香港學校網絡安全指南

第一部份：

即用式網絡安全政策範本

《合理使用政策》範本

[貴校名稱]

版本 X.X

起草人：	[姓名]，[職稱]，[學校名稱]
核准／生效日期：	日/月/年

本文件僅作為參考範本提供。各校在實施前，必須審閱、適配並核准內容，以符合自身環境、資源及需求。發行單位對於基於本範本所採取的任何行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 簡介 5
2. 一般政策原則 6
3. 職責分工 8
4. 可接受與不可接受的使用 10
   4.1. 教職員 10
   4.2. 學生 13
   4.3. 家長與監護人 16
   4.4. 訪客與承包商 17
5. 數據保護與隱私 18
6. 政策例外與違規 19
7. 確認書 21
   7.1. 學生／家長確認書 21
   7.2. 員工確認書 23
   7.3. 訪客／承包商確認書 24
   A. 術語表 25

1. 簡介

目的

本《可接受使用政策》（AUP）旨在為 [學校名稱] 內資訊科技（IT）資源的負責任、合乎道德且安全的使用，制定明確的指引。本政策旨在保護學生、教職員及學校社群，確保遵守相關法律與法規，並支持在學習與學校行政管理中安全且有效地使用數位工具。

適用範圍

本政策適用於所有使用本校 IT 資源的使用者，包括但不限於：

- 教學及非教學人員
- 學生
- 家長及監護人（如適用）
- 訪客、承包商及可存取本校系統或數據之第三方
- 資訊科技資源包括所有學校擁有的電腦、行動裝置、網路基礎設施、軟體、雲端服務，以及任何用於存取學校系統的個人裝置（自帶裝置，BYOD）。

定義

- **IT 系統**：由學校管理或使用的所有數碼基礎設施、裝置、服務及應用程式，包括網路、伺服器、電腦及雲端資源。
- **使用者：**所有可存取學校資訊科技系統之人員，包括教職員、學生及經授權之第三方。
- 自攜設備；指使用個人裝置存取學校系統。
- **數據外洩**：　未經授權存取、洩露或遺失個人或機密數據。
- **個人數據：**與可識別個人有關的資訊，包括學生及教職員。
- **網絡安全事件：**任何針對資訊或資訊系統的未經授權存取、使用、揭露、干擾、修改或破壞之企圖或實際行為。

2. 一般政策原則

範本說明：請概述禁止行為。請根據您的環境需求，適當地增刪範例。

可接受使用概述

[學校名稱] 所有資訊科技資源的使用者，必須以負責任且符合道德的方式使用這些資源，並支持學校的教育及行政目標。可接受的使用方式包括：

- 為教學、學習、研究、行政管理及經核准的課外活動，存取並使用學校資訊科技資源。
- 無論在線上或線下，均須尊重他人的權利、隱私及財產。
- 遵守所有適用法律、學校政策及授權協議。

不當使用概覽

資訊科技資源的不當使用包括但不限於：

- 存取、建立或分享非法、不當或具冒犯性的內容。
- 未經授權存取或篡改他人的帳戶、檔案或數據。
- 從事網路霸凌、騷擾或任何形式的線上虐待行為。
- 下載或安裝未經批准的軟體或應用軟件。
- 利用資訊科技資源謀取個人商業利益或進行未經授權的募款。
- 任何危及學校 IT 系統安全性、完整性或可用性的活動。

安全與隱私原則

[範本註：請概述您對保護資訊科技系統及個人資料的期望。請根據貴校的要求調整此清單。]

所有使用者均應：

- 保護其使用者名稱、密碼及存取憑證；切勿與他人分享。
- 不使用設備時，應登出或鎖定裝置。
- 如發現疑似安全事件、資料外洩或可疑活動，請向 [請填寫負責人員或聯絡窗口] 通報。
- 尊重個人及敏感資訊的機密性與隱私權。
- 僅在獲得授權且為學校目的所需時，方可收集、存取或分享個人數據。

監控與執行

範本備註：請具體說明貴校的監控措施與執行機制。請配合貴校的實際情況及法律要求進行調整。

[學校名稱] 保留監控其 IT 資源使用情況的權利，以確保遵守本政策、支援營運需求，並保護使用者與數據。監控可能包括：

- 檢視網路流量、電子郵件及互聯網使用紀錄。
- 檢查校方擁有的裝置及儲存裝置，以確認是否符合政策規定。

違反本政策者，可能面臨紀律處分，處分程度視情況而定，最高可包括暫停資訊科技存取權限、啟動紀律程序或採取法律行動。

3. 職責分工

學校管理層／IT 協調員

[範本註：請指明負責政策監督、IT 系統管理及合規性的職責。]

- 制定、維護及更新《可接受使用政策》。
- 向所有使用者傳達政策要求。
- 提供適當的資訊科技培訓與資源。
- 透過技術與程序控制措施，確保資訊科技系統及數據受到保護。
- 監控合規狀況並調查潛在違規行為。
- 向相關主管機關及利害關係人通報重大事件。
- 審查並回應與資訊科技使用相關的意見回饋或事件。

教學及非教學人員

[範本註：請視不同職務角色酌情調整。]

所有教學及非教學人員均有責任：

- 依照本政策使用學校資訊科技資源，並以身作則展現負責任的數位行為。
- 監督學生使用資訊科技資源，並向資訊科技統籌員或校方管理層報告任何濫用情況或疑慮。
- 保護敏感資訊（例如學生數據），並遵循數據保護程序。
- 完成所需的資訊科技及網絡安全培訓。
- 立即通報資訊科技安全事件、疑似資料外洩或政策違規行為。

學生

[範本註：請根據學生的年齡層及數位成熟度進行調整。]

所有學生均有責任：

- 將資訊科技資源用於經核准的教育目的。
- 遵守教師及職員關於資訊科技使用的指示。
- 在線上尊重他人的權利、隱私及財產。
- 對個人登入憑證保持機密性。
- 如發現可疑活動、霸凌或濫用資訊科技資源，應立即通報。

註：年幼的學生可能需要額外的監督與指導。

家長與監護人

[範本註：請根據貴校的實際情況調整內容，以反映家長的參與程度。]

家長及監護人應負責：

- 支持學校推動資訊科技資源負責任且安全使用的相關措施。
- 與子女共同審閱並討論《合理使用政策》。
- 確保同意書（如需）已審閱並簽署。
- 向學校教職員回報對學生使用資訊科技的疑慮。

訪客、承包商及第三方

[範本註：請明確規定學校資訊科技系統非常規使用者的相關要求。]

可存取學校資訊科技資源的訪客、承包商及第三方須負責：

- 依照本政策使用資訊科技資源，且僅限於授權用途。
- 遵守所有相關的機密性和安全要求。
- 向資訊科技協調員或學校管理層報告任何安全事件或政策違規行為。
- 於合作關係結束時歸還或停用存取憑證。

4. 可接受與不可接受的使用

4.1. 教職員

[範本註：請根據貴校對教職員的期望調整這些要點。]

允許的使用

- 將學校資訊科技資源用於教學、行政管理、專業發展及經核准的課外活動。
- 在學校規範範圍內存取、製作及分享教育資料。
- 使用經核准的學校平台與學生、家長及同事進行溝通。
- 應依照學校政策及隱私法規儲存與處理個人及具有機密性的資訊。
- 僅將互聯網及電子郵件用於工作相關目的。

不可接受的使用行為

- 存取、建立或散佈具冒犯性、非法或不當的內容。
- 將 IT 資源用於個人商業利益、未經授權的募款或政治活動。
- 分享登入憑證或允許未經授權的人員存取學校系統。
- 下載或安裝未經批准的軟體或應用軟件。
- 未經適當授權即洩露機密或敏感資訊。
- 繞過、停用或干擾安全控制措施或監控系統。

安全責任

[範本註：請根據貴校的安全程序增刪條目。]

- 使用強效且獨特的密碼，並定期更換。
    - 請勿使用您的生日、「123456」、「password」或家人的名字作為密碼。
    - 密碼長度至少為 8 個字符，並混合使用字母（大寫與小寫）、數字及符號。
    - 範例：「SchooL2024!」比「school」或「123456」更安全。
    - 請勿重複使用其他網站或個人帳戶的密碼。
    - 考慮使用密語——一句您容易記住但他人難以猜測的短句，例如「SunnyDays!Read2Learn」。
    - 如果您認為可能有人知道您的密碼，請立即更改。
    - 切勿將密碼寫在電腦旁的便利貼上，或與任何人分享。
- 請勿與任何人分享密碼。
- 當裝置無人看管時，請鎖定或登出。
- 如有任何疑似安全漏洞、網路釣魚企圖或可疑活動，請立即向 IT 協調員報告。
- 確保所有數據儲存與傳輸均符合學校的數據保護政策。
- 僅允許經授權的學生進入虛擬教室，並在必要時驗證學生身分。
- 請勿公開分享虛擬教室連結或會議密碼，亦勿與未經授權者分享。

- 使用虛擬教室平台提供的等候室、密碼保護及其他安全功能。
- 下課後應立即結束虛擬課程，並確保錄影檔案依照學校政策安全儲存。
- 視需要將參與者靜音，並停用學生的攝影機／麥克風，以防止干擾或不當行為。
- 在虛擬課程期間，提醒學生遵守線上禮儀及隱私規範。
- 在錄製課程前須告知學生及家長，並在學校政策或當地法律要求時取得同意。
- 僅將課程錄影儲存於經核准且安全的學校平台，切勿儲存於個人裝置或消費級雲端服務中。
- 定期檢視並刪除不必要的錄影或包含學生資訊的檔案。
- 僅透過經核准的學校管道（例如：安全的學習管理系統、學校電子郵件）分享作業、資源及連結。
- 切勿在公開網站或社交媒體上發布課堂連結、作業或學生作品。
- 請警惕假冒學生、家長或學校管理員發送的釣魚電子郵件或信息。
- 在回應意外收到的敏感資訊請求前，請先進行核實。
- 與學生及家長的所有通訊往來，均須使用學校官方通訊管道。
- 顯示學生在聊天室和分組討論室中的互動，以防止霸凌、騷擾或分享不當內容。
- 向學生提供明確指引，說明如何通報在網路上遇到的任何疑慮或不當事件。
- 請勿向學生透露您的個人聯絡方式或社群媒體帳號。
- 避免在直播課程或共享資料中討論或展示敏感的個人或學生資訊。

個人裝置的使用（自帶裝置）

[範本註：請說明貴校的自帶設備（BYOD）政策。若不允許自帶設備，請刪除此節。]

- 教職員僅可在符合學校安全要求的情況下，將個人裝置用於工作用途。
- 個人裝置必須安裝最新的防毒軟體，並使用安全的密碼。
- 僅可透過經核准的應用程式或安全連線存取學校系統。
- 若用於學校公務的個人裝置遺失或遭竊，請立即通報。

4.2. 學生

可接受的使用規範

[範本註：請根據年齡層（小學與中學）調整措辭。]

- 請將資訊科技資源用於學習、研究及與學校相關的活動。
- 使用資訊科技設備或平台時，須遵循教師及職員的指示。
- 在網路上進行溝通時，應保持尊重與負責任的態度。
- 僅可瀏覽教職員指示之合適網站及內容。

不可接受的使用行為

- 存取、製作或分享非法、冒犯性或不當的內容。
- 參與網路霸凌、騷擾或任何形式的線上虐待。
- 試圖繞過學校的安全措施或互聯網過濾機制。
- 分享個人密碼或使用他人的帳戶。
- 損壞或干擾學校設備、軟體或網路。

數位公民素養與安全

[範本註：請根據貴校學生群體的實際情況補充相關指引。]

- 學生應在線上及線下互動中，以尊重與禮貌的態度對待所有人。
- 個人資訊（包括姓名、地址、電話號碼及密碼）必須受到保護，不得向陌生人透露或公開張貼於網路上。
- 任何網路霸凌事件、收到可疑信息，或接觸到不安全或不當的線上內容，都必須立即向可信賴的成人或學校工作人員通報。
- 學生必須遵守著作權法，不得剽竊、複製或濫用數位內容。所有來源均須妥善標示出處。

安全責任

[範本註：請根據貴校的安全程序增刪條目。]

- 學生必須選擇不易被猜中的密碼（避免使用姓名、生日，或「password」、「123456」等簡單字詞）。
- 密碼應盡可能包含字母、數字及符號的組合。
- 切勿將密碼分享給朋友、同學，或任何除可信賴的成年人（例如需要協助時的父母或老師）以外的人。
- 請勿將密碼寫在他人可見之處（例如課桌或裝置上）。
- 若您認為有人知道您的密碼，請立即更改密碼並告知老師。
- 如有要求，請為每個學校帳戶或平台使用不同的密碼。

- 切勿使用他人的使用者名稱或帳號登入學校系統或裝置。
- 使用完畢後，請務必登出帳戶並關閉所有學校應用程式或網站，特別是在共用或公共裝置上。
- 除非老師另有指示，否則請使用您的真實姓名和學校提供的帳號參加線上課程。
- 請勿將虛擬教室連結、會議密碼或代碼分享給非班級成員的人士。
- 請在安全且合適的環境中參與線上課程，並遵循老師關於鏡頭／麥克風使用的一切指示。
- 未經老師和學校明確許可，請勿錄製、截圖或分享線上課程或同學的畫面。
- 僅按照指示與老師或同學分享課業、檔案或信息。
- 請勿上傳、散佈或轉發不當、冒犯性或受版權保護的資料。
- 在提交或發佈檔案前，請務必再次確認，以確保您分享的是正確的資訊，且對象正確。
- 未經許可，請勿在社交媒體上發布或分享與學校相關的資訊、圖片或影片。
- 請勿製作或分享可能令他人難堪、威脅或傷害他人的內容。
- 請記住，任何上傳至網路的內容都可能永久存在且被他人看見；分享前請三思。
- 切勿在網路上分享您的地址、電話號碼、學生證號或其他個人資訊，除非學校平台有此要求。
- 請勿向同學索取個人資訊，亦請勿在未經他人同意的情況下分享他人的資訊。
- 無論在線上或線下，請隨時尊重同學和老師的隱私。
- 請妥善保管您的個人裝置，切勿在公共場所將其置於無人看管之處。
- 若在網路上看到或收到可疑、不當或令你感到不適的內容，請立即向老師或 IT 人員報告。
- 若您認為自己的帳戶遭駭客入侵，或懷疑有人正在使用您的帳戶，請告知您信任的成年人。
- 切勿試圖駭入、停用或繞過任何學校的安全設定、過濾器或監控工具。
- 切勿點擊可疑連結或下載來源不明的附件，即使它們看似來自朋友。
- 僅將學校的裝置、帳戶和網路用於學習或其他經批准的活動。
- 如果您不確定某件事是否安全或被允許，請在繼續之前詢問老師或 IT 人員。

個人裝置的使用（自帶裝置，BYOD）

[範本註：請說明貴校的 BYOD 政策。若不允許使用 BYOD，請刪除此節。]

- 學生僅在獲得教職員明確許可的情況下，方可在校內或為學校相關工作使用個人裝置。
- 所有在校園內或用於學校活動的個人裝置，必須符合教育目的，並遵守所有適用的學校資訊科技及安全政策。
- 嚴禁使用個人裝置存取、儲存或散佈不當內容，或以任何方式干擾學校活動。
- 若發生個人裝置遺失、遭竊或遭濫用之情況，必須立即向校方主管報告。
- 學生有責任確保其裝置的安全，包括維持最新的安全設定，以及不向他人透露裝密碼。

4.3. 家長與監護人

[範本註：請根據貴校對家校合作及數位公民素養的方針調整這些要點。]

支持負責任的使用

- 請與您的孩子一起檢視並討論學校的《可接受使用政策》。
- 鼓勵您的孩子在家中及學校皆遵循安全且負責任的網路使用規範。
- 支持學校在推廣數位公民素養、網路安全及尊重他人的網路行為方面的努力。
- 強調保護個人資訊的重要性，並鼓勵學生舉報任何有關網路霸凌或不當內容的疑慮。

同意與監督

- 請填妥並交回所有與您子女使用學校資訊科技資源、數位平台及線上服務相關的必要同意書。
- 請監督子女在家中使用科技設備的情況，特別是年幼的學生。
- 如有任何關於子女使用科技設備的具體疑慮或要求，請告知學校。
- 若您發現任何問題，或對子女的數位安全或網路體驗有任何疑問，請與學校教職員聯繫。

4.4. 訪客與承包商

合理使用規範

[範本註：請明確列出針對外部使用者的任何限制或要求。]

- 僅將學校資訊科技資源用於經授權的公務、教育或支援目的。
- 僅可存取與您的職務或與學校合作關係相關的系統、數據及資訊。
- 使用資訊科技資源時，請遵守所有學校政策及安全程序。
- 請維持機密性並保護在訪校或提供服務期間接觸到的任何個人或敏感資訊。

不可接受的使用行為

- 未經授權試圖存取、修改或分享機密或敏感的學校資訊。
- 將學校的 IT 資源用於個人、商業或與學校無關的活動。
- 將未經批准的硬件、軟體或數據引入學校網路。
- 從事任何可能危及學校資訊科技系統安全或完整性的活動。
- 未遵守學校職員關於資訊科技使用的指示。

5. 數據保護與隱私

個人及機密數據之處理

[範本註：請根據貴校的數據處理慣例及法規要求（例如香港《個人資料（私隱）條例》）調整這些要點。]

- 所有使用者必須依照學校政策及適用的數據保護法例處理個人及具有機密性的數據。
- 唯經授權之人員方可存取個人、敏感或具有機密性的資訊，且僅限於合法的教育或行政目的。
- 未經適當授權，不得向校外披露、分享或轉移個人數據（例如學生紀錄、教職員資訊或家長聯絡資訊）。
- 載有機密資料的電子及紙本紀錄必須安全儲存，並採取適當的防護措施，以防止未經授權的存取、遺失或盜竊。
- 使用者必須確保數據僅在必要期間內保留，並在不再需要時予以安全刪除或銷毀。
- 任何涉及個人資料的外部數位平台或雲端服務之使用，均須經學校管理層批准，並符合隱私與安全要求。

通報安全事件

[範本註：請說明貴校的事件通報流程及負責聯絡人。]

- 所有使用者必須立即向 [插入負責人員，例如：IT 協調員、數據保護官] 通報任何實際或疑似之資料外洩、個人／機密資料遺失或其他安全事件。
- 事件範例包括：數據意外洩露、存有學校數據的裝置遺失或遭竊、帳戶遭未經授權存取，或收到可疑電子郵件。
- 可透過 [插入通報方式：電子郵件、電話、親臨或指定線上表單] 進行通報。
- 學校將立即調查所有通報的事件，採取適當措施以減輕風險，並在法律要求時通知相關主管機關或受影響的個人。
- 用戶必須在調查期間全力配合，並遵循任何指示以協助控制或解決事件。

6. 政策例外與違規

政策審查與更新

[範本註：請指定您的審查時程與更新流程。]

- 本《可接受使用政策》將至少每 [插入週期，例如：年／學年] 進行一次檢討，或於技術、法規或學校運作發生重大變更時進行檢討。
- 審查程序將由 [請填寫負責單位，例如：資訊科技統籌員或校務管理層] 主導，並視情況輸入教職員、學生及其他利害關係人的意見。
- 本政策的更新或修訂須經 [請填寫核准單位，例如：校務管理委員會或校長] 核准。
- 如有重大政策變更，將通知所有使用者，並視需要提供更新版本。

紀律處分與執行

[範本註：請根據貴校的紀律架構及升級處理流程進行調整。]

- 違反本《可接受使用政策》可能導致紀律處分，包括但不限於：
    - 口頭或書面警告
    - 暫停或撤銷資訊科技使用權限
    - 額外培訓要求
    - 留校察看、停學或開除（針對學生）
    - 紀律處分程序或僱傭處分（適用於教職員）
    - 終止服務或存取權限（適用於承包商／訪客）
- 若涉及潛在犯罪活動或法律違規，學校可將該事項轉交執法機關或監管機構處理。
- 紀律處分將依據 [插入相關校規，例如《學生行為準則》、《教職員手冊》] 執行。

職責與聯絡方式

[範本註：請填寫貴校的聯絡窗口及負責人。]

如有疑問或欲通報與本政策相關之問題，請聯絡：

- 資訊科技協調員：[請填入姓名／電子郵件／電話]
- 數據保護官：[請填寫姓名／電子郵件／電話]
- 校長或學校行政辦公室：[請填寫聯絡資訊]
- 事件通報：[請填寫通報方式或連結]

