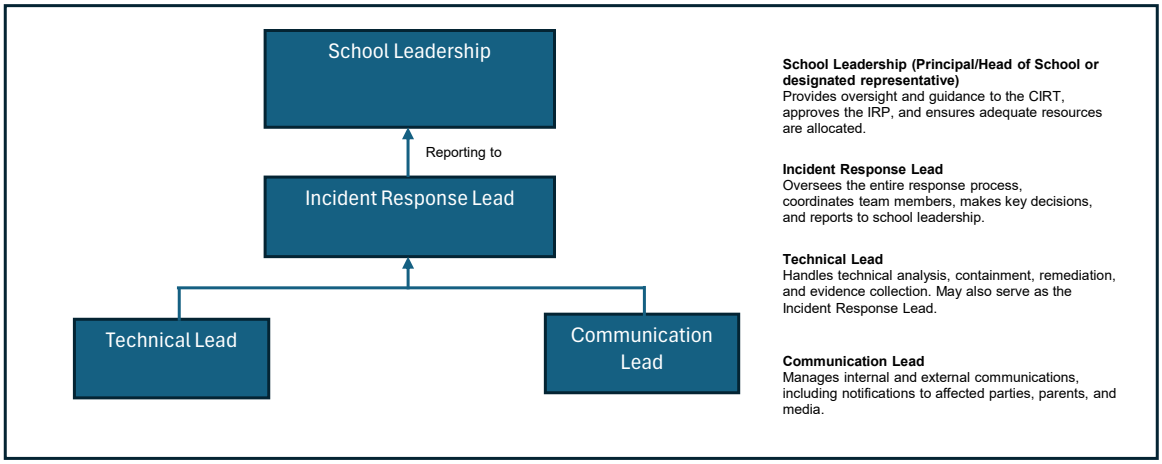
Tiered CIRT Structures for Schools:

The following tiered structure provides a framework for schools to establish a CIRT based on their size, resources, and specific needs. These tiers offer flexibility, allowing schools to adapt the model to their context.

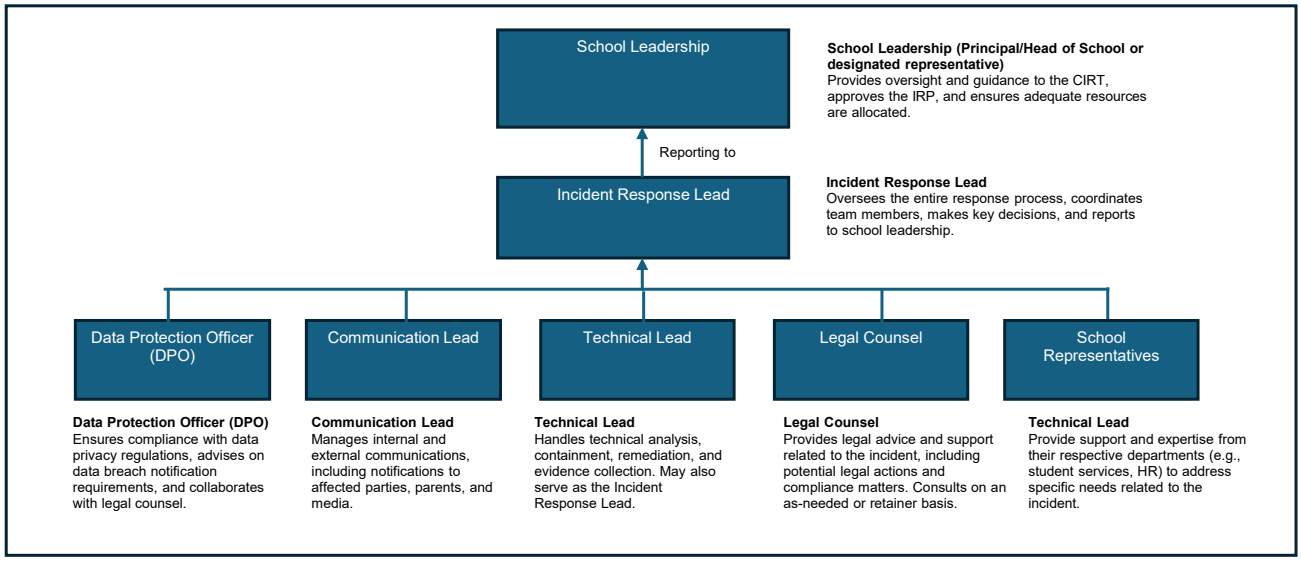
Tier 1: Simplified School CIRT (Small School/Limited Resources)



Tier 2: Formalized School CIRT (Larger School/Moderate Resources)



Tier 3: Comprehensive School CIRT



Implementing the CIRT structure:

1. Assess your school's needs and resources: Determine which tier is most appropriate based on your school's size, budget, and technical expertise.

2. Identify and train CIRT members: Select individuals with the necessary skills and provide them with appropriate training on incident response procedures.

3. Develop an Incident Response Plan (IRP): A comprehensive IRP outlines the steps to be taken in the event of a cyber incident. It should include roles and responsibilities, communication protocols, and technical procedures.

4. Regularly test and update the IRP: Conduct drills and exercises to ensure the CIRT is prepared to handle real-world incidents. Review and update the IRP at least annually or as needed.

By following these steps, schools can establish a robust CIRT structure that effectively protects their data and ensures a swift and coordinated response to cyber threats. This information, along with the tiered structure, should be clearly documented and readily accessible to all relevant staff.

1. Roles and Responsibilities

2. CIRT Roles and Responsibilities

This table outlines the key roles and responsibilities within a school-based Computer Incident Response Team (CIRT). The roles described below can be adapted to fit the specific needs and resources of individual schools. Some roles may be combined, and external expertise may be leveraged as needed.

This structure is designed to be scalable and adaptable. Smaller schools with limited resources may consolidate roles, while larger schools or districts might have more specialized roles. It's crucial to clearly define these roles and responsibilities *before* an incident occurs to ensure a coordinated and effective response.

CIRT Role	Tier Applied	Responibilities	Requirements
School Leadership (Principal/Head of School or designated representative)	1,2,3	Provides overall leadership/direction for CIRT. Approves IRP, allocates resources, communicates with school board/district leadership.	Understanding of school operations, risk management, data security best practices.
Designated Point of Contact (DPC) / Incident Response Lead	1,2,3	Oversees the entire incident response process, coordinates team members, makes key decisions, and reports to school leadership. Serves as the primary point of contact for external agencies.	Strong leadership, communication, organizational skills. Knowledge of cybersecurity best practices and incident response frameworks.
Technical Lead	2,3	Handles technical aspects: analysis, containment, eradication, recovery. Manages technical staff/vendors.	Deep technical expertise in network security, system administration, data recovery. Experience with security tools/technologies.
Communications Lead	2,3	Develops/executes communication strategies for internal/external stakeholders. Manages media relations/public communications.	Excellent communication/writing skills. Experience with crisis communication/public relations.
Data Protection Officer (DPO)	3	Ensures compliance with data privacy regulations (PDPO, etc.). Advises on data breach notifications. Collaborates with legal counsel.	Deep understanding of data privacy laws and regulations. Experience with data governance and compliance. Legal background helpful.
School Department Representatives (e.g., Student Services, HR, Instruction)	3	Provide support and expertise from their respective departments to address specific needs related to the incident (e.g., student counseling, staff training, curriculum adjustments).	Knowledge of their department's functions and how they relate to cybersecurity incidents. Ability to collaborate effectively with the CIRT.
Legal Counsel (as needed)	3	Provides legal advice/support related to the incident, including potential legal actions/compliance matters.	Expertise in data privacy law, contract law, negligence and liabilities, etc.