所有查詢及報告均會按照學校政策，保持機密性。

7. 確認書

7.1. 學生／家長確認書

學生／家長確認書

可接受使用政策

學校名稱：_____

政策版本／日期：_____

學生姓名：_____

班級／年級：_____

確認聲明：

本人已收到、閱讀並理解 [學校名稱] 資訊科技資源之《合理使用政策》。

身為學生，我同意在使用學校科技設備及線上服務時，遵守本政策所載之規則與責任。

身為家長／監護人，本人同意協助學校推廣安全且負責任的數碼科技使用方式，視需要監督子女使用數位裝置，並若對本政策有任何疑問或顧慮，將主動聯繫學校。

學生簽名：_____ 日期：_____

家長／監護人姓名：_____

家長／監護人簽名：_____ 日期：_____

聯絡電話／電子郵件：_____

僅供辦公室使用：

收件人：_____ **日期：**_____

如有疑問請聯絡

- 資訊科技統籌員：[請填寫姓名／電郵／電話]
- 學校管理辦公室：[請填寫聯絡資料]

7.2. 員工確認書

教職員確認書

可接受使用政策

學校名稱：_____

政策版本／日期：_____

員工姓名：_____

職位／部門：_____

電子郵件／聯絡電話：_____

確認聲明：

本人確認已收到、閱讀並理解 [學校名稱] 資訊科技資源《合理使用政策》。本人同意遵守該政策所述之要求、責任及期望。本人明白違反該政策可能導致紀律處分，包括喪失資訊科技使用權限，或依學校政策規定採取進一步行動。

本人明白，若對本政策任何方面有疑問，有責任向資訊科技統籌員或校方管理層尋求澄清。

簽名：_____ 日期：_____

僅供辦公室使用：

收件人：_____ 日期：_____

諮詢聯絡人

- 資訊科技統籌員：[請填寫姓名／電郵／電話]
- 學校管理辦公室：[請填寫聯絡資料]

7.3. 訪客／承包商確認書

訪客／承包商確認書

可接受使用政策

學校名稱：_____

政策版本／日期：_____

訪客／承包商姓名：_____

所屬機構／公司（如適用）： _____

來訪／服務目的： _____

聯絡電話／電子郵件：_____

確認聲明：

本人確認已收到、閱讀並理解 [學校名稱] 針對訪客及承包商所制定的資訊科技資源《合理使用政策》。

本人同意在存取或使用任何學校資訊科技資源、系統或數據時，均將遵守該政策之規定。本人明白若未遵守該政策，可能導致存取權限被撤銷，或終止本人與該校之合作關係。

若對本政策有任何疑問，我將向學校的資訊科技協調員或指定聯絡人尋求澄清。

簽名：_____ **日期：**_____

僅供辦公室使用：

收件人：_____ **日期：**_____

疑問聯絡窗口

- 資訊科技統籌員：[請填寫姓名／電郵／電話]
- 學校管理辦公室：[請填寫聯絡資料]

A. 術語表

術語	定義
存取控制	用於限制僅授權使用者才能存取 IT 系統、數據或地點的流程與技術。
人工智能	能夠執行通常需要人類智慧的任務（例如學習或解決問題）的電腦系統或軟體。
資產	學校擁有或管理的任何裝置、軟體、數據或系統，包括硬件、軟體及雲端服務。
備份	為防止數據遺失或損毀而另行儲存的數據副本，以便進行復原。
自攜設備	使用個人擁有的裝置（例如筆記型電腦、智慧型手機）進行學校活動或存取學校系統。
雲端服務	由第三方主機託管並透過互聯網存取的線上服務（例如：儲存空間、應用程式、平台）。
機密數據	必須防止未經授權存取的資訊，例如學生紀錄或個人資料。
網絡安全事件	任何針對資訊或資訊系統所進行的未經授權存取、使用、揭露、干擾、修改或破壞之企圖或實際行為。
數據加密	將數據轉換為編碼形式以防止未經授權存取的過程。
數據外洩防護 (DLP)	旨在防止敏感資訊遭未經授權分享或遺失的工具或流程。
數據保護	為保護個人、敏感或機密資訊免遭未經授權的存取、揭露、竄改或破壞而採取的措施。
終端裝置	任何連接至學校網路的裝置（例如：電腦、平板電腦、智慧型手機）。
防火牆	一種安全系統（硬件或軟體），根據預先設定的規則監控並控制進出網路的流量。
事件	任何可能危及學校資訊或資訊系統機密性、完整性或可用性的事件。
IT 協調員	負責監督學校資訊科技系統、安全及合規事宜的人員或職位。
日誌	用於監控與追蹤責任的事件記錄，例如系統存取或數據變更。
流動裝置管理 (MDM)	用於監控、管理及保障學校運作中所使用行動裝置的工具或流程。
多重認證 (MFA)	一種安全流程，要求使用者提供兩項或更多獨立的憑證以驗證其身分。
網路分段	將電腦網絡劃分為多個子網路，以提升安全性與效能。
修補程式管理	透過套用修補程式（patches）來解決漏洞或錯誤，以保持軟體最新的流程。
個人數據	任何與已識別或可識別之個人有關的資訊，例如姓名、身分證號碼或聯絡資料。
實體存取控制	用於限制進入建築物、房間或其他敏感區域的措施。
權限／特權存取	授予需執行管理或敏感任務之使用者的高階系統存取權限。
勒索軟體	一種惡意軟體，會鎖定或加密受害者的數據，並要求支付贖金以解鎖數據。

術語	定義
遠端存取	指從學校實體場地外部存取學校 IT 系統或數據的能力，通常透過 VPN 或安全連線實現。
敏感數據	一旦洩露可能對個人或學校造成損害的數據，例如健康紀錄或紀律處分報告。
供應商	向學校供應貨品或服務的任何第三方供應商或服務提供者，尤其是那些能夠存取數據或系統的供應商。
使用者	任何獲授權使用學校資訊科技資源的教職員、學生或其他人士。
漏洞	系統、軟體或流程中的弱點，可能被利用以危害安全性。
無線安全	為保護無線（Wi-Fi）網路免受未經授權的存取或攻擊而實施的存取控制措施與實務做法。

類別	檢查清單項目	優先級	指引／範例	實施狀態
治理與合規	2.1 法律與法規遵循	P1	遵守《個人資料（私隱）條例》（第 486 章）及個人資料私隱專員公署（PCPD）的要求（個人資料的收集、使用、儲存及披露），以符合個人資料私隱專員公署（PCPD）的規定	
治理與合規	2.1 法律與法規遵循	P2	遵守教育局（EDB）相關通告／指引（例如《學校資訊保安 — 建議做法》）。	
治理與合規	2.1 法律與法規遵循	P2	遵守其他適用法例及標準（例如：《版權條例》、《電腦罪行條例》、行業守則）。	
治理與合規	2.1 法律與法規遵循	P2	顯示器顯示法例／指引的變動，並確保政策與實務持續符合規定。	
治理與合規	2.2 政策管理與檢討	P2	取得學校管理層／管治機構對網絡安全政策／程序的正式批准。	
治理與合規	2.2 政策管理與檢討	P2	至少每年或於發生重大變更（技術、法律、運作）時檢討政策。	
治理與合規	2.2 政策管理與檢討	P3	對所有政策進行版本控制（批准日期、更新、審查）。	
治理與合規	2.2 政策管理與檢討	P1	向教職員、學生及第三方傳達政策；視需要提供培訓與宣導。	
治理與合規	2.2 政策管理與檢討	P3	利用回饋、事件及稽核結果推動持續改善。	
治理與合規	2.2 政策管理與檢討	P1	高階領導層須對資訊保安的政策管理、合規性及治理負責。	
資產管理	3.1 資訊科技資產清單	P1	維護所有 IT 資產的最新清單；將整體責任指派給 IT 協調員／學校秘書。	
資產管理	3.1 資訊科技資產清單	P2	建立並維護一份文件編製的安全配置流程，適用於學校 IT 部門管理的所有 IT 資產與設備，包括硬件、軟體及網路設備。	
資產管理	3.1 資訊科技資產清單	P2	確保清單包含硬件、軟體／授權及雲端服務。	
資產管理	3.1 資訊科技資產清單	P2	當資產被購置、重新分配或報廢時，應更新清單。	
資產管理	3.1 資訊科技資產清單	P2	至少每年或每半年審查一次資產清單。	
資產管理	3.1 資訊科技資產清單	P1	使用既定的追蹤方法/工具 [例如：試算表、資產管理系統]。	
資產管理	3.1 資訊科技資產清單	P2	遵循資產歸還與安全處置程序（例如：處置前進行安全擦除）。	
資產管理	3.1 資訊科技資產清單	P1	建立定期（每週、每兩週）的流程，以移除或拒絕學校網路中的未授權資產。	
資產管理	3.1 資訊科技資產清單	P1	每月檢視軟體資產清單，確保其獲得積極支援，並移除任何裝置上存在的未經授權軟體。	
資產管理	3.2 數據分類與處理	P1	建立並維護數據管理流程及數據清單。內容應涵蓋以下項目 • 數據擁有人 • 數據保存期限與銷毀要求 • 數據分類與處理； 數據分類至少應分為「機密」、「內部」或「公開」。 • 機密（例如：學生健康紀錄、紀律處分報告） • 內部（例如：教職員備忘錄、課程計畫草稿） • 公開（例如：學校通訊、活動傳單）	
資產管理	3.2 數據分類與處理	P1	將機密／內部數據的存取權限限制於授權人員／職務，例如教師、行政人員、IT 管理員等。可透過數據存取控制清單（ACL）來實現。	
資產管理	3.2 數據分類與處理	P1	對敏感數據採取適當的保護措施（例如：數據加密工具、密碼保護）。	
資產管理	3.2 數據分類與處理	P1	對共用資料夾實施最小權限存取控制清單，限制學生及教職員對數據的存取權限。	
資產管理	3.2 數據分類與處理	P3	至少每半年或每年檢視一次數據分類與處理規範。	
資產管理	3.2 數據分類與處理	P2	安全地刪除／銷毀不再需要的數據（例如：數位碎紙；銷毀列印清單）。	
存取控制	4.1 使用者帳戶管理	P1	建立並維護帳戶清單；包括使用者、管理員及服務帳戶。此清單應包含每個人的姓名、使用者名稱、啟用/停用日期及所屬部門。清單中的帳戶應按定期時程進行授權，至少每季一次。	
存取控制	4.1 使用者帳戶管理	P1	安全管理學校擁有的資產和軟體，透過安全的網路協定配置軟體和裝置設定。此外，應停用預設帳戶並防止其被使用。	
存取控制	4.1 使用者帳戶管理	P2	將使用者帳戶管理責任指派給 IT 協調員或管理員。	
存取控制	4.1 使用者帳戶管理	P1	確保每位使用者皆擁有唯一的使用者 ID；落實個人責任制。	
存取控制	4.1 使用者帳戶管理	P2	透過正式流程（使用存取申請系統或 IT 工單系統）來建立、修改或撤銷帳戶。	
存取控制	4.1 使用者帳戶管理	P2	至少每年或每半年審查一次有效帳戶；停用或移除閒置帳戶（例如，90 天未活動）。	
存取控制	4.1 使用者帳戶管理	P1	當使用者離職或職務變更時，應立即撤銷其存取權限。若帳戶連續 45 天未使用，應停用該休眠帳戶。	
存取控制	4.2 特權存取	P1	建立專用的管理員帳戶，該帳戶應使用僅限管理員的憑證及提升的權限，且不得用於日常常規運作。	
存取控制	4.2 特權存取	P2	在建立帳戶或授予特定使用者權限前，應維持簡明的申請/核准程序。	
存取控制	4.2 特權存取	P1	特權帳戶僅用於管理任務；不得用於例行活動。	
存取控制	4.2 特權存取	P2	避免在終端設備上授予本地管理員權限；如有必要，須取得 IT 安全主管或同等職位人員的批准，並進行文件編製及定期審查。	
存取控制	4.2 特權存取	P1	要求所有管理存取帳戶（無論是現場管理或透過服務供應商管理）皆須註冊多因素驗證。	
存取控制	4.2 特權存取	P2	特權存取必須經由 IT 資安負責人/IT 管理員申請並核准。	
存取控制	4.2 特權存取	P1	為特權與非特權活動分別維護獨立的憑證。	
存取控制	4.2 特權存取	P2	使用中央日誌平台（例如 SIEM 或日誌伺服器）記錄並定期審查特權操作。	
存取控制	4.3 密碼政策	P1	強制執行最低密碼長度 [例如 8 個以上字符]及複雜度（包含字母、數字、符號）。	
存取控制	4.3 密碼政策	P1	防止使用常見或弱密碼，禁止共享密碼，並禁止在不同的學校系統中重複使用密碼。	
存取控制	4.3 密碼政策	P3	要求定期變更密碼，至少每 [例如 90 天] 一次，或根據風險評估進行調整。	
存取控制	4.3 密碼政策	P1	在 [例如 5] 次登入失敗後實施帳戶鎖定。	
存取控制	4.3 密碼政策	P2	安全儲存密碼（進行雜湊運算和/或加密）。	
存取控制	4.3 密碼政策	P1	在可行情況下，為敏感帳戶/系統啟用身分驗證方法，例如多因素驗證 (MFA)。	
存取控制	4.4 遠端及第三方存取	P1	要求使用安全的通道進行遠端存取（例如：VPN、加密連線）。	
存取控制	4.4 遠端及第三方存取	P1	要求所有形式的遠端存取均須使用 MFA 服務進行驗證並協助使用者登入。	
存取控制	4.4 遠端及第三方存取	P2	僅在獲得 IT 管理員明確批准，且範圍與期限明確界定的情況下，才授予遠端/第三方存取權限。	
存取控制	4.4 遠端及第三方存取	P2	記錄並審查所有第三方存取活動。	
存取控制	4.4 遠端及第三方存取	P1	任務完成後，應立即撤銷臨時/緊急存取權限。	
網路安全	5.1 網路分段	P1	使用分段方法（例如 VLAN、獨立的 Wi-Fi SSID）將內部網路（例如管理員、學生、訪客）進行分段。	
網路安全	5.1 網路分段	P1	使用私有 IP；防止內部系統直接連接到互聯網。	
網路安全	5.1 網路分段	P1	僅允許授權裝置進入各區段；禁止未受管理/個人裝置進入員工/管理員網路。	
網路安全	5.1 網路分段	P3	至少每年或每半年檢視一次分段與存取控制。	
網路安全	5.2 防火牆與邊界安全	P1	在互聯網通訊閘及關鍵區段之間部署並維護防火牆，並採用不同類型的防火牆，例如硬件防火牆、基於雲端的防火牆解決方案。此外，應考慮在終端使用者裝置上實施防火牆解決方案。	

網路安全	5.2 防火牆與邊界安全	P1	預設拒絕所有流量；僅允許經批准的服務/埠，例如 HTTPS、電子郵件 (SMTP)。	
網路安全	5.2 防火牆與邊界安全	P2	檢視/更新防火牆規則並監控日誌（透過防火牆日誌伺服器，如有 SIEM 則透過 SIEM）。	
網路安全	5.2 防火牆與邊界安全	P2	在所有裝置上移除或停用未使用的網路服務/功能。	
網路安全	5.3 無線安全	P1	使用強效的 Wi-Fi 加密（WPA3；若不可用則使用 WPA2）。	
網路安全	5.3 無線安全	P1	設定並定期更新強效 Wi-Fi 密碼；避免廣泛分享。	
網路安全	5.3 無線安全	P2	確保全校網路基礎架構保持最新狀態；運行最新穩定版軟體，並定期（每兩週、每月）檢視以確認軟體支援狀況。	
網路安全	5.3 無線安全	P2	使用驗證方法控制 Wi-Fi 存取控制，例如 MAC 篩選、使用者驗證入口網站。	
網路安全	5.3 無線安全	P1	提供獨立的訪客 Wi-Fi 網路，僅限於受限的互聯網存取。	
網路安全	5.3 無線安全	P3	至少每月或每季顯示未經授權/非法的 AP/裝置。	
網路安全	5.3 無線安全	P2	強制執行行動裝置的安全設定（密碼/PIN碼、停用不必要的功能）。	
網路安全	5.3 無線安全	P2	提醒使用者勿在公共 Wi-Fi 上存取敏感的學校數據。	
端點與裝置安全	6.1 學校自有裝置	P2	依照政策保護及管理所有學校自有裝置。	
端點與裝置安全	6.1 學校自有裝置	P1	使用最新的安全控制措施（例如：防惡意軟件、防火牆、安全更新）。在所有終端使用者裝置上啟用 DNS 過濾服務。	
端點與裝置安全	6.1 學校自有裝置	P2	確保校方裝置僅允許使用獲得完整技術支援且為最新版本的網頁瀏覽器與電子郵件客戶端，並移除或封鎖過時版本。	
端點與裝置安全	6.1 學校自有裝置	P1	為學校裝置配置惡意軟件防禦簽名檔的自動更新。	
端點與裝置安全	6.1 學校自有裝置	P1	僅允許授權使用者使用；禁止共用帳號/密碼。	
端點與裝置安全	6.1 學校自有裝置	P1	配置閒置後自動鎖定 [例如 10 – 15 分鐘]。	
端點與裝置安全	6.1 學校自有裝置	P2	停用可移除媒體裝置的自動執行與自動播放功能。	
端點與裝置安全	6.1 學校自有裝置	P1	定期套用安全性更新 [例如：自動更新或至少每月一次]。	
端點與裝置安全	6.1 學校自有裝置	P1	若裝置遺失、遭竊或遭入侵，請立即向 IT 協調員/管理員通報。	
端點與裝置安全	6.2 自帶設備（BYOD）	P2	要求用於學校事務的個人裝置必須符合安全要求。	
端點與裝置安全	6.2 自帶設備（BYOD）	P2	僅在已實施安全控制措施（例如裝置密碼、最新的作業系統和安全軟體、註冊流動裝置管理等）的情況下，才允許從個人裝置存取敏感資料/系統。	
端點與裝置安全	6.2 自帶設備（BYOD）	P3	保留限制/撤銷不符合規範之裝置存取權限的權利。	
端點與裝置安全	6.2 自帶設備（BYOD）	P1	要求使用者確保其裝置安全，並立即向 IT 管理員報告事件。	
端點與裝置安全	6.2 自帶設備（BYOD）	P1	除非獲得授權，否則禁止在個人裝置上儲存或進行機密數據的處理。	
端點與裝置安全	6.3 流動裝置管理	P3	實施合理措施，以管理／保護存取學校資料的行動裝置。	
端點與裝置安全	6.3 流動裝置管理	P3	盡可能使用 MDM 解決方案 [例如 Intune、Apple School Manager] 來執行管控。	
端點與裝置安全	6.3 流動裝置管理	P2	若無 MDM，應建立替代程序（強密碼、加密、遠端清除功能）。	
端點與裝置安全	6.3 流動裝置管理	P3	限制或撤銷不符合規範裝置的存取權限。	
端點與裝置安全	6.3 流動裝置管理	P3	至少每年或每半年檢視一次裝置的安全控制措施與合規狀況。	
數據保護	7.1 數據加密	P1	在可行情況下，使用適當的加密（例如：全磁碟加密、加密共用資料夾、SSL/TLS）來保護靜止數據和傳輸中的數據。	
數據保護	7.1 數據加密	P3	若無法進行加密，則應實施其他降低風險的措施。	
數據保護	7.1 數據加密	P2	除非已獲准並採取緩解措施，否則請勿將敏感數據儲存於無法加密的裝置上。	
數據保護	7.1 數據加密	P2	安全管理加密金鑰；僅限授權人員存取。	
數據保護	7.2 數據備份與復原	P1	請定期（至少每日/每週）備份關鍵數據，並盡可能使用備份方法（自動備份軟體、雲端備份服務）。	
數據保護	7.2 數據備份與復原	P1	確保至少有一份離線/隔離的備份副本，此備份可每月更新，或按學校認為必要的時間間隔進行更新。	
數據保護	7.2 數據備份與復原	P2	若無自動化/雲端備份，請使用手動程序；並妥善保管備份媒體。	
數據保護	7.2 數據備份與復原	P1	保護備份副本（例如：加密、異地/雲端儲存服務、限制存取）。	
數據保護	7.2 數據備份與復原	P2	每年或每半年進行定期備份還原測試。	
數據保護	7.2 數據備份與復原	P2	視需要檢視並更新備份/還原程序。	
數據保護	7.3 數據外洩防護 (DLP)	P3	實施措施以降低意外／未經授權的數據遺失／洩露風險。	
數據保護	7.3 數據外洩防護 (DLP)	P3	在可行情況下，應採用技術性 DLP 控制措施（例如：DLP 軟體、電子郵件過濾、存取限制）。	
數據保護	7.3 數據外洩防護 (DLP)	P2	若無技術性 DLP 措施，則應仰賴員工意識提升／培訓，並制定明確的處理／分享政策。	
數據保護	7.3 數據外洩防護 (DLP)	P1	禁止透過不安全的管道（例如：個人電子郵件、未加密的 USB 隨身碟）傳送敏感資訊。	
數據保護	7.3 數據外洩防護 (DLP)	P1	如有實際或疑似數據遺失，請立即向 IT 管理員通報。	
供應商與第三方管理	8.1 供應商安全要求	P1	建立並維護第三方服務供應商清單，包括其分類（提供的服務、優先級等）。每年及／或發生重大變更時，應檢視並更新該清單。	
供應商與第三方管理	8.1 供應商安全要求	P2	確保供應商遵守學校的資訊保安與數據保護要求。	
供應商與第三方管理	8.1 供應商安全要求	P2	根據數據／系統／服務的敏感程度，量身訂製供應商的安全要求。	
供應商與第三方管理	8.1 供應商安全要求	P3	在可行情況下，要求供應商證明其具備安全控制措施（例如 ISO 27001、存取控制、安全處理）。	
供應商與第三方管理	8.1 供應商安全要求	P3	若供應商無法符合標準，應評估風險並實施補償性控制措施。	
供應商與第三方管理	8.1 供應商安全要求	P2	將管理供應商安全的責任指派給特定職位，例如數據保護官、IT 協調員或學校業務經理。	
供應商與第三方管理	8.2 盡職調查與合約	P1	在簽約或續約前評估供應商的安全能力（例如：問卷調查、參考資料、認證）。	
供應商與第三方管理	8.2 盡職調查與合約	P2	在可能的情況下，將數據保護／安全條款納入合約中（機密性、違規通知、稽核、資料歸還／刪除）。	
供應商與第三方管理	8.2 盡職調查與合約	P2	若無法納入詳細條款，應記錄相關風險並建立替代性保障措施。	
供應商與第三方管理	8.2 盡職調查與合約	P2	要求供應商將實際或疑似的安全事件立即通報給指定職位，例如數據保護官、IT 協調員。	
雲端服務安全	9.1 核准雲端服務清單	P2	僅使用經 IT 協調員及支援人員核准的雲端服務。	
雲端服務安全	9.1 核准雲端服務清單	P2	維持一份最新的核准雲端服務清單。[Google Workspace for Education、Microsoft 365、核准的學習平台]	
雲端服務安全	9.1 核准雲端服務清單	P1	禁止在未經核准的雲端服務上儲存或進行數據共用。	
雲端服務安全	9.1 核准雲端服務清單	P3	至少每年或每半年審查/更新核准服務清單。	
雲端服務安全	9.2 雲端數據保護	P1	保護敏感/機密雲端資料（靜態/傳輸中加密、嚴格的存取控制、分類）。	
雲端服務安全	9.2 雲端數據保護	P1	若服務可用，請啟用雲端服務存取的多重驗證 (MFA)。	
雲端服務安全	9.2 雲端數據保護	P3	若服務缺乏足夠的保護措施，應避免儲存敏感數據，或採取替代性防護措施（限制存取、匿名化、密碼保護檔案）。	
雲端服務安全	9.2 雲端數據保護	P2	將雲端數據保安的責任指派給 IT 協調員或同等職位。	
雲端服務安全	9.3 雲端存取與監控	P1	將雲端存取權限限制於授權使用者/角色，並定期（每年/每半年）進行審查。	
雲端服務安全	9.3 雲端存取與監控	P2	在可行情況下，監控雲端使用狀況以偵測未經授權的活動（例如：可疑登入、數據下載、外部分享）。	
雲端服務安全	9.3 雲端存取與監控	P3	若無法進行技術監控，請實施替代措施（提高意識、人工審查、明確報告）。	
雲端服務安全	9.3 雲端存取與監控	P1	立即向 IT 協調員報告疑似或實際發生的雲端安全事件。	
生成式人工智慧的使用	10.1 核准的人工智慧工具	P2	僅可使用經資訊科技協調員核准的生成式 AI 工具，並視需要安裝相關安全修補程式。	

生成式人工智慧的使用	10.1 核准的人工智慧工具	P2	維護一份獲准使用的人工智慧工具清單，例如 Microsoft Copilot、Google Gemini、OpenAI ChatGPT 及其他獲准的平台。	
生成式人工智慧的使用	10.1 核准的人工智慧工具	P1	切勿使用未經批准的 AI 工具來進行數據處理、儲存或生成學校數據，亦不得藉此提供學校網路存取權限。	
生成式人工智慧的使用	10.1 核准的人工智慧工具	P3	至少每年或每半年審查/更新核准的 AI 工具清單。	
生成式人工智慧的使用	10.2 人工智慧使用中的數據保護	P1	除非該工具已獲核准且供應商具備充分的數據保護措施，否則請勿將敏感/個人數據輸入 AI 工具。	
生成式人工智慧的使用	10.2 人工智慧使用中的數據保護	P2	確保使用者在使用 AI 工具時能進行數據保護。	
生成式人工智慧的使用	10.3 監控與管控	P3	顯示生成式 AI 工具的使用情況，以確保符合政策規定，並防止不當或未經授權的使用。	
生成式人工智慧的使用	10.3 監控與管控	P3	在可行情況下，實施技術控制措施（使用記錄、存取控制、內容過濾）以監控／管控 AI 的使用。	
生成式人工智慧的使用	10.3 監控與管控	P3	若無法進行技術監控，請採用替代措施（宣導、人工檢查、明確通報）。	
生成式人工智慧的使用	10.3 監控與管控	P1	若懷疑有人濫用 AI 工具或發生與 AI 相關的數據外洩事件，請立即向 IT 協調員報告。	
使用者意識與培訓	11.1 資安意識計畫	P1	以資源許可的適當形式，定期為所有使用者提供資訊保安意識培訓。	
使用者意識與培訓	11.1 資安意識計畫	P2	培訓教職員與學生，使其懂得辨識並通報裝置是否缺少安全性更新，或自動修補工具似乎失效的情況。	
使用者意識與培訓	11.1 資安意識計畫	P1	涵蓋關鍵主題（數據保護、密碼、網路釣魚、不安全公共網路的危險性，以及事件通報）。	
使用者意識與培訓	11.1 資安意識計畫	P2	若無法進行正式/自動化培訓，請採用替代方法（海報、會議、電子報）。	
使用者意識與培訓	11.1 資安意識計畫	P3	至少每年或每半年檢視／更新意識宣導材料／課程。	
使用者意識與培訓	11.1 資安意識計畫	P1	指派資訊科技協調員負責統籌相關宣導工作。	
使用者意識與培訓	11.2 可接受使用政策	P1	要求所有使用者遵守《可接受使用政策》（AUP）。	
使用者意識與培訓	11.2 可接受使用政策	P1	在註冊/入職時傳達《可接受使用政策》，並透過定期提醒進行溝通；在可行情況下取得確認。	
使用者意識與培訓	11.2 可接受使用政策	P2	針對年幼學生，採用替代性溝通方式（例如：課堂討論、教師提醒）。	
使用者意識與培訓	11.2 可接受使用政策	P1	透過學校紀律程序處理違反《可接受使用政策》的情況。	
使用者意識與培訓	11.3 外部培訓管道	P3	在可行情況下善用外部資源：數碼政策辦公室（DPO）的相關措施。	
使用者意識與培訓	11.3 外部培訓管道	P3	在可行情況下利用外部資源：香港教育局（EDB）的指引／培訓。	
使用者意識與培訓	11.3 外部培訓管道	P3	在可行情況下善用外部資源：HKCERT 的警報／資源／工作坊。	
使用者意識與培訓	11.3 外部培訓管道	P3	在可行情況下利用外部資源：HKIRC 資源（網絡安全培訓集線器、健康網絡、釣魚電郵演習）。	
事故管理	12.1 事件通報	P1	要求透過電子郵件、電話、事件報告表等各種報告方式，向 IT 協調員即時報告實際或可疑的事件。	
事故管理	12.1 事件通報	P1	透過海報、員工會議及線上資源，提供關於識別及通報事件的明確指引。	
事故管理	12.1 事件通報	P1	若無正式系統，可允許向教師／主管報告以進行升級處理。	
事故管理	12.2 事件應變與復原	P1	應迅速回應事件，以進行控制、調查及修復。	
事故管理	12.2 事件應變與復原	P2	在可能的情況下，使用已文件編製的程序/檢查清單進行應對/恢復（例如：隔離裝置、重設密碼、還原備份）。	
事故管理	12.2 事件應變與復原	P2	若無正式程序／工具，應採取合理措施以迅速控制／保護／恢復。	
事故管理	12.2 事件應變與復原	P2	透過 IT 協調員與受影響方／家長／主管機關協調溝通。	
事故管理	12.2 事件應變與復原	P2	備妥流程／聯絡資訊，以便在適當情況下向 HKCERT 通報。	
事故管理	12.2 事件應變與復原	P1	維護流程／聯絡資訊，以便向香港警方報告涉嫌犯罪／僅受影響的個案。	
事故管理	12.2 事件應變與復原	P1	備妥流程／聯絡資訊，以便在可能造成傷害／困擾的個人數據外洩事件發生時通知私隱專員公署。	
事故管理	12.2 事件應變與復原	P2	若內部資源不足以處理／從事件中恢復，應尋求合資格的外部專家協助。	
事故管理	12.3 事件後檢討	P3	在發生重大事件後進行事後檢討，以釐定成因及改進措施。	
事故管理	12.3 事件後檢討	P3	盡可能將調查結果／經驗教訓記錄在案，並與相關員工分享。	
事故管理	12.3 事件後檢討	P3	至少在員工會議中討論事件，並實施基本的糾正措施。	
事故管理	12.3 事件後檢討	P3	根據檢討結果更新政策／程序。	
監控與記錄	13.1 系統與網路監控	P2	在可行情況下，利用不同的監控方法、內建警報、安全軟體及防火牆日誌，監控關鍵系統／網路活動，以防未經授權的存取／濫用／事件。	
監控與記錄	13.1 系統與網路監控	P2	監控重點應放在關鍵資產和敏感數據上（例如：管理伺服器、學生資訊系統、雲端平台）。	
監控與記錄	13.1 系統與網路監控	P3	若無自動化工具，請定期手動檢查／審閱使用報告及使用者活動。	
監控與記錄	13.1 系統與網路監控	P2	將監控責任指派給 IT 協調員或系統管理員。	
監控與記錄	13.2 記錄管理與審查	P1	在可行情況下，使用記錄工具（例如伺服器日誌、防火牆日誌和雲端審計追蹤）來維護關鍵活動（登入、檔案存取、敏感數據變更）的日誌。	
監控與記錄	13.2 記錄管理與審查	P2	建立並維護一份書面記錄管理流程，其中應定義學校的日誌記錄要求，並定期進行審查，以及／或在發生重大變更時進行審查。	
監控與記錄	13.2 記錄管理與審查	P2	保護日誌免遭未經授權的存取、修改或刪除。	
監控與記錄	13.2 記錄管理與審查	P2	將日誌保留一段既定的保存期限（例如每季／每年），以支援調查／稽核／監管需求。	
監控與記錄	13.2 記錄管理與審查	P3	在保留期結束後安全刪除日誌，除非正在進行的調查需要保留。	
監控與記錄	13.2 記錄管理與審查	P2	定期（每月/每季）檢視日誌，以偵測可疑活動/政策違規。	
監控與記錄	13.2 記錄管理與審查	P3	若無自動化事件記錄工具，則進行手動審查並記錄與安全相關的事件。	
監控與記錄	13.2 記錄管理與審查	P1	將日誌審查中發現的重要結果/事件立即報告給 IT 協調員。	
實體與環境安全	14.1 實體存取控制	P1	將敏感區域（伺服器機房、員工工作區、檔案儲存區）的進出權限限制於授權人員。	
實體與環境安全	14.1 實體存取控制	P1	明確標示區域為公眾、員工專用或限制進入；並據此進行存取控制。	
實體與環境安全	14.1 實體存取控制	P1	在可行情況下使用實體存取控制措施（鎖具、門禁卡、進出登記簿）。	
實體與環境安全	14.1 實體存取控制	P2	若先進的控制措施的可用性低，請採用替代方案（人工監督、上鎖的櫃子、人員駐守）。	
實體與環境安全	14.1 實體存取控制	P2	監督並記錄訪客進入敏感區域的情況（例如：訪客登記簿）。	
實體與環境安全	14.1 實體存取控制	P1	將實體進出管理責任指派給 IT 協調員／管理員。	
實體與環境安全	14.2 設備安全	P1	保護存有敏感資訊的設備，防止遭竊、遺失或損壞。	
實體與環境安全	14.2 設備安全	P1	將設備放置於安全地點（上鎖的房間、遠離公共區域），並在可行時採取實體防護措施（纜繩鎖、上鎖的櫃子）。	
實體與環境安全	14.2 設備安全	P2	若無法採取進階措施，請使用實用的替代方案（定期檢查、下班後上鎖存放）。	
實體與環境安全	14.2 設備安全	P1	若設備遺失、遭竊或損壞，應立即向 IT 管理員通報。	
實體與環境安全	14.2 設備安全	P2	在處置或移交設備前，務必確保已安全刪除數據。	
維護與修補程式管理	15.1 軟體更新	P1	確保所有系統／軟體皆安裝最新的安全性更新／修補程式。	
維護與修補程式管理	15.1 軟體更新	P1	在可能的情況下，啟用作業系統、應用程式及安全工具的自動更新功能。	
維護與修補程式管理	15.1 軟體更新	P2	若無自動更新功能，請實施手動流程（排程檢查、更新日誌）。	
維護與修補程式管理	15.1 軟體更新	P1	在關鍵安全性更新發布後，應盡快進行安裝。	

維護與修補程式管理	15.1 軟體更新	P2	除非已進行風險評估並實施補償性控制措施，否則應避免使用已達生命週期終止的系統／軟體。	
維護與修補程式管理	15.1 軟體更新	P2	將第三方雲端／SaaS 平台納入更新／漏洞管理範圍（透過驗證供應商實務或合約條款確認）。	
維護與修補程式管理	15.1 軟體更新	P2	將軟體更新的責任指派給 IT 管理員。	
維護與修補程式管理	15.2 漏洞管理	P1	定期檢查系統／軟體是否存在已知漏洞（掃描工具、手動檢查、供應商通知）。	
維護與修補程式管理	15.2 漏洞管理	P3	在可用性高的情況下，使用漏洞管理工具來識別/優先處理風險。	
維護與修補程式管理	15.2 漏洞管理	P2	若無自動化工具，請監控可信來源（供應商網站、政府公告）並視需要採取行動。	
維護與修補程式管理	15.2 漏洞管理	P2	及時評估/處理已識別的漏洞，並優先處理風險最高的項目。	
維護與修補程式管理	15.2 漏洞管理	P2	向 IT 協調員報告重大風險/未解決的問題。	
維護與修補程式管理	15.2 漏洞管理	P3	評估潛在影響，並在可行情況下於部署前測試重大更新。	
維護與修補程式管理	15.3 變更管理	P3	在實施前，由 IT 協調員審查/批准重大的 IT 變更。	
維護與修補程式管理	15.3 變更管理	P3	記錄重大變更（日期、性質、負責人）。	
維護與修補程式管理	15.3 變更管理	P3	在可行情況下測試變更，以將中斷影響降至最低。	
維護與修補程式管理	15.3 變更管理	P1	要求員工立即通報因變更所引起的問題。	
政策例外與違規	16.1 例外處理程序	P2	須以書面形式向 IT 協調員提交例外申請，並附上理由及補償性控制措施。	
政策例外與違規	16.1 例外處理程序	P2	由負責啟動例外批准的人員在批准前審查並批准例外。	
政策例外與違規	16.1 例外處理程序	P2	將已批准的例外情況（範圍、期限、條件）記錄在案。	
政策例外與違規	16.1 例外處理程序	P3	應定期（例如每年）或視需要審查例外情況，以確認其持續必要性。	
政策例外與違規	16.2 紀律處分	P2	針對政策違規或未經授權的例外情況，應依照學校程序採取紀律處分。	
政策例外與違規	16.2 紀律處分	P2	在決定處分時，應考量意圖、嚴重程度及影響。	
政策例外與違規	16.2 紀律處分	P3	如遇潛在的法律/法規違規情況，應按要求向相關主管機關報告。	
文件控制	17.1 政策審查與更新歷史	不適用	至少每年/每半年或於發生重大變更時，檢討/更新本政策。	
文件控制	17.1 政策審查與更新歷史	不適用	將審查／更新的責任指派給 IT 協調員。	
文件控制	17.1 政策審查與更新歷史	不適用	記錄所有政策版本（生效日期、變更摘要、負責人）。	
文件控制	17.1 政策審查與更新歷史	不適用	將先前政策版本保留一段既定保存期限，例如 3 年。	
文件控制	17.1 政策審查與更新歷史	不適用	現行經核准的政策可用於教職員，並視情況提供予學生／家長。	

註：優先級排序（P1–P4）是基於常見安全實務及對學校環境有限資訊的一般性建議。這些並非法律、法規或專業建議，亦不保證能預防事件發生或確保合規。學

實施摘要	總計	已實施數量	實施率
P1 - 立即執行 此為最高優先級事項，須實施並納入為基礎安全層級，被視為維護安全環境的關鍵	84	0	0%
P2 - 下一步 有助於維持安全的重要防護措施，所需投入的精力雖不高，但仍能填補漏洞	83	0	0%
P3 - 稍後 用於加強保護的額外防護措施，這些措施能提升成熟度與運作節奏，實施時對資源/時間的負擔屬中等	42	0	0%

網絡安全政策範本

[貴校名稱]

版本 X.X

編製者：	[姓名]，[職稱]，[學校名稱]
核准／生效日期：	日/月/年

本文件僅作為參考範本提供。各校在實施前，必須審閱、適配並核准內容，以符合自身環境、資源及需求。發行單位對於基於本範本所採取的任何行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 前言 7
1.1. 目的 7
1.2. 適用範圍 7
1.3. 定義 7
1.4. 角色與職責 8
2. 治理與合規 9
2.1. 法律與法規合規 9
2.2. 政策管理與檢討 9
3. 資產管理 10
3.1. IT 資產清單 10
3.2. 數據分類與處理 10
4. 存取控制 11
4.1. 使用者帳戶管理 11
4.2. 特權存取 11
4.3. 密碼政策 11
4.4. 遠端及第三方存取 12
5. 網路安全 13
5.1. 網路分段 13
5.2. 防火牆與邊界安全 13
5.3. 無線安全 13
6. 端點與裝置安全 14
6.1. 學校自有裝置 14
6.2. 自攜設備 (BYOD) 14
6.3. 流動裝置管理 15
7. 數據保護 16
7.1. 數據加密 16
7.2. 數據備份與復原 16
7.3. 數據外洩防護 (DLP) 17
8. 供應商與第三方管理 18

8.1. 供應商安全要求 18
8.2. 盡職調查與合約要求 18
9. 雲端服務安全 19
9.1. 核准雲端服務清單 19
9.2. 雲端數據保護 19
9.3. 雲端存取與監控 19
10. 生成式人工智能的使用 20
10.1. 經核准的人工智能工具 20
10.1a. 禁止內容 20
10.2. AI 使用中的數據保護 20
10.3. 監控與管控 21
10.4. 公平性考慮 21
11. 使用者意識與培訓 22
11.1. 資安意識計畫 22
11.2. 可接受使用政策 22
11.3. 外部培訓管道 23
12. 事故管理 24
12.1. 事件通報 24
12.2. 事件應變與復原 24
12.3. 事後檢討 24
13. 監控與記錄 26
13.1. 系統與網路監控 26
13.2. 記錄管理與審查 26
14. 實體與環境安全 27
14.1. 實體存取控制 27
14.2. 設備安全 27
15. 維護與修補程式管理 28
15.1. 軟體更新 28
15.2. 漏洞管理 28
15.3. 變更管理 28
16. 政策例外與違規 29
16.1. 例外處理程序 29

16.2. 紀律處分 29
17. 文件管控 30
17.1. 政策檢討與更新歷史 30
附錄 31
A. 其他參考資料 31
建議事項與優先級對應表 31
實務實施指南 45
網絡安全事件應變工作流程 45
安全配置檢查清單 46
B. 術語表 47

1. 前言

1.1. 目的

[範本註：請根據貴校的資訊安全目標自訂此部分。]

本網絡安全政策範本旨在協助學校制定、正式化及維護有效的資訊科技安全政策與實務。學校應根據自身獨特背景與營運需求，對本範本進行適配。

1.2. 適用範圍

[範本註：請根據貴校的環境及使用者群組更新適用範圍。]

本政策適用於 [插入學校名稱] 內的所有資訊科技資源、數據及使用者，包括：

- 全體教職員（含教學與非教學人員）
- 學生
- 第三方服務供應商
- 可存取學校管理之資訊科技系統的訪客及承包商

1.3. 定義

[範本註：請根據貴校情況調整或新增定義。]