2. Cyber Incident Severity Level Classification

2.1. Incident Severity Classification

CIR Manager should review the reported security incident and assess the severity. Below is the incident severity level classifications and definitions.

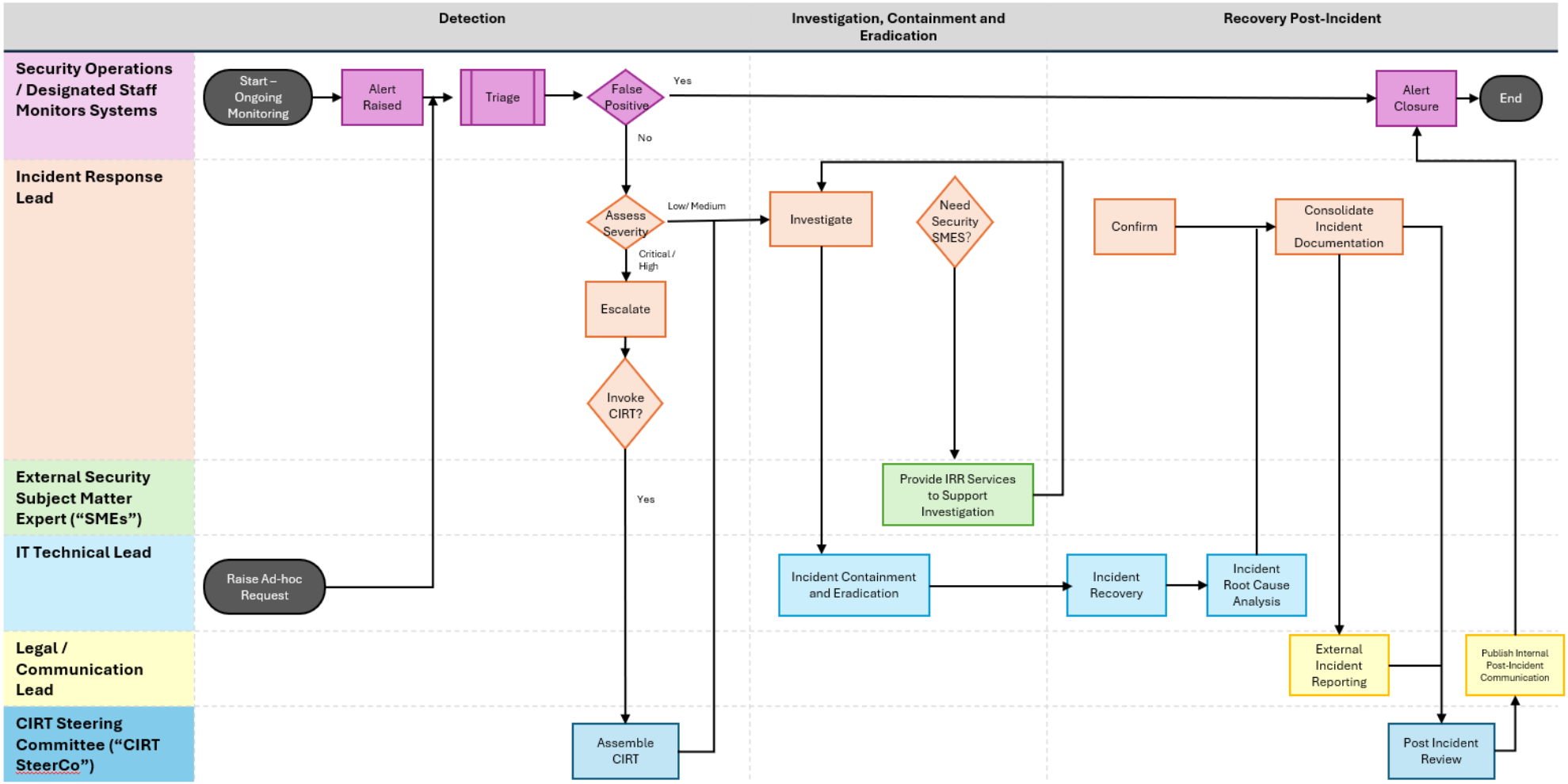
The classification is based on the MITRE category of the security incident, and the potential risk and/or impact on the University's critical assets. The disruption on operations and impact on confidentiality, integrity and availability of the University's assets is also considered.

Severity	Description of Incident (Examples)	Potential Risk and /or Impact
Critical	Ransomware Attack: Critical systems are encrypted and inaccessible, impacting essential school operations. Data is being held hostage.	- Significant disruption to teaching, learning, and administrative functions. Financial losses due to ransom payments and recovery efforts. - Reputational damage and loss of trust. - Legal and regulatory consequences.
	Major Data Breach: Large-scale theft of sensitive student or staff data, posing significant legal and reputational risks.	- Identity theft and financial fraud for affected individuals. - Legal and regulatory penalties. - Reputational damage and erosion of public trust. - Costs associated with credit monitoring and identity theft repair services.
	System Outage (critical): Essential systems are completely unavailable, severely disrupting school operations. This could be due to a targeted attack or a catastrophic failure.	- Inability to access critical systems (student information, grading, communication). - Cancellation of classes or school closure. - Safety and security risks if emergency notification systems are affected. - Financial losses due to lost productivity and recovery costs.
High	Malware Infection (spreading): Malware is actively spreading within the school network, potentially compromising multiple systems.	- Data loss or corruption. - System slowdowns or crashes. - Spread of infection to other connected networks. - Disruption to school operations and learning activities.
	Targeted Intrusion: Evidence of hackers actively targeting school systems, attempting to gain access to sensitive data or disrupt operations.	- Data breaches and theft of sensitive information. - System damage or disruption. - Reputational damage and loss of trust. - Legal and regulatory consequences.
	System Outage (major): Important systems are unavailable, disrupting key school functions.	- Disruption to specific school functions (e.g., internet access, email, library systems). - Limited access to student information or grades. - Delays in communication and administrative tasks. - Frustration and inconvenience for students, staff, and parents.
Medium	**Phishing Attack (successful):** Credentials or sensitive information have been compromised through a phishing attack.	- Unauthorized access to school systems and data. - Potential for further attacks (e.g., malware installation, data breach). - Compromised accounts used to send spam or phishing emails. - Reputational damage if the compromised account is used for malicious purposes.
	Unauthorized Access (limited): Evidence of unauthorized access to a specific system or account, but no indication of widespread compromise.	- Potential for data breaches or system damage. - Need to investigate the extent of the unauthorized access. - Need to strengthen security measures to prevent future incidents.
	Security Misconfiguration: A security vulnerability has been identified due to a system misconfiguration.	- Increased risk of cyberattacks and data breaches. - System instability or unexpected behavior. - Need to reconfigure systems to address the vulnerability.
Low	Suspicious Activity: Unusual activity has been observed, but it's unclear whether it represents a genuine threat.	Potential Security Breach - May indicate early stages of an attack or malicious activity. - Misuse of Resources: Unauthorized use of school computers or network for non-educational purposes. Violation of Acceptable Use Policy: Students or staff engaging in prohibited online activities.
	Security Alert (false positive): A security system generated an alert that, upon investigation, turned out to be benign.	- Complacency: Repeated false positives can lead to alerts being ignored in the future, potentially missing a real threat. - Consumes time and resources to investigate. - Can cause unnecessary stress and disruption. - May indicate a need to fine-tune security systems to reduce false positives.