- **資訊科技系統**：由學校管理或使用的所有數碼基礎設施、裝置、服務及應用程式，包括網路、伺服器、電腦及雲端資源。
- **數據保護**：為防止個人、敏感或機密資訊遭受未經授權的存取、揭露、變更或毀損而實施的措施與管控。
- **使用者**：所有可存取學校資訊科技系統之個人，包括教職員、學生及經授權之第三方。
- **網絡安全事件**：任何針對資訊或資訊系統所發生的未經授權存取、使用、揭露、干擾、修改或破壞之企圖或實際行為。

1.4. 角色與職責

[範本註：請根據貴校情況，為每個要點指派相應的責任。]

各校負責：

- 政策客製化：[插入負責角色] 將根據學校環境調整本範本。
- 核准與實施：[插入負責角色/委員會] 將核准並確保本政策得以實施。
- 培訓：[填入負責人] 將為教職員及學生提供必要的培訓。
- 持續檢討：[填入負責人] 將定期檢討並更新本政策。
- 政策治理：[填入負責人] 將對政策遵循情況負責。

x 註：範例中提及的特定工具或控制措施僅供說明之用，並不構成任何背書。各校須對其資訊科技環境及合規狀況承擔全部責任。

2. 治理與合規

2.1. 法律與法規合規

學校必須遵守香港所有適用於資訊保安及數據保護的法律、法規及指引。主要要求包括：

- 《個人資料（私隱）條例》（第 486 章）：學校須按照個人資料私隱專員公署（PCPD）的要求，保護學生、教職員及其他持份者的個人資料。這包括妥善收集、使用、儲存及披露個人資料。
- 教育局通告及指引：學校應遵守相關教育局通告，例如《學校資訊保安 — 建議做法》，以及任何發布的更新或特定行業的指引。
- 其他適用法例及標準：學校應知悉並遵守任何其他相關的法律或規管要求，例如《版權條例》、《電腦罪行條例》及特定行業的實務守則。

學校有責任監察相關法例及指引的變動，並確保所有資訊科技政策及做法均符合規定。

2.2. 政策管理與檢討

- **政策批准**：所有網絡安全政策及程序在實施前，必須經學校管理層或管治機構正式批准。
- **定期檢討**：應至少每年檢討一次政策，或在技術、法律要求或運作需求發生重大變化時進行檢討。
- **版本控制**：學校應保存所有政策版本的記錄，包括批准、更新及檢討日期。
- **溝通與宣導**：應向全體教職員、學生及相關第三方提供相關資訊，並視需要進行適當的培訓與宣導活動。
- **持續改進**：應利用教職員的回饋、事件報告及稽核結果，以識別可改進之處。應主動實施更新，以因應新的風險或合規要求。

註：學校高層領導最終須負責確保有效的政策管理、法律合規性，以及資訊保安的持續治理。

3. 資產管理

3.1. IT 資產清單

學校應維持所有資訊科技資產的最新清單，以支援有效的安全管理與合規性。

- [資訊負責人／職務，例如：IT 協調員、學校秘書] 負責監督及維護資產清單。
- 清單應包含所有由學校管理的關鍵 IT 資產，例如：
    - **硬件**（例如：筆記型電腦、桌上型電腦、網路交換器、平板電腦）
    - **軟體與授權**（例如：辦公室套裝軟體、防毒軟體訂閱）
    - **雲端服務**（例如：SaaS 平台、學習管理系統）
- 每當資產被購置、重新分配或報廢時，均應更新資產清單。
- 資產清單應至少每 [頻率，例如：每年/每半年] 進行一次審查。
- 學校可使用 [工具/方法，例如：試算表、資產管理系統] 進行資產清查追蹤。
- 當教職員、學生或承包商離職，或資產報廢時，應遵循資產歸還與安全處置程序（例如：處置前對硬碟進行安全擦除）。

3.2. 數據分類與處理

學校數據應根據敏感程度，並依照法律及法規要求進行分類與管理。

- 數據至少應分類為：
    - **機密性**（例如：學生健康紀錄、紀律處分報告）
    - **內部資料**（例如：教職員備忘錄、課程計畫草稿）
    - **公開資料**（例如：學校通訊、活動傳單）
- 機密及內部數據的存取權限僅限於 [授權人員/職務，例如：教師、行政人員]。
- 應採取適當的防護措施——例如 [加密工具、密碼保護]——以保護敏感數據。
- 應至少每 [頻率，例如每年] 檢視一次數據分類與處理方式。
- 對於不再需要的數據，應採用安全的刪除或銷毀方法（例如：數位碎紙軟體、銷毀列印清單）。

4. 存取控制

4.1. 使用者帳戶管理

- 將用戶帳戶管理的責任指派給 [角色，例如 IT 協調員/管理員]。
- 每位使用者必須擁有唯一的用戶 ID；凡以該 ID 執行之所有行動，均須由個人承擔責任。
- 使用者帳戶的建立、修改和撤銷，應透過正式流程，使用 [存取請求系統，例如：存取請求表單或 IT 票務系統] 進行。
- 至少每 [頻率，例如每年/每半年] 對有效帳戶進行定期審查，以移除或停用不再需要的帳戶（例如，在 [閒置天數，例如 90 天] 未使用後）。
- 當教職員、學生或承包商離開學校或變更職務時，應立即撤銷其存取權限。

4.2. 特權存取

- 特權帳戶（例如管理員）僅限用於管理任務，絕不可用於例行活動。
- 應盡可能避免在終端裝置（例如教職員或學生電腦）上授予本地管理員權限。若因特定目的需要本地管理員存取權限，必須經由 [批准角色，例如 IT 安全負責人、校長] 批准、正式進行文件編製，並定期進行審查。
- 特權存取權限必須由 [批准角色，例如：IT 安全主管、校長] 提出申請並核准。
- 特權活動與非特權活動應使用不同的憑證組合。
- 所有特權操作均應透過 [中央日誌平台，例如 SIEM 或日誌伺服器] 進行記錄並定期審查。

4.3. 密碼政策

對所有系統實施符合安全最佳實務的密碼政策：

- 最小長度：[例如 8 個字符]，需包含字母、數字及符號。
- 禁止使用常見或弱密碼，並嚴禁共享密碼。
- 要求至少每 [例如 90 天] 變更一次密碼，或依風險評估調整頻率。
- 連續輸入錯誤密碼 [例如：5] 次後，將實施帳戶鎖定。
- 安全儲存密碼（例如：進行雜湊運算和/或加密）。
- 在可行情況下，為敏感帳戶和系統啟用 [身分驗證方法，例如多重認證 (MFA)]。

4.4. 遠端及第三方存取

- 遠端存取學校系統時，必須使用安全通道（例如：VPN、加密連線）。
- 僅在獲得 [批准角色] 的明確批准，並明確界定範圍和期限的情況下，才授予遠端或第三方（例如供應商、承包商）存取權限。
- 所有第三方存取活動均須記錄並進行審查。
- 臨時或緊急存取權限必須在任務完成後立即撤銷。

5. 網路安全

學校應實施管控措施，以保護學校網路及資料免受未經授權的存取、干擾及網路威脅。這些管控措施適用於學校管理基礎架構上的所有網路區段、裝置及使用者。

5.1. 網路分段

- 內部網路必須進行分段，以 [分段方法，例如 VLAN、獨立的 Wi-Fi SSID] 將敏感區域（例如行政、學生和訪客網路）分開。
- 內部網路應採用私有（非公開）IP 位址進行設計；確保任何內部系統均無法直接從互聯網存取。
- 僅允許經授權的裝置連線至各網路區段；未受管或個人裝置不得連線至教職員／管理員網路。
- 至少每 [頻率，例如每年、每半年] 檢視一次網路分段與存取控制。

5.2. 防火牆與邊界安全

- 在學校的互聯網通訊閘以及關鍵網路區段之間，部署並維護網路防火牆，使用 [防火牆類型，例如：硬件防火牆、雲端防火牆解決方案]。
- 預設情況下，阻擋所有進出網路流量，惟 [經核准的服務/埠，例如 HTTPS、電子郵件 (SMTP)] 除外。
- 定期檢視並更新防火牆規則，並透過 [中央日誌平台，例如：防火牆日誌伺服器、SIEM] 顯示日誌以偵測未經授權的活動。
- 移除或停用所有裝置上未使用的網路服務與功能。

5.3. 無線安全

- 所有學校無線網路必須採用強加密 [加密標準，例如 WPA3；若不可用，則使用 WPA2]。
- 設定並定期更新強效的 Wi-Fi 密碼；避免廣泛分享密碼。
- 使用 [驗證方法，例如 MAC 位址過濾、使用者驗證入口網站] 來進行 Wi-Fi 存取控制。
- 為訪客提供獨立的訪客 Wi-Fi 網路，且僅限於受限的互聯網存取。
- 至少每 [頻率，例如每月、每季] 顯示器一次未經授權或惡意存取點及裝置。
- 強制執行行動裝置的安全設定（例如：要求輸入密碼/PIN 碼，除非必要，否則停用藍牙、NFC、定位服務等非必要功能）。
- 提醒使用者不要在公共 Wi-Fi 網路上下載敏感的學校數據。

6. 端點與裝置安全

學校應保護所有存取學校數據或系統的裝置，使其免受安全威脅及未經授權的存取。

6.1. 學校自有裝置

- 所有學校擁有的裝置（例如電腦、平板電腦、伺服器）都必須依照學校政策進行保護與管理。
- 裝置必須視情況使用最新的安全控制措施 [例如：防惡意軟件、防火牆、安全更新]。
- 僅授權使用者方可存取學校所有之裝置；禁止共享帳號或密碼。
- 裝置必須配置為在一段時間未操作後自動鎖定 [例如 10 – 15 分鐘]。
- 必須定期安裝安全更新 [頻率，例如：自動更新或至少每月一次]。
- 若裝置遺失、遭竊或安全受損，必須立即向 [職務，例如：IT 協調員/管理員] 通報。

6.2. 自攜設備 (BYOD)

- 用於學校用途的個人裝置（例如筆記型電腦、平板電腦、智慧型手機）必須符合學校的安全要求。
- 只有在實施了 [安全控制措施，例如：裝置密碼、最新的作業系統和安全軟體、註冊流動裝置管理] 的情況下，才允許透過個人裝置存取敏感的學校數據或系統。
- 學校保留限制或撤銷不符合規範之裝置存取權限的權利。
- 使用者須對其裝置的安全負責，並須立即向 [職位，例如 IT 協調員/管理員] 報告任何安全事件。
- 除非獲得特別授權，否則不得使用個人裝置儲存或處理機密學校數據。

6.3. 流動裝置管理

- 學校應實施合理措施，以管理及保障存取學校系統或數據的行動裝置。
- 在可能的情況下，學校可使用流動裝置管理 (MDM) 解決方案 [例如 Microsoft Intune、Apple School Manager] 來執行安全設定（例如螢幕鎖定、加密、遠端清除）。
- 若專用的 MDM 解決方案不可用，學校將制定替代程序，以確保對裝置套用必要的安全設定（例如：要求使用強密碼、啟用裝置加密，以及確保在裝置遺失或遭竊時能夠遠端清除資料）。
- 存取學校系統或數據的裝置必須符合學校的安全要求，若不符合要求，其存取權限可能會受到限制或撤銷。
- 安全控制措施與裝置合規性將至少每 [頻率，例如每年、每半年] 進行一次審查。

7. 數據保護

學校應依照法律及法規要求，保護所有個人、機密性及敏感數據，防止其遺失、遭未經授權存取或遭濫用。

7.1. 數據加密

- 儲存於學校系統及裝置上的資料（「靜態資料」）以及透過網路傳輸的資料（「傳輸中資料」），應在可行情況下使用適當的加密方法進行保護 [例如：全磁碟加密、加密檔案共享、電子郵件及網路流量的 SSL/TLS]。
- 若加密在技術上或財務上不可行，則必須實施替代性的風險降低措施 [例如：限制實體存取、將數據儲存於安全地點、提供員工關於安全處理的培訓]。
- 敏感數據不得儲存於無法支援加密的裝置或媒體上，除非 [例外程序，例如經 IT 協調員/校長批准，並已實施緩解措施]。
- 加密金鑰必須受到安全管理，且僅限授權人員存取。

7.2. 數據備份與復原

- 關鍵學校數據必須定期 [頻率，例如：每日、每週] 進行備份，並盡可能使用 [備份方法，例如：自動備份軟體、雲端備份服務]。
- 如果無法使用自動化或雲端備份解決方案，則必須建立並遵循手動備份程序，並確保備份媒體的安全（例如：上鎖儲存、存取控制）。
- 備份副本必須受到保護，防止未經授權的存取（例如：加密、存放在校外或雲端，並限制存取權限）。
- 必須定期進行備份還原測試 [頻率，例如：每年、每半年]，以確保在發生數據遺失或系統故障時，能夠恢復數據。
- 必須定期檢視並視需要更新備份與還原程序。

7.3. 數據外洩防護 (DLP)

- 學校應實施相關措施，以降低敏感數據因意外或未經授權而遺失、洩露或共用的風險。
- 在可能的情況下，應使用技術控制措施 [例如：DLP 軟體、電子郵件過濾、存取限制] 來偵測並防止未經授權的數據傳輸。
- 如果技術性的 DLP 解決方案的可用性不足，學校將依靠意識宣導、教職員／學生培訓，以及關於適當數據處理與共用的明確政策。
- 教職員與學生必須了解其數據保護責任，包括不得透過不安全的管道（例如：個人電子郵件、未加密的 USB 隨身碟）傳送敏感資訊。
- 任何實際或疑似數據遺失事件，必須立即向 [職位，例如：數據保護官、IT 協調員] 報告。

8. 供應商與第三方管理

學校應確保可能接觸學校數據、系統或設施的供應商、承包商及第三方服務提供者，均符合適當的安全標準。

8.1. 供應商安全要求

- 向學校提供貨品或服務的供應商及第三方，必須遵守學校的資訊保安與數據保護要求。
- 對供應商的安全要求應與所涉及的數據、系統或服務的敏感程度相稱 [例如：雲端儲存服務供應商與清潔承包商]。
- 在可行情況下，供應商必須證明已實施安全管控措施（例如：ISO 27001 認證、適當的存取控制、安全數據處理）。
- 若供應商因實際或預算限制而無法符合正式安全標準，學校必須評估風險並實施補償性控制措施 [例如：限制數據共用、限制存取權限、加強監控]。
- 供應商安全管理的責任由 [職位，例如：數據保護官、資訊科技協調員、學校行政經理] 承擔。

8.2. 盡職調查與合約要求

- 在與新供應商簽約或續約前，學校必須評估供應商保護學校數據與系統的能力 [例如：透過安全問卷、背景查核、公開認證]。
- 與處理敏感數據或資訊系統的供應商簽訂的合約，應在可行情況下包含具體的數據保護及資訊保安條款 [例如：機密性、資料外洩通知、稽核權、資料歸還或刪除]。
- 若無法納入詳細的安全條款（例如針對次要供應商），學校必須記錄相關風險並建立替代性保障措施 [例如：盡量減少數據共用、採用短期協議，或實施技術限制]。
- 供應商必須立即向 [職位，例如：數據保護官、IT 協調員] 報告任何涉及學校數據的實際或疑似安全事件。

9. 雲端服務安全

學校應確保使用雲端服務儲存、處理或分享學校資料時，符合適當的安全與數據保護標準。

9.1. 核准雲端服務清單

- 僅限經 [職位，例如：資訊科技協調員、數據保護主任、校長] 核准之雲端服務，方可用於學校數據及運作。
- 學校將維護一份最新的核准雲端服務清單 [例如：Google Workspace for Education、Microsoft 365、核准的學習平台]。
- 教職員與學生不得使用未經核准的雲端服務來儲存或進行數據共用。
- 核准服務清單將至少每 [頻率，例如：每年、每半年] 進行一次審查與更新。

9.2. 雲端數據保護

- 所有儲存於雲端的敏感或機密性學校資料，必須透過適當的安全措施加以保護 [例如：靜態與傳輸中的加密、嚴格的存取控制、資料分類]。
- 在可用情況下，應啟用多重認證 (MFA) 來存取雲端服務。
- 若某項雲端服務無法提供足夠的數據保護功能，學校將評估風險，並採取以下措施之一：(a) 避免將敏感數據儲存於該服務中，或 (b) 採取替代性防護措施 [例如：限制可信賴使用者存取、將數據匿名化、使用密碼保護的檔案]。
- 管理雲端數據保安的責任由 [職位，例如：IT 協調員、數據保護官] 承擔。

9.3. 雲端存取與監控

- 雲端服務的存取權限必須限制在授權使用者及角色 [例如：教職員、學生、經核准的承包商] 範圍內，並定期進行審查 [頻率，例如：每年、每半年]。
- 在可行情況下，應監控雲端服務的使用狀況，以防範未經授權的活動 [例如：可疑登入、數據下載、在校園網域外分享]。
- 若技術監控的可用性低，學校將實施替代措施 [例如：使用者意識培訓、定期手動審查帳戶活動、建立明確的事件通報管道]。
- 任何涉及雲端服務的疑似或實際安全事件，必須立即向 [職位，例如：IT 協調員、數據保護官] 報告。

10. 生成式人工智能的使用

學校應確保生成式 AI 工具（例如：聊天機械人、文字／圖像生成器、自動批改系統）的使用，在支援教學與學習的同時，亦能保障隱私、數據保安及符合倫理規範。

10.1. 經核准的人工智能工具

- 僅限經 [職位，例如：IT 協調員、數據保護官、校長、AI 委員會] 核准的生成式 AI 工具，方可用於與學校相關的活動。
- 學校將維護一份獲准使用的人工智能工具清單 [例如：Microsoft Copilot、Google Gemini、OpenAI ChatGPT、經核准的教育平台]。
- 教職員與學生不得使用未經核准的人工智能工具來處理、儲存或生成學校數據。
- 核准的人工智能工具清單將至少[頻率，例如：每年、每半年] 進行一次審查與更新。
- 審批決定應按風險分級將每項人工智能工具分類——不可接受風險／高風險／有限風險／低風險——並按分級調整管治要求（例如：支援評分或收生決定等高風險工具，須經資訊科技督導小組批准並在全校推行前強制人手覆核；一般寫作輔助等低風險工具則可循上述標準審批流程處理）。
- 就每項經核准的人工智能工具，訂明可使用之裝置及可使用之使用者群組。

10.1a. 禁止內容

- 絕對不能使用人工智能工具危害國家安全；如課題涉及國家安全、主權／領土爭議、不正確價值觀等敏感內容，應予刪除，並尋求學校管理層的意見。
- 嚴禁使用人工智能工具生成違反社會道德規範的內容（例如色情、暴力、違法行為，或蓄意捏造／傳播虛假資訊）。

10.2. AI 使用中的數據保護

- 除非該工具已正式獲准用於此類用途，且供應商能證明具備充分的數據保護措施 [例如：隱私權政策、合約條款、可信的聲譽]，否則不得將敏感或個人的學校資料輸入生成式 AI 工具。
- 教職員與學生在使用 AI 工具時，有責任進行數據保護。
- 任何持有學校數據的人工智能工具帳戶，須設有強度足夠且獨一無二的登入憑證及多重要素認證；如工具設有相關選項，預設應關閉對話記錄保存或「用作模型訓練的數據共享」功能。
- 教職員如須將學生作業上載至人工智能平台以進行批改或生成評語，須先移除任何可識別個人身分的資料，以確保完全符合《個人資料（私隱）條例》。人工智能生成的評分或評語，絕不可以直接採用——教師須先運用專業判斷審核，方可交予學生。

10.3. 監控與管控

- 必須顯示生成式 AI 工具的使用情況，以確保符合學校政策，並防止不當或未經授權的使用。
- 在可行情況下，應實施技術管控措施 [例如：使用記錄、存取限制、內容過濾] 以監控及管控 AI 的使用。
- 若技術監控的可用性低，學校將採取替代措施 [例如：使用者意識培訓、定期人工檢查、明確的濫用通報程序]。
- 任何實際或疑似濫用 AI 工具，或涉及 AI 的數據外洩事件，均須立即向 [職位，例如：IT 協調員、數據保護官] 通報。
- 將通報範圍擴展至涵蓋任何未經授權輸入人工智能工具的數據，以及任何違法或明顯不當的人工智能生成內容；教職員應扮演人手覆核者角色，確保人工智能生成內容符合學校價值觀，方可使用或分享。
- 明確將利用深度偽造（deepfake）技術進行的網絡欺凌，以及「起底」（未經同意披露／分享他人個人資料）列為須通報的具體濫用情況。嚴重個案應上報校方管理層，並按學校現有機制處理，必要時諮詢輔導人員及家長。

10.4. 公平性考慮

- 若功課要求學生在家中使用人工智能工具（尤其是需要付費的進階功能），或屬於佔分比重高的家課，應考慮此舉是否會令欠缺同等資源或家庭支援的學生處於不利位置，並相應調整功課設計。

11. 使用者意識與培訓

學校應確保所有教職員、學生及相關利害關係人皆知悉其在資訊保安方面的責任，並了解如何安全且適當使用學校系統與數據。

11.1. 資安意識計畫

- 學校將針對所有使用者 [例如：教職員、學生、承包商]，以符合可用資源的適當形式 [例如：線上培訓、工作坊、印刷指南、簡報]，定期提供資訊保安意識教育。
- 意識提升計畫將涵蓋關鍵主題，例如數據保護、密碼安全、網路釣魚、安全使用互聯網，以及事件通報。
- 若無法進行正式或自動化培訓，學校將採用替代方法 [例如：海報、教職員會議、通訊、課堂討論]。
- 資訊安全意識相關材料及課程將至少每 [頻率，例如：每年、每半年] 進行一次檢討與更新。
- 安全意識協調的責任由 [職位，例如：IT 協調員、數據保護官、校長] 負責。

11.2. 可接受使用政策

- 所有使用者必須遵守學校的《可接受使用政策》（AUP），該政策規定了使用學校設備、網路及數據時應遵守的行為規範與禁止事項。
- 《可接受使用政策》將傳達給所有使用者 [例如：在入學時、新員工入職培訓時、定期提醒]，並可能要求使用者確認已理解並同意 [例如：透過簽署表格、線上確認]。
- 若無法取得正式確認（例如：針對年幼學生），學校將確保透過其他方式傳達相關要求 [例如：課堂討論、教師提醒]。
- 違反《可接受使用政策》之行為，將依照學校紀律程序處理。

11.3. 外部培訓管道

學校應考慮利用外部管道與資源，以提升教職員、學生及利害關係人的資訊保安意識。

- **政府及公共部門的倡議**：
    - **數碼政策辦公室（DPO）：**在「智慧城市藍圖」及網絡安全運動下提供資源與計劃（例如：研討會、工作坊、宣導活動）。
    - **香港教育局（EDB）**：提供有關電子學習安全、數據私隱及網絡倫理的指引與培訓材料。學校可申請支援或專業發展課程。
- **非政府組織（NGO）及協會：**
    - **香港電腦緊急事故應變小組協調中心（HKCERT）：**提供免費資源、警報、培訓課程及度身訂造的工作坊。
    - **香港互聯網註冊管理有限公司（HKIRC）：**提供免費資源，例如員工培訓平台（Cybersec Training Hub）、網站安全檢查（Healthy Web）、釣魚電郵演習活動等

12. 事故管理

學校應確保所有資訊保安事件，包括資料外洩、網絡攻擊，以及裝置遺失或遭竊，均能及時且有效地處理，以將影響降至最低並協助恢復運作。

12.1. 事件通報

- 所有使用者必須立即向 [職位，例如：資訊科技統籌員、數據保護主任、校長] 報告實際或懷疑的資訊保安事件，並使用 [報告方法，例如：電郵、電話、事件報告表]。
- 學校將向教職員和學生提供明確的指引，說明如何識別和通報事件 [例如：海報、教職員會議、線上資源]。
- 若正式的通報系統不可用，使用者可直接向其教師或主管通報事件，由其向上級通報。

12.2. 事件應變與復原

- 學校將及時應對安全事件，並採取措施控制、調查及補救情況。
- 在可能的情況下，學校將使用已文件編製的程序或檢查清單來指導應對與恢復工作 [例如：隔離受影響的裝置、重設密碼、還原備份]。
- 若正式程序或技術工具不可用，學校將盡合理努力控制事件、保護受影響的數據，並盡快恢復正常運作。
- 與受影響人士、家長或當局的溝通，將由 [職位，例如校長、資訊科技統籌員] 視情況進行協調。
    - **香港電腦緊急事故應變小組協調中心 (HKCERT)：**
        - 用於通報多點網絡攻擊或尋求建議。
        - 電話：8105 6060 | hkcert@hkcert.org | 事件報告表
    - **香港警務處：**
        - 用於舉報懷疑的犯罪活動，或當學校是唯一受影響方時。
        - 電話：2860 5012 | 網上舉報中心
    - **個人資料私隱專員公署 (PCPD)：**
    - 若個人數據（學生、教職員、家長）遭洩露，特別是可能導致傷害或困擾的情況。請使用私隱專員公署的數據外洩通報表格或網上表格。
- 若學校現有人員缺乏有效管理、調查或從安全事件中恢復所需的知識、經驗或資源，學校應尋求合資格的外部專家協助。

12.3. 事後檢討

- 發生重大安全事件後，學校將進行事後檢討，以查明原因、評估應對措施的成效，並提出改善建議。
- 在可行情況下，將把調查結果及汲取的教訓進行文件編製，並與相關人員分享，以降低事件重演的風險。

- 至少，將在教職員會議中討論該事件，並實施基本的糾正措施。
- 學校將根據檢討結果，視需要更新政策與程序。

13. 監控與記錄

學校應監控其系統和網絡，以偵測、調查和應對安全威脅或政策違規行為，並保留相關記錄以支持安全與問責。

13.1. 系統與網路監控

- 學校將在可行情況下，使用 [監控方法，例如內建警示、安全軟體、防火牆日誌]，監控關鍵系統和活動網絡，以偵測未經授權存取、濫用或安全事件的跡象。
- 監控工作應著重於關鍵資產和敏感資料 [例如：行政伺服器、學生資訊系統、雲端平台]。
- 若自動化監控工具的可用性低，學校將採用替代方法 [例如：定期人工檢查、檢視系統使用報告、抽查使用者活動]。
- 監控責任由 [職位，例如：IT 協調員、系統管理員] 負責。

13.2. 記錄管理與審查

- 學校將記錄關鍵系統及網路活動 [例如：登入、檔案存取、敏感資料變更]，並在可行情況下使用 [記錄工具，例如：伺服器日誌、防火牆日誌、雲端審計追蹤]。
- 日誌必須受到保護，防止未經授權的存取、修改或刪除。
- 日誌應至少保留 [保留期限，例如 3 個月、1 年]，以配合可能的調查、稽核或法規要求。
- 保留期結束後，除非正在進行的調查有此需求，否則應將記錄安全刪除。
- 日誌將定期 [頻率，例如每月、每季] 進行檢視，以偵測可疑活動或政策違規。
- 若自動化記錄管理工具不可用，學校將進行手動記錄審查，並保留與安全相關事件的基本記錄。
- 在日誌審查過程中發現的重要結果或事件，必須立即向 [職位，例如：IT 協調員、數據保護官] 報告。

14. 實體與環境安全

學校應保護其設施、設備及資訊免受實體威脅、未經授權的存取、遺失或損壞。

14.1. 實體存取控制

- 對包含敏感資訊或關鍵系統的區域（例如：伺服器機房、員工工作區、檔案儲存室）的進出，必須僅限於經授權的人員。
- 校內區域應明確標示為公眾區域、教職員專用區域或限制區域（例如：伺服器機房），並據此實施存取控制。
- 應盡可能採用實體存取控制措施 [例如：鎖具、門禁卡、進出登記簿]，以防止未經授權的進入。
- 若先進的控制措施的可用性低，學校將採取替代措施 [例如：人工監督、上鎖的櫃子、人員在場監督]。
- 訪客進入敏感區域時，必須透過 [方法，例如訪客登記簿、簽到表] 進行監督與記錄。
- 實體進出管理之責任由 [職務，例如：辦公室經理、IT 協調員、校長] 負責。

14.2. 設備安全

- 含有敏感資訊的學校設備（例如：電腦、伺服器、備份裝置）必須受到保護，以防盜竊、遺失或損壞。
- 設備應放置於安全地點 [例如：上鎖的房間、遠離公共區域]，並在可行情況下採取實體防護措施 [例如：纜繩鎖、上鎖的櫃子]。
- 若先進的安全措施的可用性有限，學校將採用實用的替代方案 [例如：定期檢查設備、下班後將攜帶式裝置存放在上鎖的抽屜中]。
- 若設備遺失、遭竊或損壞，必須立即向 [職位，例如：辦公室經理、IT 協調員] 報告。
- 在處置或轉移設備之前，必須進行檢查，以確保所有敏感數據均已安全刪除或移除。

15. 維護與修補程式管理

學校應確保所有系統和軟體均定期維護和更新，以降低安全漏洞和軟體缺陷帶來的風險。

15.1. 軟體更新

- 所有學校擁有的系統和軟體必須保持最新狀態，並安裝最新的安全更新和修補程式（可用）。
- 在可能的情況下，應啟用作業系統、應用程式及安全工具（例如防毒軟體、瀏覽器）的自動更新功能。
- 若自動更新的可用性低，學校將建立手動流程 [例如：排程檢查、更新記錄]，以確保及時安裝更新。
- 針對關鍵安全漏洞的更新，應在發布後盡快套用。
- 除非已進行風險評估並實施補償性控制措施，否則不得將供應商不再提供支援（生命週期結束）的系統和軟體用於學校活動。
- 確保第三方雲端服務和 SaaS 平台（例如學習管理系統、協作工具）納入更新和漏洞管理流程，方法是驗證供應商的更新做法，或透過合約確保及時套用更新。
- 管理軟體更新的責任由 [職位，例如 IT 協調員、系統管理員] 承擔。

15.2. 漏洞管理

- 學校將定期使用 [方法，例如：漏洞掃描工具、手動檢查、供應商通知]，檢視系統和軟體是否存在已知的安全漏洞。
- 如有可用性，應使用漏洞管理工具來識別風險並進行優先排序。
- 若自動化工具的可用性低，學校將監控可信來源 [例如：供應商網站、政府公告] 以獲取相關安全警報，並視需要採取行動。
- 已識別的漏洞應及時進行評估和處理，並優先處理那些對學校運作或數據構成最大風險的漏洞。
- 重大風險或無法在內部解決的問題，必須向 [職位，例如：IT 協調員、校長] 報告並經其審查。
- 在套用重大更新之前，學校將評估潛在影響，並在可行情況下於受控環境中測試更新，以將中斷影響降至最低。

15.3. 變更管理

- 對學校 IT 系統、軟體或網路設定的重大變更（例如安裝新應用程式、重大更新、變更安全設定），在實施前應由 [職位，例如 IT 協調員、校長] 進行審查並批准。
- 所有重大變更均應進行文件編製，包括日期、變更性質及負責人。
- 在可能的情況下，應先對變更進行測試，以避免中斷服務。
- 員工應盡快報告因變更而產生的任何問題，以便迅速處理。

16. 政策例外與違規

學校理解，在某些情況下，可能無法完全遵守所有資訊保安政策。在此類情況下，應遵循正式的例外處理程序。所有員工及使用者均須遵守本政策；違反者可能面臨紀律處分。

16.1. 例外處理程序

- 針對本政策的例外申請必須以書面形式提交給 [職位，例如：校長、資訊科技協調員、數據保護官]，並說明例外原因及已實施的任何補償性控制措施。
- 所有豁免申請在獲准前，均須經由 [職位，例如：校長、資訊科技委員會、數據保護官] 審查並核准。
- 經核准的例外情況必須進行文件編製，內容應包含例外範圍、有效期限及相關條件。
- 將定期檢討各項例外規定 [頻率，例如：每年一次，或視需要而定]，以判定其是否仍有必要。

16.2. 紀律處分

- 違反本政策或未經授權的例外情況，可能會導致紀律處分，處分程度最高可達 [後果，例如：譴責、停學、開除]，並依照學校的教職員與學生紀律程序辦理。
- 學校在決定適當處置時，將考慮違規行為的意圖、嚴重程度及影響。
- 若涉及可能違反法律或法規的情況，將根據要求向 [外部主管機關，例如：教育局、警方、數據保護監管機構] 通報事件。

17. 文件管控

本校將確保所有資訊保安政策均經妥善文件編製、管控並保持最新狀態。此舉有助於維持一致性與問責制，並確保所有使用者皆參照正確版本。

17.1. 政策檢討與更新歷史

- 本政策應至少每 [頻率，例如：每年、每兩年] 進行檢討，並在必要時更新；或因應法規、技術或學校運作上的重大變動而進行檢討與更新。
- 檢討與更新由 [職位，例如：校長、資訊科技統籌員、數據保護主任] 負責。
- 本政策的所有版本均須記錄在案，內容應包含生效日期、變更摘要及負責更新之人員。
- 為便於參考及確保問責，應將先前版本保留 [保留期限，例如 3 年]。
- 本政策的現行及經核准版本將可用於全體教職員，並在適當情況下可用於學生及家長。

附錄

A. 其他參考資料

以下補充參考資料可用於支持本政策的有效實施：

建議事項與優先級對應表

上述範本中的建議已依據下列表格中的優先級進行對應。優先級的劃分方式如下：

- P1 – 立即執行：最高優先級，須作為安全基準層級予以實施與整合，被視為維護安全環境的關鍵要素。
- P2 – 後續：有助於維持安全的重要防護措施，實施難度不高但仍能填補漏洞
- P3 – 稍後：用於增強防護的額外措施，可提升系統成熟度與運作節奏，實施時對資源/時間的負擔屬中等
- P4 – 延後/規劃：基於規模或時機考量，可在長期實施的措施，由各校依據可用資源獨立處理

以下是政策範本與其相對優先級的對照表：

類別	範本項目	優先級	指引／範例
治理與合規	2.1 法律與法規遵循	P1	遵守《個人資料（私隱）條例》（第 486 章）及個人資料私隱專員公署（PCPD）的要求（個人資料的收集、使用、儲存及披露），以符合個人資料私隱專員公署（PCPD）的規定
管治與合規	2.1 法律及監管合規	P1	遵守教育局（EDB）的相關通告／指引（例如《學校資訊保安 — 建議做法》）。
管治與合規	2.1 法律及規例合規	P2	遵守其他適用法律及標準（例如：《版權條例》、《電腦罪行條例》、行業守則）。
管治與合規	2.1 法律及監管合規	P1	監察法律／指引的變動，並確保政策及做法持續符合規定。
管治與合規	2.2 政策管理與審查	P1	取得學校管理層／管治機構對網絡安全 政策／程序的正式批准。
治理與合規	2.2 政策管理與審查	P2	至少每年或於發生重大變更（技術、法律、營運）時檢討政策。

治理與合規	2.2 政策管理與審查	P2	對所有政策進行版本控制（批准日期、更新、審查）。
治理與合規	2.2 政策管理與審查	P1	向員工／學生／第三方傳達政策；視需要提供培訓／宣導。
治理與合規	2.2 政策管理與審查	P2	利用回饋、事件及稽核結果推動持續改善。
治理與合規	2.2 政策管理與檢討	P1	高階領導層須對資訊保安的政策管理、合規性及治理負責。
資產管理	3.1 資訊科技資產清查	P1	維持所有 IT 資產的最新清單；將整體責任指派給 IT 協調員／學校秘書。
資產管理	3.1 資訊科技資產清單	P2	確保清單包含硬件、軟體／授權及雲端服務。
資產管理	3.1 IT 資產清點	P2	在資產被取得、重新分配或報廢時更新清單。
資產管理	3.1 資訊科技資產清點	P2	至少每年或每半年檢視一次資產清單。
資產管理	3.1 資訊科技資產清單	P1	使用既定的追蹤方法／工具 [例如：試算表、資產管理系統]。
資產管理	3.1 資訊科技資產清點	P2	遵循資產歸還及安全處置程序（例如：處置前進行安全清除）。
資產管理	3.2 數據分類與處理	P1	數據至少應分類為「機密」、「內部」或「公開」。 • 機密性（例如：學生健康紀錄、紀律報告） • 內部（例如：教職員備忘錄、課程計畫草稿） • 公開（例如：學校通訊、活動傳單）
資產管理	3.2 數據分類與處理	P2	將機密／內部數據的存取權限限制於獲授權的人員／職務，例如教師、行政人員、IT 管理員等。
資產管理	3.2 數據分類與處理	P1	對敏感數據採取適當的保護措施（例如：數據加密工具、密碼保護）。
資產管理	3.2 數據分類與處理	P3	至少每半年或每年檢視一次數據分類與處理做法。

資產管理	3.2 數據分類與處理	P4	安全地刪除／銷毀不再需要的數據（例如：數位銷毀；銷毀列印清單）。
存取控制	4.1 用戶帳戶管理	P3	將用戶帳戶管理的責任指派給 IT 協調員或管理員。
存取控制	4.1 用戶帳戶管理	P2	確保每位使用者皆擁有唯一的用戶 ID；落實個人責任制。
存取控制	4.1 使用者帳戶管理	P3	透過正式流程，利用存取請求系統或 IT 票務系統來建立、修改或撤銷帳戶。
存取控制	4.1 用戶帳戶管理	P2	至少每年/每半年檢視一次有效帳戶；停用/移除閒置帳戶（例如，90 天未活動）。
存取控制	4.1 使用者帳戶管理	P1	當使用者離職或變更職務時，應立即撤銷其存取權限。
存取控制	4.2 特權存取	P4	特權帳戶僅用於管理任務；不得用於例行活動。
存取控制	4.2 特權存取	P2	避免在終端設備上使用本機管理員權限；如有必要，須取得 IT 資安主管或同等職位人員的批准，並進行文件編製及定期審查。
存取控制	4.2 特權存取	P2	要求特權存取須經 IT 資安負責人／IT 管理員申請並核准。
存取控制	4.2 特權存取	P2	為特權活動與非特權活動分別維護獨立的憑證。
存取控制	4.2 特權存取	P2	使用中央日誌平台（例如 SIEM 或日誌伺服器）記錄並定期檢視特權操作。
存取控制	4.3 密碼政策	P1	強制執行密碼最小長度 [例如：8 個以上字符] 及複雜度（包含字母、數字和符號）。
存取控制	4.3 密碼政策	P1	防止使用常見/弱密碼；禁止共享密碼。
存取控制	4.3 密碼政策	P1	要求定期變更密碼，至少每 [例如 90 天] 一次，或根據風險而定。
存取控制	4.3 密碼政策	P1	在 [例如 5] 次登入失敗後實施帳戶鎖定。

存取控制	4.3 密碼政策	P2	安全儲存密碼（進行雜湊運算和/或加密）。
存取控制	4.3 密碼政策	P1	在可行情況下，為敏感帳戶/系統啟用身分驗證方法，例如多因素驗證 (MFA)。
存取控制	4.4 遠端及第三方存取	P1	要求遠端存取必須使用安全通道（例如 VPN、加密連線）。
存取控制	4.4 遠端及第三方存取	P2	僅在獲得 IT 管理員明確批准，且範圍與期間已明確定義的情況下，才授予遠端／第三方存取權限。
存取控制	4.4 遠端及第三方存取	P2	記錄並審查所有第三方存取活動。
存取控制	4.4 遠端及第三方存取	P1	任務完成後，應立即撤銷臨時/緊急存取權限。
網路安全	5.1 網路分段	P2	使用分段方法（例如 VLAN、獨立的 Wi-Fi SSID）將內部網路（例如：管理員、學生、訪客）進行分段。
網路安全	5.1 網路分段	P1	使用私有 IP；防止內部系統直接連接到互聯網。
網路安全	5.1 網路分段	P1	僅允許授權裝置進入各區段；阻止未受管理/個人裝置進入員工/管理員網路。
網路安全	5.1 網路分段	P2	至少每年或每半年檢視一次分段與存取控制。
網路安全	5.2 防火牆與邊界安全	P1	在互聯網通訊閘以及關鍵區段之間部署並維護防火牆，並使用不同類型的防火牆，例如硬件防火牆、基於雲端的防火牆解決方案。
網路安全	5.2 防火牆與邊界安全	P1	預設拒絕所有流量；僅允許經批准的服務/埠，例如 HTTPS、電子郵件 (SMTP)。
網路安全	5.2 防火牆與邊界安全	P3	檢視/更新防火牆規則並監控日誌（透過防火牆日誌伺服器，如有 SIEM 則透過 SIEM）。
網路安全	5.2 防火牆與邊界安全	P2	在所有裝置上移除／停用未使用的網路服務／功能。