3. Incident Response Procedure

3.1. Incident Response Flowchart

For Illustrative Purpose Only



#	Incident Type	A. Preparation	B. Detection and Analysis Phase	C. Containment	D. Eradication and Recovery	E. Post-Incident Activity
	Responsible Party	Incident Response Lead (e.g., Principal/Business Manager), Technical Lead (e.g., IT Coordinator), Communication Lead (e.g., Office Manager)	IT Staff / All Staff & Students (as reporters)	Technical Lead, Incident Response Lead	Technical Lead	Incident Response Lead, Technical Lead, Communication Lead
1	Ransomware Attacks	1. Establish/Maintain CIRT: Define a core Cyber Incident Response Team (CIRT) with clear roles. 2. Backups: Maintain regular, automated backups of all critical data. Crucially, ensure at least one copy is offline/air-gapped and immutable. 3. Test Backups: Regularly test data restoration to ensure backups are viable. 4. Tools: Deploy and maintain Endpoint Detection and Response (EDR) or robust antivirus solutions. Use email filtering to block malicious attachments. 5. Training: Train staff to identify phishing emails and suspicious links, as these are common entry points.	1. Initial Detection: Reports of inaccessible files, new file extensions, ransom notes appearing on screens, or antivirus alerts for ransomware activity. 2. Analysis: Confirm the incident is ransomware. Identify the scope (which systems/servers are affected?). Use EDR/AV logs to identify the initial point of compromise if possible. Do not click on any links in the ransom note.	1. Isolate Immediately: Disconnect affected devices from the school network (unplug Ethernet cable, disable Wi-Fi). Do not turn them off, as this can lose valuable forensic data. 2. Segment Network: If the attack is widespread, consider taking the entire network segment (e.g., student network) or the whole school network offline to prevent further spread. 3. Disable Accounts: Disable the user account associated with the initial infection. Change passwords for all administrative and service accounts as a precaution.	1. Consult Experts: Inform your IT provider or a cybersecurity expert. Do not attempt to pay the ransom (as advised by NCSC/ACSC). 2. Eradicate: Wipe and re-image all affected systems from a known-good "golden image". Do not just run an antivirus scan. 3. Restore: Restore data from the most recent, tested, and clean offline backup. Ensure the backup predates the initial infection time ("dwell time"). 4. Patch: Identify and patch the vulnerability that allowed the attack (e.g., unpatched software, weak RDP credentials).	1. Report: Report the incident to relevant authorities (e.g., Police, UK's Action Fraud/NCSC, Australia's ReportCyber). 2. Assess Data Breach: Determine if personal data was accessed or exfiltrated. If so, report to the data protection authority (e.g., UK's ICO, Office of the Australian Information Commissioner - OAIC) and notify affected individuals (parents/staff) as required. 3. Lessons Learned: Conduct a post-incident review to identify weaknesses in security controls and improve the response plan.
2	Phishing & Malware Infections	1. Technical Controls: Implement strong email filtering (anti-spam, anti-phishing). Use up-to-date endpoint antivirus/anti-malware. Block known malicious websites via DNS filtering. 2. User Training: Conduct regular, mandatory cybersecurity awareness training for all staff focusing on identifying phishing attempts. 3. Reporting Process: Establish a simple, clear process for users to report suspected phishing emails (e.g., forward to a specific IT email address). 4. Least Privilege: Ensure users only have the access rights necessary for their roles.	1. Initial Detection: User reports a suspicious email, clicks a link, or opens an attachment. Antivirus software alerts on a threat. A device begins acting erratically (slow, pop-ups). 2. Analysis: The IT team examines the reported email's headers and content without clicking links. They analyse the malware signature from the AV alert to understand its nature (e.g., keylogger, info-stealer, trojan).	1. Isolate Device: Immediately disconnect the user's device from the network. 2. Reset Credentials: Force a password reset for the affected user's account, as their credentials may have been compromised. 3. Block Indicators: Block the sender's email address and any malicious domains/IPs found in the phishing email at the network firewall or email gateway. 4. Scan Mailboxes: Search all school mailboxes for other instances of the same phishing email and delete them centrally.	1. Eradicate: Perform a full system scan with reputable antivirus/anti-malware tools. For high-risk infections (like credential stealers), the safest option is to wipe and re-image the device. 2. Verify Integrity: Check the device for persistence mechanisms (e.g., scheduled tasks, registry changes) that the malware may have installed. 3. Recover: Restore any corrupted or lost user data from a clean backup if necessary. Reconnect the cleaned/rebuilt device to the network.	1. Communication: Send an alert to all staff with details of the phishing campaign (e.g., subject line, sender) and remind them not to engage with it. 2. Review: Analyse why the phishing email bypassed filters and adjust rules if possible. 3. Targeted Training: Use the incident as a real-world example in future training. The user who reported it should be acknowledged positively. If a user fell for it, provide them with supportive, remedial training.
3	Lost or Stolen Devices	1. Asset Inventory: Maintain an accurate inventory of all school-owned devices (laptops, tablets). 2. Technical Controls: Enforce mandatory full-disk encryption (e.g., BitLocker for Windows, FileVault for macOS) on all portable devices. 3. MDM: Enrol all mobile devices in a Mobile Device Management (MDM) solution that allows for remote lock and wipe capabilities. 4. Policy & Training: Have a clear policy requiring staff and students to report lost or stolen devices immediately. Train them on this procedure.	1. Initial Detection: A staff member or student reports that their school-issued device is lost or has been stolen. 2. Analysis: Immediately confirm the user's identity and the details of the lost device from the asset inventory. Determine what kind of data was likely on the device (e.g., student records, sensitive emails) and whether it was encrypted.	1. Remote Lock/Wipe: Immediately use the MDM solution to trigger a remote lock on the device to prevent access. If the device is unlikely to be recovered or contains highly sensitive data, trigger a remote wipe. 2. Revoke Access: Disable the user's school account temporarily to prevent access to cloud services (email, shared drives). 3. Change Passwords: Force a password reset for the user.	1. Eradicate: The remote wipe action serves as eradication of the data on the lost device. Mark the device as "lost/stolen" in the asset inventory. 2. Recover: Provision a new, secure device for the user. Restore their data from cloud services or backups onto the new device. Re-enable their school account.	1. Report to Police: If the device was stolen, advise the user to report the theft to the police and obtain a crime reference number. 2. Assess Data Breach: This is a physical data breach. If the device was not encrypted and contained personal data, it is a reportable incident. Notify the data protection authority (ICO/OAIC) and affected individuals as required by law. 3. Review Policy: Review physical security and device handling policies to see if improvements can be made.
4	Accidental Data Disclosure	1. Data Classification: Establish a simple data classification policy (e.g., Public, Internal, Confidential) and train staff on it. 2. Training: Train staff on common mistakes, such as using 'Reply All' inappropriately, sending emails to the wrong recipient, or misconfiguring file sharing permissions. 3. DLP Tools: If possible, implement basic Data Loss Prevention (DLP) rules in your email system to warn users before they send emails containing sensitive keywords (e.g., "student ID") outside the school.	1. Initial Detection: A user self-reports that they have sent an email with sensitive data to the wrong person, or a recipient notifies the school they have received data in error. 2. Analysis: Quickly verify the incident. Identify exactly what data was disclosed, who it was sent to (internal/external), and the sensitivity of the information.	1. Attempt Recall: Immediately attempt to recall the email (understanding this is not always effective, especially for external recipients). 2. Contact Recipient: Contact the unintended recipient(s) by phone or a separate email, explain the error, and formally request that they delete the information and confirm deletion in writing. 3. Revoke Access: If the data was shared via a cloud link (e.g., SharePoint, Google Drive), immediately revoke access to the file or folder.	1. Eradicate: Eradication is achieved when you receive confirmation that the unintended recipient has deleted the data. Document this confirmation. 2. Recover: No technical recovery is needed. The focus is on procedural recovery: ensuring the original data is secured and the user understands the mistake.	1. Assess Breach: This is a data breach. The Incident Lead must assess the risk of harm to the individuals whose data was disclosed. 2. Report: Based on the risk assessment, report the breach to the data protection authority (ICO/OAIC) if it meets the mandatory reporting threshold. 3. Notify: Inform the affected individuals (or their parents) about the breach, the potential impact, and the steps taken to mitigate it. 4. Training: Provide remedial training to the staff member involved and use the anonymised scenario in wider staff training.