網路安全	5.3 無線安全	P1	使用強效的 Wi-Fi 加密（WPA3；若不可用則使用 WPA2）。
網路安全	5.3 無線安全	P1	設定並定期更新強效的 Wi-Fi 密碼；避免廣泛分享。
網路安全	5.3 無線安全	P2	使用驗證方法（例如 MAC 篩選、使用者驗證入口網站）來進行 Wi-Fi 存取控制。
網路安全	5.3 無線安全	P2	提供一個獨立的訪客 Wi-Fi 網路，僅限於受限的互聯網存取。
網路安全	5.3 無線安全	P3	至少每月/每季顯示未經授權/惡意 AP/裝置。
網路安全	5.3 無線安全	P3	實施行動裝置安全設定（密碼/PIN 碼、停用不必要的功能）。
網路安全	5.3 無線安全	P2	提醒使用者不要在公共 Wi-Fi 上存取敏感的學校數據。
端點與裝置安全	6.1 學校自有裝置	P3	依照政策保護／管理所有學校自有裝置。
端點與裝置安全	6.1 學校自有裝置	P2	使用最新的安全控制措施（例如：防惡意軟件、防火牆、安全更新）。
端點與裝置安全	6.1 學校自有裝置	P1	僅允許授權使用者；禁止共用帳號／密碼。
端點與裝置安全	6.1 學校自有裝置	P1	配置閒置後自動鎖定 [例如 10 – 15 分鐘]。
端點與裝置安全	6.1 學校自有裝置	P1	定期套用安全性更新 [例如：自動更新或至少每月一次]。
端點與裝置安全	6.1 學校自有裝置	P1	若裝置遺失、遭竊或遭入侵，請立即向 IT 協調員／管理員通報。
端點與裝置安全	6.2 自帶設備（BYOD）	P3	要求用於學校事務的個人裝置必須符合安全要求。
端點與裝置安全	6.2 自帶設備（BYOD）	P2	僅在實施安全控制措施（例如裝置密碼、最新作業系統與安全軟體、註冊流動裝置管理等）的情況下，才允許透過個人裝置存取敏感資料／系統。
端點與裝置安全	6.2 自帶設備 (BYOD)	P3	保留限制/撤銷不符合規範之裝置存取權限的權利。

端點與裝置安全	6.2 自帶設備 (BYOD)	P1	要求使用者確保其裝置安全，並立即向 IT 管理員通報事件。
端點與裝置安全	6.2 自帶設備（BYOD）	P1	除非獲得授權，否則禁止在個人裝置上儲存/處理機密數據。
端點與裝置安全	6.3 流動裝置管理	P4	實施合理措施，以管理／保障存取學校數據的行動裝置。
端點與裝置安全	6.3 流動裝置管理	P4	盡可能使用 MDM 解決方案 [例如 Intune、Apple School Manager] 來實施管控措施。
端點與裝置安全	6.3 流動裝置管理	P2	若無 MDM，請建立替代程序（強密碼、加密、遠端清除功能）。
端點與裝置安全性	6.3 流動裝置管理	P3	限制或撤銷不符合規範裝置的存取權限。
端點與裝置安全	6.3 流動裝置管理	P2	至少每年或每半年檢視一次裝置的安全控制措施與合規性。
數據保護	7.1 數據加密	P1	在可行情況下，使用適當的加密方式（例如：全磁碟加密、加密共用資料夾、SSL/TLS）保護靜止數據和傳輸中的數據。
數據保護	7.1 數據加密	P3	若無法進行加密，則應實施其他降低風險的措施。
數據保護	7.1 數據加密	P3	除非已獲批准並採取緩解措施，否則請勿將敏感數據儲存於無法加密的裝置上。
數據保護	7.1 數據加密	P2	安全管理加密金鑰；僅限授權人員存取。
數據保護	7.2 數據備份與復原	P1	定期（至少每日/每週）備份關鍵數據，並盡可能使用備份方法（自動備份軟體、雲端備份服務）。
數據保護	7.2 數據備份與還原	P3	若無自動化/雲端備份，請使用手動程序；並妥善保管備份媒體。
數據保護	7.2 數據備份與復原	P2	保護備份副本（例如：加密、異地/雲端儲存服務、限制存取）。
數據保護	7.2 數據備份與復原	P2	每年/每半年進行定期備份還原測試。

數據保護	7.2 數據備份與復原	P1	視需要檢視並更新備份／還原程序。
數據保護	7.3 數據外洩防護 (DLP)	P2	實施措施以降低意外／未經授權的數據遺失／洩露風險。
數據保護	7.3 數據外洩防範 (DLP)	P2	在可能的情況下，使用技術性的 DLP 控制措施（例如 DLP 軟體、電子郵件過濾、存取限制）。
數據保護	7.3 數據外洩防護 (DLP)	P3	若無技術性 DLP，則應依賴意識提升／培訓以及明確的處理／共享政策。
數據保護	7.3 數據外洩防護 (DLP)	P1	禁止透過不安全的管道（例如 個人電子郵件、未加密的 USB 隨身碟）傳送敏感資訊。
數據保護	7.3 數據外洩防護 (DLP)	P1	如有實際或疑似數據遺失，請立即向 IT 管理員報告。
供應商與第三方管理	8.1 供應商安全要求	P3	確保供應商遵守學校的資訊保安與數據保護要求。
供應商與第三方管理	8.1 供應商安全要求	P1	根據數據／系統／服務的敏感程度，量身訂製供應商安全要求。
供應商與第三方管理	8.1 供應商安全要求	P2	在可行情況下，要求供應商證明其具備安全控制措施（例如 ISO 27001、存取控制、安全處理）。
供應商與第三方管理	8.1 供應商安全要求	P2	若供應商無法符合標準，應評估風險並實施補償性控制措施。
供應商與第三方管理	8.1 供應商安全要求	P1	將管理供應商資安的責任指派給特定職位，例如數據保護官、資訊科技協調員或學校行政經理。
供應商與第三方管理	8.2 盡職調查與合約	P1	在簽訂合約或續約前，評估供應商的安全能力（例如：問卷調查、參考資料、認證）。
供應商與第三方管理	8.2 盡職調查與合約	P2	在可能的情況下，於合約中納入數據保護／安全條款（機密性、違約通知、稽核、資料歸還／刪除）。

供應商與第三方管理	8.2 盡職調查與合約	P2	若無法制定詳細條款，應記錄相關風險並建立替代性保障措施。
供應商與第三方管理	8.2 盡職調查與合約	P1	要求供應商立即向指定人員（例如數據保護官、IT 協調員）報告實際或疑似的安全事件。
雲端服務安全	9.1 核准雲端服務清單	P2	僅使用經 IT 協調員及支援人員核准的雲端服務。
雲端服務安全	9.1 核准雲端服務清單	P2	維持一份最新的核准雲端服務清單。[Google Workspace for Education、Microsoft 365、核准的學習平台]
雲端服務安全	9.1 核准雲端服務清單	P1	禁止在未經核准的雲端服務上儲存或進行數據共用。
雲端服務安全	9.1 核准雲端服務清單	P2	至少每年或每半年檢視/更新核准服務清單。
雲端服務安全	9.2 雲端數據保護	P1	保護敏感／機密的雲端資料（靜態與傳輸中的加密、嚴格的存取控制、資料分級）。
雲端服務安全	9.2 雲端數據保護	P1	在可用性高的情況下，為雲端服務存取啟用多因素驗證。
雲端服務安全	9.2 雲端數據保護	P3	如果某項服務缺乏足夠的保護，請避免儲存敏感數據，或採取其他防護措施（限制存取、匿名化、密碼保護檔案）。
雲端服務安全性	9.2 雲端數據保護	P3	將雲端數據保安的責任指派給 IT 協調員或同等職位。
雲端服務安全	9.3 雲端存取與監控	P1	將雲端存取權限限制於授權使用者／角色，並定期（每年／每半年）進行審查。
雲端服務安全	9.3 雲端存取與監控	P2	在可行情況下，監控雲端使用狀況以偵測未經授權的活動（例如：可疑登入、數據下載、外部分享）。
雲端服務安全	9.3 雲端存取與監控	P4	若無法進行技術監控，應實施替代措施（提高意識、人工審查、明確的報告）。
雲端服務安全	9.3 雲端存取與監控	P1	立即向 IT 協調員報告疑似／實際的雲端安全事件。

生成式人工智能的使用	10.1 經核准的人工智能工具	P1	僅可使用經 IT 協調員核准的生成式 AI 工具。
生成式人工智能的使用	10.1 經核准的人工智能工具	P1	應維護一份獲准使用的人工智能工具清單，例如 Microsoft Copilot、Google Gemini、OpenAI ChatGPT 及其他獲准的平台。
生成式 AI 的使用	10.1 核准的人工智能工具	P1	請勿使用未經核准的人工智能工具來進行數據處理、儲存或生成學校數據。
生成式人工智能的使用	10.1 經核准的人工智能工具	P2	至少每年或每半年檢視／更新核准的人工智能工具清單。
生成式 AI 的使用	10.2 人工智能應用中的數據保護	P1	除非該工具已獲批准且供應商具備充分的數據保護措施，否則請勿將敏感/個人數據輸入 AI 工具。
生成式人工智能的使用	10.2 人工智能應用中的數據保護	P2	確保使用者在使用 AI 工具時能進行數據保護。
生成式人工智能的使用	10.3 監控與控制	P3	顯示生成式 AI 工具的使用情況，以確保符合政策規定，並防止不當或未經授權的使用。
生成式人工智能的使用	10.3 監控與管控	P3	在可行情況下實施技術控制（使用記錄、存取限制、內容過濾），以監控／控制 AI 的使用。
生成式 AI 的使用	10.3 監控與管控	P3	若無法進行技術監控，請採用替代措施（提升意識、人工檢查、明確報告）。
生成式 AI 的使用	10.3 監控與控制	P1	若懷疑有人濫用 AI 工具或發生與 AI 相關的數據外洩，請立即向 IT 協調員報告。
使用者意識與培訓	11.1 資安意識培訓計畫	P1	以資源許可的適當形式，定期為所有使用者提供資訊保安意識培訓。
使用者意識與培訓	11.1 資安意識計畫	P1	涵蓋關鍵主題（數據保護、密碼、網路釣魚、安全使用互聯網、事件通報）。
使用者意識與培訓	11.1 資安意識計畫	P2	若無法實施正式/自動化培訓，請採用替代方法（海報、會議、電子報）。
使用者意識與培訓	11.1 安全意識計畫	P2	至少每年或每半年檢視／更新意識宣導資料／課程。

使用者意識與培訓	11.1 資安意識計畫	P1	將協調安全意識的責任指派給 IT 協調員。
使用者意識與培訓	11.2 合理使用政策	P1	要求所有使用者遵守《可接受使用政策》（AUP）。
使用者意識與培訓	11.2 合理使用政策	P1	在註冊/入職時傳達《可接受使用政策》，並透過定期提醒進行宣導；在可行情況下取得確認。
使用者意識與培訓	11.2 合理使用政策	P2	針對年幼學生，採用替代性溝通方式（例如：課堂討論、教師提醒）。
使用者意識與培訓	11.2 合理使用政策	P1	透過學校紀律程序處理違反《可接受使用政策》的情況。
使用者意識與培訓	11.3 外部培訓管道	P3	在可行情況下善用外部資源：數位政策辦公室（DPO）的相關措施。
使用者意識與培訓	11.3 外部培訓管道	P3	在可行情況下善用外部資源：香港教育局（EDB）的指引／培訓。
用戶意識與培訓	11.3 外部培訓渠道	P3	在可行情況下善用外部資源：HKCERT 的警報／資源／工作坊。
用戶意識與培訓	11.3 外部培訓渠道	P3	在可行情況下善用外部資源：HKIRC 資源（網絡安全培訓集線器、健康網絡、釣魚電郵演習）。
事故管理	12.1 事件通報	P1	要求透過各種通報方式（包括電郵、電話、事件通報表格）向 IT 協調員即時通報實際發生或懷疑發生的事件。
事故管理	12.1 事件通報	P1	透過海報、員工會議及線上資源，就如何識別及通報事件提供明確指引。
事故管理	12.1 事件通報	P1	若無正式系統，應允許向教師／主管報告以便向上級通報。
事故管理	12.2 事件應變與復原	P1	應迅速回應事件，以進行控制、調查及修復。
事故管理	12.2 事件應變與復原	P2	在可行情況下，使用已文件編製的程序/檢查清單進行應變/復原（例如：隔離裝置、重設密碼、還原備份）。

事故管理	12.2 事件應變與復原	P1	若無正式程序／工具，應採取合理步驟以迅速控制／保護／恢復。
事故管理	12.2 事件應變與復原	P1	透過 IT 協調員，與受影響方／家長／當局協調溝通事宜。
事故管理	12.2 事件應變與復原	P1	維護流程／聯絡資訊，以便在適當情況下向 HKCERT 報告。
事故管理	12.2 事件應變與復原	P1	維護流程／聯絡資訊，以便向香港警方報告可疑罪行／僅受影響的個案。
事故管理	12.2 事件應變與復原	P1	維護流程／聯絡資訊，以便在可能造成傷害／困擾的個人數據外洩事件發生時通知私隱專員公署。
事故管理	12.2 事件應變與復原	P2	若內部資源不足以處理事件或進行復原，應尋求合格的外部專家協助。
事故管理	12.3 事件後檢討	P3	在重大事件發生後進行事件後檢討，以釐清原因並提出改善措施。
事故管理	12.3 事件後檢討	P3	盡可能將調查結果／經驗教訓記錄下來，並與相關人員分享。
事故管理	12.3 事件後檢討	P3	至少在員工會議中討論事件，並實施基本的矯正措施。
事故管理	12.3 事件後檢討	P3	根據檢討結果更新政策／程序。
監控與記錄	13.1 系統與網路監控	P2	在可行情況下，利用各種監控方法、內建警示、安全軟體及防火牆日誌，監控關鍵系統／網路活動，以偵測未經授權的存取、濫用行為及事件。
監控與記錄	13.1 系統與網路監控	P2	監控重點應放在關鍵資產和敏感數據上（例如：管理伺服器、學生資訊系統、雲端平台）。
監控與記錄	13.1 系統與網路監控	P3	若無自動化工具，請定期手動檢查／審閱使用報告及使用者活動。

監控與記錄	13.1 系統與網路監控	P1	將監控責任指派給 IT 協調員或系統管理員。
監控與記錄	13.2 記錄管理與檢視	P1	盡可能使用記錄工具（例如伺服器日誌、防火牆日誌和雲端審計追蹤）來維護關鍵活動（登入、檔案存取、敏感數據變更）的日誌。
監控與記錄	13.2 記錄管理與檢視	P1	保護日誌免遭未經授權的存取、修改或刪除。
監控與記錄	13.2 記錄管理與檢視	P2	將日誌保留一段既定的保存期限（例如每季/每年），以支援調查、稽核及法規遵循需求。
監控與記錄	13.2 記錄管理與檢視	P3	在保留期結束後安全刪除日誌，除非正在進行的調查需要保留。
監控與記錄	13.2 記錄管理與檢視	P1	每月/每季定期檢視日誌，以偵測可疑活動/政策違規。
監控與記錄	13.2 記錄管理與檢視	P2	若無自動化日誌工具，請進行手動檢視並記錄與安全相關的事件。
監控與記錄	13.2 記錄管理與檢視	P1	請立即向 IT 協調員報告來自日誌 審查的重要發現／事件。
實體與環境安全	14.1 實體存取控制	P1	將敏感區域（伺服器機房、員工工作區、檔案儲存區）的進出權限限制於獲授權人員。
實體與環境安全	14.1 實體存取控制	P1	應明確標示區域為公眾、員工專用或限制進入；並據此進行存取控制。
實體與環境安全	14.1 實體存取控制	P2	盡可能使用實體存取控制措施（鎖具、門禁卡、進出登記簿）。
實體與環境安全	14.1 實體存取控制	P2	若進階管控措施的可用性低，請使用替代方案（人工監督、上鎖的櫃子、人員駐守）。
實體與環境安全	14.1 實體存取控制	P2	監督並記錄訪客進入敏感區域的情況（例如：訪客登記簿）。
實體與環境安全	14.1 實體存取控制	P1	將實體進出管控的責任指派給 IT 協調員／管理員。

實體與環境安全	14.2 設備安全	P1	保護含有敏感資訊的設備，防止遭竊、遺失或損壞。
實體與環境安全	14.2 設備安全	P2	將設備安置於安全地點（上鎖的房間、遠離公共區域），並在可行情況下採取實體防護措施（如纜繩鎖、上鎖的櫃子）。
實體與環境安全	14.2 設備安全	P3	若無法採取進階措施，請採用實用的替代方案（定期檢查、非辦公時間上鎖存放）。
實體與環境安全	14.2 設備安全	P1	如遇設備遺失、遭竊或損壞，應立即向 IT 管理員通報。
實體與環境安全	14.2 設備安全	P3	在處置或移交設備前，請確保已安全刪除數據。
維護與修補程式管理	15.1 軟體更新	P1	確保所有系統／軟體皆安裝最新的安全性更新／修補程式。
維護與修補程式管理	15.1 軟體更新	P1	在可能的情況下，啟用作業系統、應用程式及安全工具的自動更新功能。
維護與修補程式管理	15.1 軟體更新	P2	若無自動更新功能，請實施手動流程（排程檢查、更新日誌）。
維護與修補程式管理	15.1 軟體更新	P1	在關鍵安全性更新發布後，應盡快進行安裝。
維護與修補程式管理	15.1 軟體更新	P2	除非已進行風險評估並實施補償性控制措施，否則應避免使用已達生命週期終止的系統／軟體。
維護與修補程式管理	15.1 軟體更新	P2	將第三方雲端／SaaS 平台納入更新／漏洞管理（透過驗證供應商做法或合約確認）。
維護與修補程式管理	15.1 軟體更新	P1	將軟體更新的責任指派給 IT 管理員。
維護與修補程式管理	15.2 漏洞管理	P2	定期檢查系統／軟體是否存在已知漏洞（掃描工具、手動檢查、供應商通知）。
維護與修補程式管理	15.2 漏洞管理	P3	在可行的情況下，使用漏洞管理工具來識別風險並進行優先級排序。

維護與修補程式管理	15.2 漏洞管理	P2	若無自動化工具，請監控可信來源（供應商網站、政府公告），並視需要採取行動。
維護與修補程式管理	15.2 漏洞管理	P2	及時評估/處理已識別的漏洞，並優先處理風險最高的漏洞。
維護與修補程式管理	15.2 漏洞管理	P1	向 IT 協調員報告重大風險／未解決的問題。
維護與修補程式管理	15.2 漏洞管理	P3	評估潛在影響，並在可行情況下於部署前測試主要更新。
維護與修補程式管理	15.3 變更管理	P3	在實施前，由 IT 協調員審查/批准重大的 IT 變更。
維護與修補程式管理	15.3 變更管理	P3	記錄重大變更（日期、性質、負責人）。
維護與修補程式管理	15.3 變更管理	P3	在可能的情況下測試變更，以將中斷降至最低。
維護與修補程式管理	15.3 變更管理	P1	要求員工及時報告因變更而產生的問題。
政策例外與違規	16.1 例外處理流程	P1	須以書面形式向 IT 協調員提交例外申請，並附上理由及補償性控制措施。
政策例外與違規	16.1 例外處理流程	P1	由負責啟動例外批准的人員在批准前審查並核准例外。
政策例外與違規	16.1 例外處理流程	P2	文件編製已批准的例外情況（範圍、期限、條件）。
政策例外與違規	16.1 例外處理流程	P2	應定期（例如每年）或視需要審查例外情況，以確認其持續必要性。
政策例外與違規	16.2 紀律處分	P1	針對政策違規或未經授權的例外情況，應依照學校程序採取紀律處分。
政策例外與違規	16.2 紀律處分	P2	在決定採取何種行動時，應考量意圖、嚴重程度及影響。
政策例外與違規	16.2 紀律處分	P3	根據要求，向相關主管機關報告潛在的法律/法規違規行為。
文件控制	17.1 政策檢討與更新歷史	不適用	至少每年/每半年或於發生重大變更時，檢討/更新本政策。
文件控制	17.1 政策檢討與更新歷史	不適用	將審查／更新的責任指派給 IT 協調員。

文件控制	17.1 政策檢討與更新歷史	不適用	記錄所有政策版本（生效日期、變更摘要、負責人）。
文件控制	17.1 政策檢討與更新歷史	不適用	將先前政策版本保留一段既定的保存期限，例如 3 年。
文件控制	17.1 政策檢討與更新歷史	不適用	向員工提供當前已批准的政策，並視情況向學生／家長提供其可用性。

實務實施指南

實務指南的標題如下：

- 資產管理 – 實務指南
- 存取控制 – 實務指南
- 密碼管理 – 實務指南
- 維護與修補程式管理 – 實務指南
- 數據備份與復原 – 實務指南
- 資料處理與數據保護 – 實用指南
- 電子郵件安全 – 實用指南
- 流動裝置管理 – 實用指南
- 網路管理與無線安全 – 實用指南
- 實體與環境安全 – 實用指南
- 監控與記錄 – 實務指南
- 供應商與第三方關係 – 實務指南
- 生成式人工智能的應用 – 實務指南

網絡安全事件應變工作流程

涵蓋網路事件應變小組（CIRT）的設計、角色與職責、通報與升級流程、詳細的事件應變程序，並包含針對常見校園安全事件的情境式應變手冊，例如：

- 勒索軟體攻擊
- 網路釣魚與惡意軟件感染
- 裝置遺失或遭竊
- 意外數據外洩
- 網站篡改
- 拒絕服務 (DoS) 攻擊

安全配置檢查清單

本指南提供逐步檢查清單與實用指引，協助教職員依據政策要求，對學校裝置、系統及應用程式進行配置與安全防護。內容涵蓋伺服器、電腦、行動裝置、網路設備及常用軟體的關鍵安全設定。檢查清單包含建議的基礎配置、強化措施及定期檢視要點，以確保持續抵禦安全威脅。

這些文件針對學校的特定情境，提供逐步操作指引、檢查清單及情境應對手冊。建議使用者在日常運作中參考這些資料，以獲取實務指導。

B. 術語表

術語	定義
存取控制	用於限制僅授權使用者才能存取 IT 系統、數據或地點的流程與技術。
人工智能	能夠執行通常需要人類智慧的任務（例如學習或解決問題）的電腦系統或軟體。
資產	學校擁有或管理的任何裝置、軟體、數據或系統，包括硬件、軟體及雲端服務。
備份	為防止數據遺失或損毀而另行儲存的數據副本，以便進行復原。
自攜設備	使用個人擁有的裝置（例如筆記型電腦、智慧型手機）進行學校活動或存取學校系統。
雲端服務	由第三方主機託管並透過互聯網存取的線上服務（例如：儲存空間、應用程式、平台）。
機密數據	必須防止未經授權存取的資訊，例如學生紀錄或個人數據。
網絡安全事件	任何針對資訊或資訊系統所進行的未經授權存取、使用、揭露、干擾、修改或破壞之企圖或實際行為。
數據加密	將數據轉換為編碼形式以防止未經授權存取的過程。
數據外洩防護 (DLP)	旨在防止敏感資訊遭未經授權分享或遺失的工具或流程。
數據保護	為保護個人、敏感或機密資訊免遭未經授權的存取、揭露、竄改或破壞而採取的措施。
端點	任何連接到學校網路的裝置（例如：電腦、平板電腦、智慧型手機）。
防火牆	一種安全系統（硬件或軟體），根據預先設定的規則監控並控制進出網路的流量。
事件	任何可能危及學校資訊或資訊系統機密性、完整性或可用性的事件。
IT 協調員	負責監督學校資訊科技系統、安全及合規事宜的人員或職位。
日誌	用於監控與追蹤責任的事件記錄，例如系統存取或數據變更。
流動裝置管理 (MDM)	用於監控、管理及保障學校運作中所使用行動裝置的工具或流程。
多重認證 (MFA)	一種安全流程，要求使用者提供兩項或更多獨立的憑證以驗證其身分。
網路分段	將電腦網絡劃分為多個子網路，以提升安全性與效能。
修補程式管理	透過套用修補程式（patches）來解決漏洞或錯誤，以保持軟體最新的流程。
個人數據	任何與已識別或可識別之個人有關的資訊，例如姓名、身分證號碼或聯絡資料。
實體存取控制	用於限制進入建築物、房間或其他敏感區域的措施。
權限／特權存取	授予需執行管理或敏感任務之使用者的高階系統存取權限。
勒索軟體	一種惡意軟體，會鎖定或加密受害者的數據，並要求支付贖金以換取解鎖。

遠端存取	指從學校實體場地外部存取學校 IT 系統或數據的能力，通常透過 VPN 或安全連線實現。
敏感數據	一旦洩露可能對個人或學校造成損害的數據，例如健康紀錄或紀律處分報告。
供應商	向學校供應貨品或服務的任何第三方供應商或服務提供者，尤其是那些能夠存取數據或系統的供應商。
使用者	任何獲授權使用學校資訊科技資源的教職員、學生或其他人士。
漏洞	系統、軟體或流程中的弱點，可能被利用以危害安全性。
無線安全	為保護無線（Wi-Fi）網路免受未經授權的存取或攻擊而實施的存取控制措施與實務做法。

第二部份:

真實案例參考

資產管理實務指南

版本 1.0

本文件旨在作為實用指南，僅供參考。學校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及需求。作者對基於本指南所採取的任何行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 前言 5
2. 建立資產管理清單 6
2.1. 硬件資產清單 6
2.2. 軟體資產清單 6
2.3. 硬件資產狀態稽核紀錄 7
2.4. 報廢記錄 7
2.5. 借出／歸還記錄 7
3. 建立硬件資產管理程序 7
3.1. 更新硬件資產清單 7
3.2. 硬件資產清單審查 8
3.3. 資產分類 8
3.4. 硬件資產狀態稽核 10
3.5. 故障資產的更換 10
3.6. 硬件資產的處置 10
3.7. 借用與歸還程序 11
4. 建立軟體資產管理程序 13
4.1. 更新軟體資產管理清單 13
4.2. 軟體資產清單審查 13
附錄 14
硬件清單內容建議 14
術語表 17

1. 前言

1.1. 目的與範圍

本指南為全港學校的資產管理提供實用建議及基本標準，旨在協助教育機構建立一致的標準，以落實有效的資產管理程序，確保學校系統及敏感資料的安全與完整性。

本指南的範圍涵蓋硬件資產與軟體資產的資產清單編製及管理程序。此外，亦提供一份建議的硬件資產清單，供各校納入庫存管理，作為滿足學校需求的基準。本指南的設計旨在適應不同規模的學校、系統類型及可用資源。

1.2. 目標讀者（IT 管理員與技術人員）

本指南適用於資訊科技管理員、技術人員，以及任何負責管理學校環境中使用者帳戶或資訊科技系統的人員。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，IT 團隊將能更有效地：

- 識別並追蹤學校 IT 基礎架構順暢運作所需的各類資產
    - 涵蓋通常透過授權取得的硬件與軟體資產
- 依據資產的使用狀態維護紀錄，並提供更新時程與狀態稽核
- 及時對 IT 資產進行定期檢視
- 在資產損壞或故障時，遵循標準程序進行更換

鼓勵各校根據自身技術環境及運作需求，適配這些建議。

2. 建立資產管理清單

本節概述學校建立資產管理清單的流程，以協助其執行資產管理程序。請將這些建議作為基礎，並根據貴校的工作流程進行調整。

2.1. 硬件資產清單

- 目的：將每項硬件資產的狀態彙整於一份主清單中，以便快速查閱。
- 內容：所有學校擁有的電腦硬件及其相關資訊，例如硬件序號、用途及其位置。有關所有建議的資訊類型，請參閱附錄。

調整建議：

- 指派資訊科技部門彙編此清單。鑑於清單旨在便於日後查閱，建議使用數據庫或試算表以利篩選與查詢。
- 為確保硬件清單的準確性，應制定相關政策，禁止人員自行安裝或處置硬件資產。
- 並非所有欄位都必須針對每項資產填寫，僅需填寫相關資訊即可（例如：顯示器沒有 CPU，因此 CPU 型號欄位可填寫「N/A」）。

實務範例：

- 建立用於管理硬件資產的數據庫或試算表。附錄中已列出建議進行文件編製的資訊清單。
- 若需從頭建立清單，可考慮指派專人指導終端使用者（其他員工）回報其系統資訊（如 CPU 型號、記憶體容量及磁碟容量等），以減少後續工作量。

2.2. 軟體資產清單

- 目的：追蹤每項硬件資產的授權資訊及已安裝軟體。
- 內容：學校自有電腦軟體的詳細資訊，包括授權數量、到期日期、已安裝裝置（例如：資產編號）及版本號。

實作建議：

- 指派 IT 部門彙整此清單。由於此清單旨在便於日後查閱，建議使用數據庫或試算表以便篩選與查詢。
- 除軟體版本外，建議針對工作站、個人電腦及伺服器以外的設備（例如：網路設備）一併列出固件資訊。
- 為避免歧義並利於日後資料表關聯，建議參照「硬件清單」中的資產編號。
- 請考慮採用技術管控措施，禁止使用未經核准的應用程式。

2.3. 硬件資產狀態稽核紀錄

- 目的：記錄任何硬件資產狀態稽核案例，特別是失敗案例及其理由。此記錄可作為日後更換或處置硬件資產的依據。
- 內容：資產編號、稽核日期與時間、成功/失敗的理由。

2.4. 報廢記錄

- 目的：記錄任何待核准的硬件資產處置提案。
- 內容：資產編號、報廢理由、狀態（待核准／待報廢／已報廢）。

2.5. 借出／歸還記錄

- 目的：透過追蹤借用者，確保借用資產的責任歸屬。
- 內容：資產編號、借用者、借用日期與時間、歸還日期與時間。

3. 建立硬件資產管理程序

本節說明學校如何利用硬件管理清單，建立適當的硬件資產管理程序。適當的硬件資產管理程序旨在提供所有硬件資產的最新資訊，以便在需要時能夠取得這些資訊。

3.1. 更新硬件資產清單

在以下情況下應更新硬件資產清單：

- 購置／更換硬件設備
- 硬件報廢
- 硬件的再利用，包括測試硬件的部署。
- 硬件稽核
- 硬件故障

- 在檢視硬件資產清單時發現的任何差異。

3.2. 硬件資產清單審查

硬件資產清單審查由兩部分組成，應定期（例如每年）一併進行。

- **完整性**：檢查所有硬件資產是否已列入硬件資產清單。
- **正確性**：檢查硬件資產清單中的所有記錄是否有效，且無已處置資產的記錄。

實務建議：

- 「完整性」部分需在整個校園範圍內搜尋硬件設備，這可能需要投入較多心力。建議制定相關程序，讓所有員工都能主動通報此類資產，以減輕資訊科技部門的負擔。
- 「正確性」審查應相對簡單，因為庫存清單可用性高，且資產位置已進行文件編製。

實務範例：

- 使用貼紙標籤標示所有硬件（例如：資產編號、用途），以便日後快速查閱。若發現未貼有此類標籤的硬件，該硬件可能未被列入資產清單中。
- 請員工向 IT 部門通報任何未貼標籤的硬件。
- 使用掃描器或腳本生成各系統已安裝應用軟件的彙總報告。此報告可與軟體清單進行交叉比對。

3.3. 資產分類

根據敏感度（例如：數據儲存處、若系統癱瘓對運作的影響）對所有資產進行分類，以確定適當的保護等級供日後參考。將此分類納入「硬件資產清單」的記錄中。

《香港政府資訊科技保安指引》（G3）**附錄 C** 根據機密性、完整性及可用性（CIA）為資訊系統定義了三級分類：

- **第 1 級（低影響）**：公開或非敏感數據（例如學校網站內容）。若發生遺失或外洩，影響極輕微。

- **第 2 級（中等影響）**：敏感但非高度機密性之數據（例如：教職員電子郵件、學生出勤紀錄）。若遭洩漏，可能造成中度干擾或隱私疑慮。

- **第 3 級（高／關鍵影響）**：高度機密性或關鍵數據（例如：學生個人資料、考試成績、財務紀錄）。若數據外洩，可能導致重大的法律、聲譽或營運損害。

3.4. 硬件資產狀態稽核

硬件資產狀態審計是針對硬件資產狀態進行的簡易檢查，旨在確認其能否持續執行指定任務，應定期（例如每年）對《硬件資產清單》上的所有資產進行此項審計。

針對特定資產的狀態審計亦可視情況臨時進行，例如當有使用者回報系統故障時。

若資產運作正常：

- 請更新「硬件資產清單」中該資產的最後審核日期。

否則：

- 更新「硬件資產清單」中該資產的最後審核日期。
- 將該資產標記為「狀態審計失敗」
- 對該資產執行更換與處置程序。
- 在「資產狀態審計記錄」中進行審計失敗的理由文件編製。

適用建議：

- 不同資產的狀態可交由 IT 人員根據專業判斷來決定。

3.5. 故障資產的更換

當資產發生故障時，請考慮以下事項：

- **確認保固狀況：**將資產編號與《硬件資產清單》進行比對，以確認是否有保固服務及相關聯絡資訊。
- **確認是否有可用替換資產：**查閱《硬件資產清單》，確認是否有適合替換的可用硬件。

修改《硬件資產清單》，以反映任何硬件狀態的變更。

部署任何硬件變更時，請參閱《維護與修補程式管理實務指南》以獲取更換的詳細資訊。

3.6. 硬件資產的處置

若需處置硬件資產，請遵循以下程序：

- 在「硬件資產清單」中將待處置的資產標記為「待處置」。
- 將報廢理由及待報廢資產新增至「報廢紀錄」中。

- 經核准後，請依照政府電子廢棄物處置政策，或本校的一般資產處置政策進行處置。若資產內含營運資料，請參照《資料處理與保護 – 實務指南》進行安全處置。
- 資產處置完成後，請更新「硬件資產清單」中的相關資產，以反映該資產已處置。

3.7. 借用與歸還程序

準備工作

- **資產資格檢查**：使用借出/歸還清單核實資產的可用性與狀況。僅標記為「可用」且運作良好的資產方可借出。
- **借用者核實**：確認借用者的身分（例如：學生證、教職員證）及資格（例如：無逾期未歸還紀錄或使用限制）。針對學生，借用高價值物品時須取得家長同意。

借出流程

- **文件編製**：在《借還清單》及／或《硬件資產清單》中記錄交易，並註明：
    - 借用者姓名、聯絡資訊及身分（學生／教師／職員）。
    - 資產詳情（編號/標籤號碼、描述、現狀，如有照片請一併附上）。
    - 借出日期/時間及約定歸還日期。
- **簽署協議**：請借用者簽署協議，確認對該資產負有責任，包括因損壞或遺失可能產生的費用。
- **交接**：實際交付資產，並在「硬件資產清單」中將狀態更新為「已借出」。

歸還流程

- **歸還提交**：借用者須於指定時段內將資產歸還至指定地點。
- **檢查**：工作人員檢查資產狀況，並與借出記錄進行比對（例如，記錄任何損壞或缺失的零件）。
- **文件編製更新**：在借還清單中記錄歸還資訊，包括：
    - 歸還日期/時間。
    - 歸還後的狀況評估。
    - 有關問題或解決方案的備註。
- **結案**：經核實後，請在相關清單中將該資產標記為「可用性高」，並在需要採取進一步行動（例如：維修）時通知借用者。

記錄保存與審查

- 請以安全且便於存取的格式（例如：共用試算表、數據庫或資產管理軟體）維護借還清單，並備份資料。
- 定期審查清單以識別模式（例如：頻繁逾期），並進行準確性審計。

逾期與爭議處理

- **逾期處理流程**：若資產未於到期日歸還，應發送逐步升級的通知（例如：每日提醒，隨後通知主管／家長）。寬限期（例如：3 天）過後，應依據任何簽署協議中的約定，實施限制措施（例如：限制未來借用）或收取費用。
- **爭議解決**：若發生爭議（例如：既有損壞），請參照借還清單紀錄作為證據。

實務建議：

- 借用協議應涵蓋借用者對資產的維護、歸還，以及潛在維修或更換費用的責任。協議亦應明確規定借用期限、延期條件，以及逾期歸還或損壞的後果，以確保責任歸屬與合規性。

4. 建立軟體資產管理程序

本節說明學校如何運用「軟體管理清單」，建立完善的軟體資產管理程序。完善的軟體資產管理程序旨在提供所有軟體資產的最新資訊，以便在需要時能即時取得相關資料。

4.1. 更新軟體資產管理清單

在以下情況下應更新《軟體資產清單》：

- 取得軟體授權
- 軟體授權更新
- 安裝軟體
- 軟體報廢
- 軟體／固件變更
- 可能導致運行中軟體/固件變更的硬件變更（例如：更換網路設備）
- 在軟體資產清單審查中發現的任何不一致之處。

4.2. 軟體資產清單審查

軟體資產清單審查包含兩個部分，應定期（例如每年）一併進行。

- **完整性**：檢查學校目前使用的所有軟體是否已列入軟體資產清單。
- **正確性**：檢查軟體清單中的所有記錄是否有效，且沒有已淘汰軟體的記錄。

實作建議：

- 建議使用軟體掃描工具，掃描每台學校擁有的工作站上已安裝的軟體。
- 參照硬體資產清單，以確認工作站/個人電腦/伺服器以外的裝置（例如網路設備）之固件版本

附錄

硬件清單內容建議

欄位名稱	描述	數據類型	備註
Asset_ID	硬件資產的唯一識別碼（例如：自動產生或學校專屬的代碼，如 SCH-Comp-001）。	字串或整數	數據庫表的主鍵。
Asset_Type	硬件的類別（例如：桌上電腦、膝上電腦、印表機、投影機、平板電腦、伺服器、顯示器）。	字串	為確保學校環境中的資料一致性，請使用下拉式選單。
製造商	裝置的品牌或製造商（例如：戴爾、惠普、蘋果、愛普生）。	字串	
型號	具體型號名稱或編號（例如：Inspiron 15、iPad Air）。	字串	
序號	該裝置的製造商序號。	字串	此資訊對於保固索賠及唯一識別至關重要。
CPU_Specifications	處理器的詳細規格（例如：Intel Core i7-10700K 3.8GHz、AMD Ryzen 5）。	字串	請包含時脈、核心數，以及適用的世代資訊。
RAM	記憶體容量與類型（例如：16GB DDR4）。	字串	
儲存容量	硬磁碟或 SSD 容量與類型（例如：1TB HDD、512GB SSD）。	字串	
螢幕尺寸	螢幕尺寸（以英吋為單位，例如 15.6 吋、24 吋）——適用於桌上型電腦、筆記型電腦或獨立顯示器。	字串	若為非顯示裝置（如印表機），請留空。
作業系統	已安裝的作業系統及其版本（例如：Windows 11、macOS Ventura、Chrome OS）。	字串	
IP_Address	已連線裝置的網路 IP 位址。	字串	對於電腦或印表機等連網硬件，此為選填項目。

MAC_Address	網路界面的硬件 MAC 位址。	字串	對 IT 安全與追蹤很有幫助。

硬件清單內容建議（續）

位置	當前物理位置（例如：101 室、圖書館、行政辦公室、A 棟）。	字串	追蹤學校內的教室、大樓或部門。
指派對象	資產所分配的對象或部門（例如：約翰·多伊老師、科學系、學生證號 12345）。	字串	為確保責任歸屬，請包含使用者 ID 或姓名。
購買日期	資產的購買日期。	日期	格式：YYYY-MM-DD。
Purchase_Price	購買時的成本（例如：$850.00）。	小數或貨幣	如有需要，請包含貨幣符號。
供應商	供應商或賣方（例如：百思買、學區供應商）。	字串	
Funding_Source	資金來源（例如：學校預算、補助金、捐款）。	字串	適用於學校追蹤預算與補助款。
保固到期日期	保固的截止日期。	日期	針對即將到期的項目自動發送提醒。
服務合約詳情	任何現行服務協議的說明（例如：與 ABC Tech 簽訂的 3 年現場維修服務）。	字串	包含合約編號或條款。
支援聯絡資訊	支援聯絡資訊（例如：供應商電話：555-1234，電子郵件：support@vendor.com）。	字串	多個聯絡人可用分號分隔。
Insurance_Details	如適用，請提供保險單資訊（例如：受學校保單編號 #XYZ 保障）。	字串	適用於學校內的高價值物品。
狀態	當前運作狀態（例如：有效、維修中、報廢、遺失/被盜）。	字串	使用下拉式選單：運作中、需維修、已退役。
狀態	物理或功能狀態（例如：極佳、良好、尚可、不良）。	字串	依據稽核結果；包含損壞相關註記。
最後審核日期	最近一次狀態審計或檢查的日期。	日期	

硬件清單內容建議（續）

折舊值（可選）	資產的當前折舊價值。	小數或貨幣	根據購置價格和使用年限計算得出；適用於財務報表。
備註	其他備註或歷史紀錄（例如：升級歷史、維修記錄）。	文字	自由字段，供填寫其他詳細資訊。