#	Incident Type	A. Preparation	B. Detection and Analysis Phase	C. Containment	D. Eradication and Recovery	E. Post-Incident Activity
5	Website Defacement	1. Secure Access: Enforce strong, unique passwords and Multi-Factor Authentication (MFA) for all website admin accounts. Limit the number of admin accounts. 2. Patching: Keep the website's Content Management System (CMS), themes, and plugins fully patched and updated at all times. 3. Backups: Maintain regular, automated backups of the website files and database. Store them separately from the web server. 4. Monitoring: Use a file integrity monitoring service to alert on unauthorised changes to website files.	1. Initial Detection: The school is alerted by a staff member, student, parent, or through website monitoring that the website content has been altered with unauthorised messages or images. 2. Analysis: Verify the defacement. Take screenshots as evidence. Check server logs to identify suspicious IP addresses or activity around the time of the defacement.	1. Take Site Offline: Immediately take the website offline and replace it with a static, pre-prepared maintenance page (e.g., "Our website is temporarily unavailable. We are working to restore it soon."). This prevents further reputational damage. 2. Preserve Evidence: Take a full backup/snapshot of the defaced site for later investigation before making any changes.	1. Identify Vulnerability: Analyse logs and files to find the point of entry (e.g., a vulnerable plugin, compromised password). 2. Eradicate & Recover: Delete all website files from the server. Restore the website files and database from the most recent known-clean backup. Do not just try to edit the defaced pages. 3. Secure: Change all administrative, database, and FTP passwords. Apply the patch for the vulnerability that was exploited. Scan the restored site for any remaining backdoors. 4. Bring Online: Once secure, bring the restored website back online.	1. Review: Conduct a review of the incident to confirm the root cause. 2. Improve Security: Implement additional security measures based on the review, such as a Web Application Firewall (WAF) or more stringent access controls. 3. Communication: Inform the school community (if necessary) that the website issue has been resolved and security has been enhanced.
6	Denial-of-Service (DoS) Attacks	1. Know Your Provider: Have the 24/7 technical support contact details for your Internet Service Provider (ISP) and website hosting provider readily available. 2. Use Protection Services: For critical services like the school website, use a cloud-based DNS/proxy service (e.g., Cloudflare) that includes DDoS mitigation. 3. Scalable Hosting: Host critical services on platforms that can scale to absorb minor traffic spikes. 4. Network Monitoring: Have basic network traffic monitoring in place to identify unusual spikes.	1. Initial Detection: Reports that the school website, learning platform, or entire internet connection is offline or unusably slow. Monitoring tools show an extremely high volume of incoming network traffic. 2. Analysis: Differentiate between a simple outage and a DoS attack. A DoS is indicated by a massive, sustained flood of traffic from many (DDoS) or few (DoS) sources, overwhelming the server or network link.	1. Contact Provider: This is the most critical step. Immediately contact your ISP or website hosting provider. Inform them you believe you are under a DoS attack. They have the network-level tools to mitigate it ("blackholing" traffic, rate limiting). 2. Enable Mitigation: If you use a service like Cloudflare, enable its "I'm Under Attack" mode. 3. Communicate Internally: Inform staff that key services are down due to a suspected network attack and that you are working with the provider to resolve it.	1. Work with Provider: The provider will perform the eradication by filtering out the malicious traffic. Your role is to monitor the status of your services. 2. Recovery: As the provider's mitigation takes effect, services will gradually become available again. Test key services (website, email) to confirm they are operational.	1. Post-Attack Analysis: Debrief with your provider to understand the nature and scale of the attack. 2. Implement Recommendations: Implement any security recommendations from your provider to better withstand future attacks. . Communication: Inform the school community that services have been restored. It is not always necessary to specify the cause was a DoS attack; "technical difficulties" or a "network disruption" is often sufficient.

Appendix - Criteria / Considerations to Trigger CIRT

This table provides general criteria for considering when to activate a school's incident response plan and potentially involve external support. Each school must adapt these criteria to its specific context, resources, and risk tolerance. Consultation with legal counsel and IT professionals is recommended.

Key Factor	
Scope of Impact	**Is the school the only affected party?** Likely, unless the attack targets a shared service provider. Investigate to confirm. **How many systems or users are affected?** A single compromised account vs. a widespread infection requires different responses. **What type of data is involved?** Sensitive student data breaches require higher levels of response.
Potential Consequences	**Financial Impact:** Recovery costs, potential fines for data breaches (depending on local regulations), and disruption to educational services. **Operational Impact:** Disruptions to teaching, learning, administrative tasks, and communication. **Reputational Impact:** Damage to the school's image and public trust.
Impact of Stakeholders	**Staff and Teachers:** Disrupted lesson planning, grading, communication, and increased workload. **Students:** Disruptions to learning, access to resources, and grading. **Partnering Institutions:** Impact on other schools, libraries, or organizations relying on shared systems. **Parents:** Concerns and communication needs.
Legal and Regulatory Obligations	**Data Breach Notification Laws:** Determine if the incident triggers mandatory reporting requirements. **Contracts and Agreements:** Review relevant contracts for incident response obligations. **School Policies:** Ensure compliance with internal policies and procedures.

Appendix – Cyber Incident Response Team Contact List

Please complete this contact list with the names, roles, and contact information for all members of the Incident Response Team. This list should be readily accessible during an incident and updated regularly.

Role	Name	Primary Phone	Secondary Phone	E-mail
Designated Point of Contact (Tier 1) / Incident Response Lead (Tier 2/3)				
Technical Lead (Tier 2/3)				
Communications Lead (Tier 2/3)				
IT Administrator/Support				
Principal/Superintendent				
External IT Service Provider				
Law Enforcement (Non-Emergency)				
Legal Councel (if applicable)				
[Other - Customize]				

Appendix - Regulatory and Law Enforcement Contact

	When to report	Contact
Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)	- If the incident is a potenital multiple point attack targeting at school	Tel: 8105 6060, Fax: 8105 9760 Email address: hkcert@hkcert.org Online form: https://www.hkcert.org/form/incident-report-end-user-sme/entry
Is the school the only party affected by this issue or incident?	Likely, unless the attack targeted a shared service provider used by multiple schools. This needs investigation.	Tel: 2860 5012 e-Report Centre: https://www.police.gov.hk/ppp_en/contact_us.html
Privacy Commissioner for Personal Data (PCPD)	- If personal data of students, staff, or parents is compromised - Especially if the breach could cause harm or distress to affected individuals	If personal data is involved in a security incident, B/D should report the case to PCPD as soon as possible by using the data breach notification form available at PCPD's web site: (https://www.pcpd.org.hk/english/resources_centre/publications/forms/files/DBN_e.pdf). The data breach notification form can also be submitted online through PCPD's website (https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn_form.html).

Appendix - Incident Handling Form

I. General Information			
Incident Handler's Information			
Is the school the only party affecte		Location:	
Title:		Department:	
Office / Mobile Number:		Incident Date/Time:	
Impact on staff and teachers			
Name:		Date / Time:	
Title:		Office / Mobile Number:	
II. Incident Details			
Type of Incident:	☐ Data Leakage ☐ Website Defacement ☐ Phishing Attack ☐ Ransomeware Attack ☐ Distributed Denial of Service (DDOS) ☐ System Compromise/Operation Impairment ☐ Others: _____		
Incident Description / Findings / Actions Taken:			
Data Involved:	☐ Personal Data (Staff / Student) ☐ Operationl Data ☐ Others ☐ None		
Estimated Number of Affected Records Compromised:	☐ >1,000 rows ☐ <1,000 to >500 rows ☐ <500 to >100 rows ☐ <100 rows ☐ If exact number is known: _____ ☐ None		
Estimated Number of Affected Users/GB of Data:	☐ >5,000 ☐ <5,000 to >500 ☐ <500 ☐ If exact number is known: _____ ☐ None		

Affected Staff / Student List:

#	Name	Department/Location	Contact	Remarks

Observed Impact:	☐ Financial Impact ☐ Reputational Impact ☐ Legal/Regulatory Compliance Impact ☐ Operational Impact ☐ Others: _____
Impact Details and Potential Risk (s):	
III. Follow-Up Actions	
Follow up Action(s) Taken (if any):	
Require External Expertise?	☐ Yes ☐ No
Preferred External Expert (if any)	

Appendix A – Action Log

#	Action/Issue	Responsible Party	Date/Time	Status

Appendix - Post Incident Evaluation

Post-Incident Evaluation Form			
Incident Ref. Number:		Evaluation Date/Time: (hh:mm DD/MMM/YYYY)	
Incident Declaration: (hh:mm DD/MMM/YYYY)		Incident Termination: (hh:mm DD/MMM/YYYY)	
Impact on staff and teachers	The incident may disrupt teachers' lesson planning, grading, and communication. Administrative staff may face significant workload increases related to recovery efforts. Payroll could be affected. Students may experience disruptions to learning, access to resources, and grading. Partnering institutions (e.g., other schools, libraries) relying on shared systems may also be affected. Parents will likely be concerned and require communication. ☐ Business System Compromise / Operation Impairment ☐ Others: _____		
Incident Description:			
I. General Information			
Reporting Entity Information			
Name:		Location:	
Title:		Department:	
Office/Mobile Number:		E-mail:	
II. Evaluation Details			
a. Incident Response (IR) Procedure			
IR Procedure Followed:	☐ Yes ☐ No If No, reasons for deviation:		
Additional Action(s) Taken:	☐ Yes If Yes, list the action(s) taken: ☐ No		
b. Detection, Containment, Eradication Efficiency			
Required Information Available On-Time:	☐ Yes ☐ No If No, what was missing and reason for delay:		
Required Resource(s) Available On-Time:	☐ Yes ☐ No If No, what was missing and reason for unavailability:		
Required Task(s) Completed On-Time:	☐ Yes ☐ No If No, what task(s) and reason for delay:		
External Expertise(s) Hired:	☐ Yes If Yes, what were the expertise(s) and vendor(s) name: ☐ No		
c. Operational Recovery			
Operational Capability Restored On-Time:	☐ Yes ☐ No If No, reason for delay:		
d. Incident Analysis			
Root Cause Analysis Conducted:	☐ Yes If Yes, list the root cause(s): ☐ No		
Necessary Corrective Actions Identified:	☐ Yes If Yes, list the corrective action(s) to be taken, responsible party and schedule: ☐ No		
Monitoring Control Improvement Identified:	☐ Yes If Yes, how could it be improved against similar incidents: ☐ No		
Additional Tool(s) Procurement Suggestion:	☐ Yes If Yes, list the tool(s): ☐ No		
e. Policy & Procedure			
Playbook Update Required:	☐ Yes If Yes, list the area(s) for update and reason: ☐ No		
Other Policy & Procedure Update Required:	☐ Yes If Yes, list the policy / procedure and reason: ☐ No		
f. Other Comments			
III. Improvement Roadmap			
Quick-Wins (immediate)			
Short-Term (3 months)			
Long-Term (6 months)			

Appendix - Escalation Procedure Based on Incident Severity Level (Reference)

This table is a general reference and must be tailored to fit the specific circumstances, resources, and organizational structure of each individual school. Before using this table, please review and customize it to reflect your school's specific context. Ensure all placeholder roles ([Role/Title]) are clearly defined and individuals are assigned responsibilities.

Severity	Description of Incident	Escalation Procedure
Critical	**Ransomware Attack:** Critical systems are encrypted and inaccessible, impacting essential school operations. Data is being held hostage. **Major Data Breach:** Large-scale theft of sensitive student or staff data, posing significant legal and reputational risks. **System Outage (critical):** Essential systems are completely unavailable, severely disrupting school operations. This could be due to a targeted attack or a catastrophic failure.	**Immediate escalation to [School Board/Governing Body/Superintendent] and legal counsel.** - Activate the school's incident response plan. - Engage external cybersecurity experts and law enforcement. - Communicate transparently with affected parties (students, parents, staff).
High	**Malware Infection (spreading):** Malware is actively spreading within the school network, potentially compromising multiple systems. **Targeted Intrusion:** Evidence of hackers actively targeting school systems, attempting to gain access to sensitive data or disrupt operations. **System Outage (major):** Important systems are unavailable, disrupting key school functions.	- Escalate to [Designated Senior Administrator/Principal]. - Activate the school's incident response plan. - Investigate the scope and impact of the incident. - Consider engaging external cybersecurity experts.
Medium	**Phishing Attack (successful):** Credentials or sensitive information have been compromised through a phishing attack. **Unauthorized Access (limited):** Evidence of unauthorized access to a specific system or account, but no indication of widespread compromise. **Security Misconfiguration:** A security vulnerability has been identified due to a system misconfiguration.	- Report to the designated incident response lead ([Role/Title]). - Investigate the incident and contain the potential impact. - Implement corrective actions and document the incident.
Low	**Suspicious Activity:** Unusual activity has been observed, but it's unclear whether it represents a genuine threat. **Security Alert (false positive):** A security system generated an alert that, upon investigation, turned out to be benign.	**Document the event and inform the incident response lead.** - Assess the risk and determine if further action is required.

Part IV :

Recommended Cybersecurity Configuration Checklist

Category	Checklist Item	Priority	Description	Guidance / Examples	Reference	Implementation Status
Architecture and Infrastructure	DMZ	High	Is the web server located within a DMZ, separating it from the internal network?	**DMZ Implementation:** Place the school's web server in a DMZ, separating it from the internal network where student data and other sensitive information are stored. This limits the impact of a potential web server compromise. **Firewall rules:** Configure firewall rules to restrict traffic between the DMZ, the internal network, and the internet. Allow only necessary traffic (e.g., HTTP/HTTPS) to the web server from the internet. **Example:** If the school uses a simple firewall appliance, configure it to create a separate network zone for the DMZ and apply appropriate access control rules.	8.1.1 (a)	
Architecture and Infrastructure	Firewall Diversity	Medium	Are different vendors or types of firewalls used for the internal and external networks?	**Firewall diversity:** If possible (and within budget), use firewalls from different vendors or different firewall technologies for the internal and external network perimeters. This reduces the risk of a single vulnerability affecting both firewalls. **Example:** Use a hardware firewall appliance for the external perimeter and software firewall on the internal network.	8.1.1 (a)	
Architecture and Infrastructure	NIDS/NIPS	High	Are Network Intrusion Detection/Prevention Systems in place and updated?	**NIDS/NIPS deployment:** Deploy a Network Intrusion Detection System (NIDS) or Network Intrusion Prevention System (NIPS) to monitor network traffic for malicious activity. **Signature updates:** Keep NIDS/NIPS signatures up-to-date to detect the latest threats. **Example:** Consider open-source NIDS/NIPS solutions like Snort or Suricata if budget is limited. Configure alerts for suspicious activity.	8.1.1 (b)	
Architecture and Infrastructure	WAF	High	Is a Web Application Firewall (WAF) implemented?	**WAF implementation:** Implement a WAF to protect the web server from common web application attacks like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). **Cloud-based WAF:** Cloud-based WAF solutions can be a cost-effective option for SMEs and schools. **Example:** Consider using a cloud-based WAF service like Cloudflare or AWS WAF.	8.1.1 (b)	
Architecture and Infrastructure	Anti-DDoS	High	Are anti-DDoS measures in place?	**DDoS protection service:** Consider subscribing to a DDoS protection service to mitigate volumetric DDoS attacks. **Rate limiting:** Implement rate limiting on the web server to limit the number of requests from a single IP address. **Example:** Cloudflare offers DDoS protection as part of its services. For basic rate limiting, configure the web server (e.g., using *mod_evasive* for Apache).	8.1.1 (b), 8.7	
Architecture and Infrastructure	Firewall Configuration	High	Is the firewall configuration regularly reviewed and updated?	**Deny by default:** Implement a "deny by default" (or "implicit deny") policy at the very end of the firewall ruleset. This means that all traffic is blocked unless explicitly allowed by a firewall rule. This significantly reduces the attack surface. **Principle of least privilege:** Allow only the minimum necessary traffic through the firewall. Restrict access based on source IP, destination IP, port, and protocol. **Firewall rule review:** Regularly review and update firewall rules (e.g., quarterly) to ensure they are still appropriate and effective. Remove any unnecessary rules (e.g. a rule allowing all traffic on all ports to a server when only HTTP and HTTPS are needed, or rules that are no longer needed because the system or service they were designed for is no longer in use.) **Document firewall rules:** Maintain clear documentation of all firewall rules, including their purpose and justification. **Example:** For the school's web server in the DMZ, allow only HTTP/HTTPS (port 80/443) traffic from the internet. Block all other incoming traffic to the DMZ. Similarly, restrict traffic from the DMZ to the internal network, allowing only necessary connections.	-	

Category	Checklist Item	Priority	Description	Guidance / Examples	Reference	Implementation Status
Web Server Security	Secure Configuration	High	Is the web server configured securely?	**Disable directory listing:** Prevent browsing of website files. Example: In Apache, set *Options -Indexes* in the .htaccess file. **Customize error pages:** Provide generic error messages instead of revealing server details. **Secure configuration files (Apache/Nginx):** Restrict access to httpd.conf, nginx.conf, etc., using file system permissions (e.g., chmod 640).	8.2.3 (b)	
Web Server Security	Least Privilege	High	Are processes running with least privilege?	**Web server user:** Run Apache/Nginx as a dedicated user account (www-data, apache, etc.) with limited system privileges. **Database access:** Create specific database users for web applications with only the necessary permissions (e.g., SELECT, INSERT, UPDATE for specific tables). **Avoid using the root database account.**	8.2.3 (c)	
Web Server Security	Patching	High	Are security patches applied promptly?	**OS and web server patching:** Patch the operating system (Windows Server, Linux distro) and web server software (Apache, Nginx) regularly. **Example of patch deployment priority:** - Critical (CVSS 9.0-10.0): Immediate patching (within 24-48 hours). - High (CVSS 7.0-8.9): Patch within 1-2 weeks. - Medium (CVSS 4.0-6.9): Patch within 1-3 months. - Low (CVSS 0.0-3.9): Patch as part of regular maintenance cycles. **Test patches on a staging server:** Before applying patches to the live server, test them on a staging or development server to ensure compatibility. **Subscribe to security mailing lists for vulnerability notifications.**	8.2.3 (d)	
Web Server Security	Access Control	Medium	Are access rights configured strictly?	**Student portals:** Use strong authentication (e.g., usernames and passwords, MFA if possible) to protect student data. **Administrative interfaces:** Restrict access to administrative interfaces (e.g., web server control panel, content management system) to authorized staff only. Use strong passwords and consider MFA.	8.2.3 (e)	
Web Server Security	Account Management	Medium	Are unused accounts disabled/removed?	**Student accounts:** Disable or delete student accounts when they leave the school. **Staff accounts:** Disable or delete staff accounts when they leave the organization.	8.2.3 (f)	
Web Server Security	Password Protection	High	Are passwords stored securely (hashed/encrypted)?	**Use a strong password policy:** For Students and Staff: -- Minimum length: 8 characters -- Complexity: Require uppercase, lowercase, numbers, and symbols. -- Password reuse: Prevent reuse of the last 5 passwords. -- Password Expiration: Consider expiring passwords every 90-180 days. For Administrators: -- Minimum length: 15 characters -- Complexity: Require uppercase, lowercase, numbers, and symbols, and consider using passphrases. -- Password reuse: Prevent reuse of the last 10 passwords. Password Expiration: Expire passwords every 60-90 days. **Multi-Factor Authentication (MFA):** Mandate MFA for all administrator accounts, where possible. **Prohibit common passwords and dictionary words** (e.g., "password," "123456," "qwerty," "schoolname," " mascot," student names, teacher names, school-related terms). **Use a blacklist or a password strength checker** that includes dictionary word detection. **Hash passwords:** If developing custom applications, ensure passwords are hashed using a strong algorithm like bcrypt or Argon2, with unique salts. **Password Managers:** Encourage students, staff, and administrators to use reputable password managers.	8.2.3 (g)	
Web Server Security	HIDS/HIPS	Medium	Are HIDS/HIPS installed on web servers?	**Consider open-source options (if budget is limited):** OSSEC, Fail2ban can provide basic intrusion detection and prevention capabilities. **Integrate with existing security tools:** If the school or SME has a firewall or security information and event management (SIEM) system, integrate the web server's logs and alerts.	8.2.3 (h)	
Web Server Security	Log Review	Medium	Are security logs reviewed regularly?	**Regular log checks:** Designate a staff member to review web server logs (access logs, error logs) at least weekly. Look for unusual activity, such as failed login attempts, access from unfamiliar IP addresses, or large file downloads. **Automated log analysis**: If possible, use a log analysis tool (e.g., GoAccess for simple web log analysis, or a SIEM for more comprehensive log management) to help identify suspicious patterns.	8.2.3 (i), 8.3.1	
Web Server Security	Information Disclosure	High	Is sensitive configuration information protected?	**Server version:** Disable web server version banners in HTTP responses. Example: In Apache, set *ServerTokens Prod* and *ServerSignature Off*. **Error messages:** Configure the web server to display generic error messages to users, avoiding revealing detailed internal error information.	8.2.3 (j)	
Web Server Security	Module Management	Medium	Are unnecessary modules disabled/removed?	**Example (Apache):** Disable unused modules like *mod_dav, mod_cgi,* or others not required for the school's website functionality. This reduces the potential vulnerabilities. **Review modules regularly:** Periodically review the enabled modules and disable any that are no longer needed.	8.2.3 (k)	
Web Server Security	Service Minimization	Medium	Are unused services/ports disabled?	**Example:** If the web server is only used for hosting the school website, disable unnecessary services like FTP, SSH (if not needed for remote administration), or other unused network services. This can be done through the operating system's service management tools (e.g., services.msc on Windows, systemd on Linux).	8.2.3 (l)	
Web Server Security	Default Files	Medium	Are default/sample files removed?	**Example:** After installing the web server or a CMS, remove default installation files, test scripts, and sample pages that are not needed for the school's website. These often contain known vulnerabilities.	8.2.3 (m)	
Web Server Security	Web Crawling Restriction	Medium	Is web crawling restricted for sensitive content?	**Student directories/portals:** Use *robots.txt* to prevent search engines from indexing pages containing student data or internal school resources. **Internal staff resources:** Restrict access to staff-only sections of the website using access controls (e.g., password protection, IP address restrictions) and *robots.txt* to prevent indexing.	8.2.3 (n)	
Web Server Security	File Protection	High	Are important files protected?	**Configuration files:** Secure web server configuration files (e.g., *httpd.conf, nginx.conf*) and *.htaccess files* with appropriate file system permissions (e.g., chmod 640 on Linux/Unix systems) to prevent unauthorized modification. **Database backups:** Store database backups in a secure location, preferably offline, and encrypt them if they contain sensitive data.	8.2.3 (o)	
Web Server Security	SSL/TLS Certificate Management	High	Are private keys securely backed up and protected?	**SSL certificate and key storage:** Store SSL certificates and private keys securely, preferably offline or in a hardware security module (HSM) if available. **Backups:** Maintain secure backups of SSL certificates and keys. These are essential for restoring HTTPS functionality in case of server failure or compromise.	8.2.3 (p)	
Web Server Security	Website Backups	High	Are regular backups performed?	**Regular website backups:** Back up the entire website (files and databases) regularly, at least weekly. **Offsite backups:** Store backups in a secure, offsite location to protect against data loss due to local disasters (e.g., fire, flood). Cloud storage can be a cost-effective option for offsite backups.	8.2.3 (q)	

Category	Checklist Item	Priority	Description	Guidance / Examples	Reference	Implementation Status
Web Application Security	Data Handling	High	Is sensitive data handled in transit?	**Enforce HTTPS:** Redirect all HTTP traffic to HTTPS. Ensure that all website pages, especially those handling logins, forms, or any sensitive data, are served over HTTPS. **Use Strong SSL/TLS Ciphers and Protocols:** Disable outdated and insecure SSL/TLS versions (like SSLv2, SSLv3, TLS 1.0, and TLS 1.1) and ciphers. Prioritize strong ciphers and protocols like TLS 1.3 and TLS 1.2 with AES-256 encryption. Regularly review and update cipher suites based on industry best practices. Use tools like Qualys SSL Labs Server Test to assess your SSL/TLS configuration. **Obtain SSL Certificate from a Reputable CA:** Obtain an SSL certificate from a trusted and reputable Certificate Authority (CA). Consider using Extended Validation (EV) certificates for enhanced trust and user assurance, especially for login pages. **HSTS (HTTP Strict Transport Security):** Implement HSTS to force browsers to always connect to your website over HTTPS, even if a user manually types in "http://". This helps prevent man-in-the-middle attacks. **Avoid using query parameters for sensitive data:** Do not transmit sensitive information (e.g., passwords, student IDs) in URL query parameters. -- Example of BAD practice: *https://school.edu/grades?studentId=12345&grade=A* (Exposes student ID and grade in the URL) -- Example of GOOD practice: Use POST requests to submit sensitive data in the request body, which is not visible in the URL.	8.4.1 (c), 8.6.1(a-e, g)	
Web Application Security	Data Handling	High	Is sensitive data handled at rest?	**Database encryption:** If using a database, enable database encryption to protect data at rest. **File system encryption:** Consider encrypting the file system or specific directories containing sensitive data. Full-disk encryption is recommended for laptops and other portable devices.	8.4.1 (c), 8.6.1 (f)	
Web Application Security	Session Management	Medium	Are sessions managed securely to prevent session hijacking and maintain user privacy.?	**Secure session IDs:** Generate random, unpredictable session IDs. Avoid using predictable patterns or user-specific information in session IDs. **HTTPS for sessions:** Transmit session IDs only over HTTPS. **Session timeout:** Implement session timeouts to automatically log out inactive users. Example: Set a reasonable timeout (e.g., 15-30 minutes) for school portal sessions. **Regenerate session IDs:** Regenerate session IDs after important actions like login or password change.	-	
Web Application Security	Password Management	High	Are strong passwords enforced and updated?	**Use a strong password policy:** For Students and Staff: -- Minimum length: 8 characters -- Complexity: Require uppercase, lowercase, numbers, and symbols. -- Password reuse: Prevent reuse of the last 5 passwords. -- Password Expiration: Consider expiring passwords every 90-180 days. For Administrators: -- Minimum length: 15 characters -- Complexity: Require uppercase, lowercase, numbers, and symbols, and consider using passphrases. -- Password reuse: Prevent reuse of the last 10 passwords. Password Expiration: Expire passwords every 60-90 days. **Multi-Factor Authentication (MFA):** Mandate MFA for all administrator accounts, where possible. **Prohibit common passwords and dictionary words** (e.g., "password," "123456," "qwerty," "schoolname," " mascot," student names, teacher names, school-related terms). **Use a blacklist or a password strength checker** that includes dictionary word detection. **Hash passwords:** If developing custom applications, ensure passwords are hashed using a strong algorithm like bcrypt or Argon2, with unique salts. **Password Managers:** Encourage students, staff, and administrators to use reputable password managers.	8.5.1(d)	
Web Application Security	Injection Protection	High	Is input validated to prevent injections?	**Input validation:** Validate all user inputs (form fields, URL parameters, etc.) to prevent injection attacks. Example: For a student registration form, validate the "name" field to only accept alphanumeric characters and spaces. **Parameterized queries (for database interactions):** Use parameterized queries or prepared statements to prevent SQL injection. Never construct SQL queries by directly concatenating user input. **Output encoding:** Encode all output displayed on web pages to prevent cross-site scripting (XSS) attacks. Example: Encode <, >, &, and " characters to their HTML entity equivalents (<, >, &, ").		
Web Application Security	Access Control	Medium	Is role-based access control enforced?	**Student/Teacher/Admin roles:** Implement role-based access control to restrict access to different parts of the school website. Example: Students can access their grades and assignments, teachers can manage their classes, and administrators have full access.	-	
Web Application Security	Data Safety	High	Is HTTPS used, and data encrypted?	**HTTPS everywhere:** Enforce HTTPS for all website traffic. Obtain an SSL certificate from a reputable CA (Let's Encrypt is a free and good option). **Database encryption:** Encrypt sensitive data stored in the database. Most database systems offer encryption features. **File system encryption (for sensitive files):** Encrypt sensitive files stored on the web server's file system.	8.5.1(b), 8.6.1 (a)	
Web Application Security	Input Safety	Medium	Are uploaded file types validated/inspected?	**File type restrictions:** Limit allowed file types for uploads (e.g., only allow .pdf, .docx, .jpg). **File size limits:** Restrict the maximum file size for uploads to prevent denial-of-service attacks. **Malware scanning:** If possible, scan uploaded files for malware using a virus scanner.	-	
Web Application Security	Error Handling	Medium	Do errors avoid exposing sensitive information?	**Generic error messages**: Display generic error messages to users, avoiding revealing detailed internal error information or stack traces. Example: Instead of displaying a database error message, display a generic "An error occurred. Please try again later." message. **Log detailed errors:** Log detailed error messages to server logs for debugging purposes, but do not display them to users.	-	
Web Application Security	Logging and Monitoring	Medium	Are access logs enabled and reviewed?	**Enable web server logging:** Ensure web server access logs are enabled and record important information like IP addresses, timestamps, requested URLs, and user agents. **Regular log review:** Designate a staff member (or use automated tools) to review logs regularly (e.g., weekly) for suspicious activity like repeated failed login attempts, access from unusual locations, or requests for sensitive files. Example: Use log analysis tools like GoAccess or Webalizer to generate reports on website traffic and identify potential issues. For more advanced monitoring, consider a Security Information and Event Management (SIEM) system.	8.3.1, 8.5.1(e)	
Web Application Security	Configuration Management	Medium	Are secure default configurations used?	**Harden web server configuration:** After installing the web server (Apache, Nginx, IIS), disable unnecessary modules and features, and apply security hardening guidelines specific to the web server software. **Example (Apache):** Disable directory listing, configure custom error pages, and restrict access to configuration files. **Example (Nginx):** Limit request sizes, disable server tokens, and configure proper access controls.	8.2.3 (k, l)	

Category	Checklist Item	Priority	Description	Guidance / Examples	Reference	Implementation Status
General Website Security	Software Updates	High	Are software updates applied regularly?	**Patching schedule:** Establish a regular patching schedule for the operating system, web server software, content management system (CMS), and any other web applications. **Test updates:** Before applying updates to the live server, test them on a staging or development server to ensure compatibility. Example: Subscribe to security mailing lists or vulnerability databases to receive timely notifications about new vulnerabilities and patches.	8.5.1 (a)	
General Website Security	Secure Remote Administration	Medium	Is secure remote access used?	**Strong passwords/MFA:** Use strong passwords and multi-factor authentication (MFA) for remote access to the web server. **VPN:** Use a Virtual Private Network (VPN) for secure remote administration. **Restrict access by IP:** If possible, restrict access to administrative interfaces (e.g., web server control panel, SSH) to specific IP addresses or ranges. Example: Instead of using standard SSH port 22, change it to a non-standard port.	8.5.1 (c)	
General Website Security	Search Indexing Control	Medium	Are measures in place to prevent data leakage via search engines?	**robots.txt:** Use a robots.txt file to block search engine crawlers from accessing sensitive directories or pages. **Meta tags:** Use meta tags (e.g., *<meta name="robots" content="noindex">*) to prevent specific pages from being indexed. **Example:** Block access to student directories, staff-only sections, or internal administrative interfaces using robots.txt.	8.5.1 (f)	
General Website Security	Security Scanning	Low	Are vulnerability scans conducted?	**Regular vulnerability scanning:** Use vulnerability scanners (e.g., Nessus Essentials, OpenVAS) to periodically scan the website for known vulnerabilities. Frequency: --- External Scans (Internet-facing systems): At least bi-annually, or more frequently if your school handles highly sensitive data or has experienced recent security incidents. --- Internal Scans (Intranet systems): At least annually. **Penetration testing (if budget allows):** Consider engaging a qualified and experienced security assessor or penetration firm to conduct the penetration testing to simulate real-world attacks and identify vulnerabilities. Frequency: At least annually, or after significant system changes. Focus on critical systems and applications.	8.5.1 (g)	
General Website Security	Outsourcing Security	Medium	Does web hosting meet security requirements?	**Service Level Agreements (SLAs):** Review the web hosting provider's SLAs to ensure they meet the school's security requirements (e.g., data center security, uptime guarantees, incident response procedures). **Security audits:** If possible, request information about the web hosting provider's security audits and certifications (e.g., ISO 27001, SOC 2).	8.5.1 (h)	

Implementation Summary	Count	% Implementation
High Highest priority to implement and encorporate as a baseline level of security, deemed to be vital to uphold a secure environment (Total: 18)	0	0%
Medium Important protective measures that are beneficial to maintaining security, but may be deferred in implementation	0	0%
Low Additional protective measures for enhanced protection	0	0%