術語表

術語	定義
資產管理	在整個生命週期中，對學校 IT 資產（硬件、軟體及相關記錄）進行識別、記錄、追蹤、維護及處置的結構化流程。
硬件資產清單	學校所擁有硬件設備的主清單，包含資產編號、序號、規格、用途、位置、狀態及保固詳情等關鍵字段。
軟體資產清單	軟體名稱與授權的清單，包含授權數量、到期日期、已安裝裝置（依資產編號）、版本，以及適用的固件資訊。
資產編號 / 資產 ID	分配給每項資產的唯一識別碼或標籤，用於追蹤、稽核及清單間的交叉比對。
主清單	用於篩選/查詢所有資產資訊的單一權威清單（通常為試算表或數據庫）。
附錄字段	本指南附錄中列出的清單建議數據字段（例如：CPU、RAM、儲存空間、序號、位置）。
完整性審查	旨在確保清單中包含所有正在使用的資產（無遺漏項目）的檢查。
正確性審查	檢查以確保資產記錄準確無誤（例如：狀態、位置），且已處置或報廢的資產未被列為活躍狀態。
資產狀態稽核	定期或臨時檢查設備是否仍能發揮其預期功能；檢查結果將予以記錄（通過／未通過，並附說明）。
硬件資產狀態稽核紀錄	記錄硬件資產的審計日期與結果，包含未能通過審計的理由，以支援維修或更換的決策。
處置記錄	記錄擬議及已完成處置事項的登記簿，內容包含資產編號、理由、核准狀態及最終處置方式。
生命週期管理	資產從導入、部署、維護、轉用、更換到處置的端到端流程。
用途變更	將資產重新分配給新的角色或使用者（例如：將電腦從辦公室用途轉為測試用途）。
測試硬件	專門用於實驗室／測試的設備，仍須在資產清單中顯示，並具備明確的用途／狀態。
替換設備庫	記錄於資產清單中的備用設備，可在資產故障或送修時進行部署。
保固詳情	為每項資產記錄的支援條款（保修期、供應商聯絡資訊），用以指導維修/更換決策。
狀態	狀態資訊，例如正常運作、維修中、故障或待報廢，用於決定處理優先順序。
固件	除個人電腦/伺服器以外的裝置（例如網路設備）上需追蹤與更新的嵌入式軟體。
授權數量	記錄於軟體資產清單中，可安裝/使用某軟體的授權數量。
授權到期	軟體授權權利的終止日期；用於規劃續約或移除。
已安裝裝置對應	將軟體記錄與其安裝的硬件資產編號進行關聯。

未經授權的應用程式	未獲准在學校使用的軟體；應透過掃描器等工具偵測並移除。
軟體掃描工具	用於彙整已安裝應用軟件報告，以便與軟體資產清單進行比對的偵測工具或腳本。
軟體技術管控措施	防止安裝或執行未經批准的應用程式的配置或政策設定。
狀態字段	用於支援稽核與報告的清單字段，用以標示當前狀態（例如：啟用中、存放中、待處置、已處置）。
庫存對帳	將實體檢查與掃描結果與資產清單進行比對，以解決差異的流程。
處置程序	批准並執行資產處置的步驟，包括安全數據清除及電子廢棄物合規。
安全資料清除	在處置或重新分配設備前，使用經核准的工具／方法將裝置上的數據永久清除。
電子廢棄物合規	依照政府或學校的環境政策進行處置，包括透過經認證的回收合作夥伴進行處理。
交叉參照關鍵字	用於連結硬件與軟體記錄的共通字段（通常為資產編號）。
使用者／保管人	目前負責該資產的人員或職位；為明確責任歸屬而記錄。
位置	資產的實體位置（例如：房間號碼）；用於稽核與追蹤。
用途/角色	資產的預期功能（例如：「101 室電腦」、「教室投影機」），有助於適配性檢查與稽核。
不適用	用於不適用於特定資產之字段的佔位值（例如：顯示器的 CPU 型號）。
變更觸發條件	需要更新資產清單的事件（例如：添購、報廢、故障、稽核差異）。
資產標籤	貼在每個裝置上的可見貼紙或標籤（例如：資產 ID 和用途），用以簡化識別與稽核作業。
稽核說明	當資產未能通過狀態稽核時所記錄的說明，用以支持維修或更換的決策。
標準建置映像	已擷取並經過強化處理的配置映像，用於一致且快速地部署或重置裝置。
表格關聯	將硬件與軟體清單進行關聯的方法（例如透過資產編號），以實現合併查詢與報表生成。

《存取控制實用指南》

版本 1.0

本文件旨在作為實用指南，僅供參考。各校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及需求。作者對任何基於本指南所採取的行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 前言 5
2. 維護存取控制標準 6
2.1. 存取控制政策的制定 6
2.2. 審查觸發條件 7
2.3. 記錄與稽核 9
3. 存取控制概念 9
3.1. 基於角色的存取控制 9
3.2. 最小權限原則與知情需要原則 10
3.3. 角色分離 10
4. 技術控制 11
4.1. 密碼驗證 11
4.2. 私密金鑰 11
4.3. 一次性驗證碼 12
4.4. 多重認證 (MFA) 12
5. 檢討與改進 13
5.1. 定期政策檢討 13
5.2. 因應新威脅與新技術 13
5.3. 持續改進 13
附錄 14
術語表 14

1. 前言

1.1. 目的與範圍

本指南為全港學校提供數據標籤的實用建議及基本標準。其目的是協助教育機構建立完善的存取控制系統，並透過詳盡的存取清單追蹤權限，確保學校系統及敏感數據僅由應有權限的人員安全地存取及處理。

本指南的範圍涵蓋制定以「審查觸發條件」為核心的正式存取控制政策，所謂「審查觸發條件」是指會觸發系統性存取權限審查的特定事件，以確保合適的對象能持續保有相應的存取權限。 本指南亦涵蓋存取變更的記錄及定期審查，以維持安全的存取環境。其設計旨在適應不同規模的學校、系統類型及可用資源。這些指引源自多個經認證的來源，包括香港教育局（EDB）以及互聯網安全中心（CIS），兩者均提供了作為本指南基礎的指導方針與資源。

1.2. 適用對象（資訊科技管理員及技術人員）

本指南適用於資訊科技管理員、技術人員，以及任何負責管理學校環境中用戶帳戶或資訊科技系統的人員。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，資訊科技團隊將能更有效地：

- 透過實施基於角色的存取控制（RBAC），實現可擴展的權限管理
- 實施重要原則與技術，例如最小權限原則、角色分離及多重認證，以有效規範存取權限
- 安全地管理密碼，並在執行管理任務時使用私鑰及一次性驗證碼

我們鼓勵各校根據自身技術環境與運作需求，靈活適配這些建議。

2. 維護存取控制標準

本節說明除技術控制措施外，建立及維護適當存取控制機制所需的盡職審查。技術控制措施僅應作為執行本節所定義政策之手段。

2.1. 存取控制政策的制定

概述正式政策（存取控制政策）的制定，該政策應基於業務需求，定義授予、限制及撤銷存取權限的規則。另起草一份文件（存取清單），明確列出存取權限以追蹤已授予的存取權。

以下列出 IT 部門在執行此項工作時應考慮的事項：

- **正式申請程序**：針對需用戶提供理由的存取申請，應採用標準化表單及票務系統。
- **申請驗證**：IT 部門應如何驗證申請的真確性，例如申請需經校方管理層確認。
- **限制存取權限**：針對所提供的理由或業務需求，制定程序以確定最低必要的存取權限。
- **撤銷存取**控制：任何用於在特定期間未使用後撤銷存取控制，或透過定期審查（例如每年）撤銷存取控制的管控措施。亦應包含任何通知機制及對該等通知的應對程序。
- **入職程序**：除基於申請的程序外，任何用於入職的批次程序（例如：授予教師／學生／承包商一套基本存取權限）
- **定義審查觸發條件**：列出需審查使用者已授予存取權限的各種情境。

調整建議：

- 請將此存取控制審查與《網路管理與無線安全指南》中所述的網路隔離準備工作結合起來。
- 本文檔後續章節將提供相關概念，以協助執行本節所述的流程。

實務範例：

- 整合
- 建立一個包含以下欄位的存取清單：
  使用者 ID/姓名：任何用於識別員工的方法。
  角色/職位：例如，教師、承包商
  存取資產/系統：授予存取權限的對象。
  存取層級：例如，管理員、讀寫權限、唯讀權限。
  授予日期
  到期日期

核准人，例如：校長、IT 管理員 理由

2.2. 審查觸發條件

定義在何種情況下須審查特定使用者的存取權限。以下清單供學校參考與考量，各校應自行配合實際情況調整。

使用者生命週期與狀態變更（教職員／員工）

- **員工變動**：當教師、行政人員或資訊科技人員遭解僱、辭職、退休或僱傭合約終止時，應立即審查並撤銷其存取權限，以防止未經授權存取學校系統（例如：電子郵件、學生數據庫）。
- **職務或職位變更**：當個人獲得晉升、降職、調任至其他部門，或承擔新職責（例如教師轉任科主任）時，應進行權限審查，並依據最小權限原則調整存取權限，以符合新職務的需求。
- **臨時指派或休假**：在短期職務結束時（例如代課教師、實習生，或正在休學術假、產假或長期病假的員工），應撤銷或暫停其存取權限；僅在該人員返回並經核實後方可恢復。
- **使用者身故或喪失行為能力**：在極少數情況下，於接獲使用者身故或長期喪失行為能力通知後，應立即撤銷存取權限，並依照法律規定處理數據移交事宜。

第三方及外部合作

- **承包商或供應商合作**：於專案完成、合約到期，或不再需要第三方服務（例如 IT 維護供應商）時，應審查並撤銷存取權限，包括移除任何臨時帳戶或 VPN 存取權限。
- **供應商或服務提供者更新**：若外部服務（例如 Google Workspace 等雲端供應商）變更條款，或學校更換供應商時，應重新審查存取權限，確保舊有整合方案不會留下殘留的存取權限。

學生相關變更

- **學生狀態變更**：針對學生帳戶，應在畢業、轉學、退學或停學／開除時審查並撤銷存取權限，以維護學習管理系統中數據的持續完整性。
- **年齡或資格里程碑**：針對受年齡限制的存取權限（例如：針對未成年人的特定教育工具），應在學生達到法定年齡門檻或變更年級時進行檢視與調整。
- **學年或學期結束**：在學期結束時系統性地審查學生及臨時人員的存取權限，以存檔或撤銷權限，為下個週期做好準備。

家長專用帳戶變更

- **學生畢業／退學**：無論是因畢業或學生退學而離開學校，都必須觸發家長帳戶的自動且立即停用。
    - 若學生的兄弟姊妹亦在該校就讀，家長帳戶應維持有效，直至所有相關家庭成員皆已畢業或退學為止。
- **監護權變更：**若學生監護權或法定監護責任發生法律變更（可能因家庭狀況或學生年滿 18 歲所致），應建立正式流程，允許學校行政人員通知 IT 部門，對該學生家長帳戶的相關權限進行審查。

安全事件與威脅

- **政策違規或安全事件**：若使用者涉及安全漏洞、系統濫用（例如分享憑證）或違反可接受使用政策，應立即進行審查，並在調查期間暫時撤銷其存取權限。
- **內部威脅指標**：一旦偵測到可疑行為（例如異常登入模式，或人事部門標記的問題，如即將採取的紀律處分），應主動審查其存取權限。

合規與監管觸發條件

- **法律或監管要求**：若接獲法院命令、根據《個人資料（私隱）條例》（PDPO）提出之數據保護請求，或合規稽核發現權限過高或未符合 ISO 27002 或 G3 指引等標準，應撤銷存取權限。
- **稽核結果**：在內部或外部稽核後，依據建議進行權限審查與撤銷，例如發現職責分離問題或未經授權的權限提升。
- **政策或指引更新**：在修訂學校的《存取控制政策》或採用新標準（例如教育局建議的更新）後，進行全面審查，以確保現有存取權限符合變更內容。

例行維護與監控

- **閒置或休眠帳戶**：定期掃描並撤銷已閒置達特定期間（例如：員工為 90 天，學生為學期結束時）的帳戶存取權限，以減輕因遺忘或棄置帳戶所衍生的風險。
- **定期排程審查**：以固定間隔執行例行稽核，例如特權帳戶每季一次，或所有使用者每年一次，以確認存取權限仍符合當前業務需求，並移除任何不必要的權限。
- **培訓或認證過期**：若所需認證或培訓已過期，應撤銷專用存取權限（例如：敏感研究工具），並僅在完成更新後恢復權限。

系統、數據與組織變更

- **系統或應用程式變更**：在進行重大更新、遷移至新軟體（例如：轉換至新的雲端評分系統）或淘汰舊系統時，應審查存取權限，以確保相容性並移除過時的存取權限。
- **組織重組**：若發生學校合併、部門重組或行政架構變更，應審查所有受影響使用者的存取權限，使其與新架構相符。
- **與外部系統整合**：與合作機構（例如共享圖書館系統）整合時，應審查存取權限，以防止意外的跨系統存取。

- **資料分類變更**：若資訊資產被重新分類（例如因新的隱私考量而從公開變為機密性），應據此檢視並限制所有使用者的存取權限。
- **技術或裝置變更**：當硬件設備（例如學校發放的筆記型電腦）遺失、遭竊或報廢時，或使用者更換至需重新驗證的新設備時，應撤銷與特定設備綁定的存取權限。

事件應變與緊急狀況

- **緊急或危機狀況**：在發生網路攻擊、自然災害或大流行病等事件期間，應暫時檢視並撤銷非必要的存取權限，以將風險暴露降至最低，並僅在運作復原後視需要恢復存取權限。
- **事件後復原**：在解決任何與存取權限相關的事件後，應進行全面審查，以確認所有臨時措施（例如緊急撤銷）已妥善完成。

其他管理觸發條件

- **管理層或使用者請求**：針對主管、人力資源部門或使用者本人提出的正式請求採取行動，在不再需要存取權限時（例如完成特定任務，如考試準備）撤銷該權限。

2.3. 記錄與稽核

保留每次存取控制變更的記錄，以便日後在定期稽核中進行檢視。定期檢視已授予的存取權限。

調整建議：

- 針對特權帳戶及存取權限（例如：管理員、敏感伺服器的讀取權限）應提高審查頻率，其餘則可降低頻率。建議至少每年進行一次全面審查。

3. 存取控制概念

本節闡述常見的存取控制概念，並說明學校如何將這些概念整合至其存取控制政策中。

3.1. 基於角色的存取控制

基於角色的存取控制是一種結構化的存取控制方法，其依據預先定義且對應於職務功能的角色來分配權限，而非依賴個別使用者身分。權限與角色相關聯，使用者則被指派至特定角色，藉此確保存取管理的一致性與可擴展性。

實作建議：

- 根據操作使用情境定義角色，例如教師、承包商、IT 服務人員、家長等。
- 當人員或職務發生變動時，應更新員工的職務角色，而非個別存取權限。
- 為因應臨時存取授權需求，應建立針對特定資源的臨時存取角色（例如建立「Web 伺服器 1 讀寫」、「備份伺服器 3 讀取」等角色），如此一來，透過檢視使用者的角色即可識別任何臨時存取權限。

3.2. 最小權限原則與知情需要原則

最小權限原則與知情需要原則是兩個相似的概念，通常相輔相成，

- **最小權限：**最小權限原則規定，僅應授予使用者、系統或程序執行其授權功能所需的最低權限。
- **知情需要原則：**知情需要原則規定，資訊存取權限僅限於確實需要存取該資訊的使用者。

簡而言之，這兩項條款共同要求，僅向有需求者授予存取權限，且獲准存取者所獲得的權限，應僅限於其執行工作所需的最低限度。

實務範例：

- 假設資訊與通訊科技（ICT）教師相較於一般教師，擁有對學校基礎設施的特殊存取權限。資訊科技部門應針對此情況建立兩個角色——「教師」與「ICT 教師」。「教師」角色將指派給所有教師，以提供其基本存取權限；而「ICT 教師」角色則指派給 ICT 教師，以賦予其對學校基礎設施的特殊存取權限。

3.3. 角色分離

角色分離（xml-ph-0000@deepl.internal）是管理高度提升權限的概念。具備高度權限的帳戶應僅專用於需要這些提升權限的工作。不需提升權限的任務，應使用未提升權限的帳戶執行。

實務範例：

- 為管理員建立兩個帳戶：一個用於行政管理，另一個用於日常工作。

4. 技術控制

應用程式層的存取控制通常透過技術控制措施實現。關於實體存取控制與網路層存取控制，請參閱相關指南。

本節列出跨網路驗證使用者時採用的各項技術控制措施及其相關要點。然而，這些控制措施的範圍僅限於需要使用者互動的控制措施 。學校在實施這些技術控制措施以執行其存取控制政策時，應特別留意這些要點。

4.1. 密碼驗證

密碼至今仍是最常見的共同認證方法。實施密碼驗證時需考量以下事項：

- 強度：遵循《密碼管理指南》以對使用者實施強度要求。
- 傳輸：密碼應透過安全的端對端加密通道（例如 TLS 1.3 連線）進行傳輸，以降低洩露風險。
- 驗證伺服器管理：應對密碼進行雜湊運算並加入鹽值，以降低洩漏時的損害。

密碼本質上要求使用者透過對密碼的知情來證明其身分。

應用建議：

- 密碼的強度在很大程度上取決於其長度，以及是否曾在其他地方重複使用。請遵循《密碼管理指南》，對使用者實施強度要求。

4.2. 私密金鑰

當端點儲存的私密金鑰可用於驗證使用者身分時，主要有兩種情況：透過客戶端憑證進行驗證，或對 SSH 連線進行驗證。

- 安全性：私密金鑰通常被視為高度安全的驗證方式，能提供加密級別的熵值。
- 傳輸：密碼應透過安全的端對端加密通道（例如 TLS 1.3 連線）進行傳輸，以降低洩漏風險。
- 驗證伺服器管理：驗證伺服器上將儲存一組已接受的公開金鑰。

這基本上要求使用者透過持有私密金鑰來證明其身分。

應用建議：

- 若要透過私密金鑰進行驗證，每個用於登入系統的端點都必須擁有私密金鑰。這意味著此機制在很大程度上依賴於存放私密金鑰之系統的安全性。
- 儘管安全，但這通常難以大規模部署，且常僅用於管理任務。
- 大多數私鑰管理工具會強制要求對生成的私鑰使用密碼短語進行加密。除非有特定限制（例如自動化需求）要求不加密，否則私鑰應予以加密；若需豁免，則須採取其他補救措施（例如將私鑰離線儲存於上鎖的機櫃中、嵌入硬件密鑰等）

4.3. 一次性驗證碼

一次性驗證碼可透過「域外」挑戰碼進行設定，來源可以是驗證器、信息或電話。

- 請確保此驗證碼是透過非標準管道傳送（例如，發送至某人的手機而非其工作電子郵件，因為後者可能已遭洩露）。
- 請確保驗證碼在短時間內（例如 90 秒）過期。
- 確保僅接受最新的驗證碼。

這基本上要求使用者透過存取預先建立的「非標準」通訊管道來證明其身分，通常是透過持有其手機來達成。

實務範例：

- 專用驗證器（如 Microsoft Authenticator 或 Google Authenticator）提供的功能不僅限於生成簡單的驗證碼，但它們都要求使用者持有特定裝置。

4.4. 多重認證 (MFA)

多重認證意指任何使用者驗證都應基於以下所述的兩個或更多因素：

- 他們所知的事物：密碼、安全問題等。
- 他們所擁有的：手機、USB 上的私鑰、MFA 驗證器等
- 其身分特徵：生物特徵等

綜合考量後，上述列舉的方案是學校大規模部署的可行選項，這意味著多因素驗證的實作通常會採用「密碼 + 驗證碼／驗證器」的組合。

5. 檢討與改進

5.1. 定期政策檢討

設定提醒，至少每年一次，或在資訊科技系統有變更時，檢視貴校的資料處理與標籤標準。應讓資訊科技人員及教學／行政同仁共同參與，以收集有用的回饋意見。

5.2. 因應新威脅與新技術

請隨時掌握可能影響學校的新型網路威脅，例如網路釣魚詐騙或密碼外洩事件。同時，也應留意可能提供更佳密碼保護方案的新技術或軟體更新，例如雙因素驗證。

5.3. 持續改進

每次檢討後，請視需要更新密碼政策。將任何變更清楚地告知教職員與學生，並提供簡易的操作指引或舉辦工作坊，協助所有人遵循新規則。

附錄

術語表

術語	定義
存取控制政策	一份正式文件，用以定義授予、管理及撤銷學校系統與數據存取權限的規則、程序及責任。
存取清單	詳細的記錄或日誌，用於追蹤誰擁有對哪些內容的存取權限，內容包含使用者 ID、角色、存取層級、日期以及存取的理由。
驗證因素	用於驗證使用者身分的憑證類別：您所知曉的（密碼）、您所擁有的（手機/安全令牌）以及您本身的生物特徵。
休眠帳戶	在指定期間（例如 90 天）內未被存取的用戶帳戶，若未停用或移除，將構成安全風險。
雜湊與加鹽	一種儲存密碼的安全方法，在儲存前將密碼（雜湊值）與唯一的隨機值（鹽值）結合，使其更難被破解。
最小權限原則	一項安全概念，要求僅授予使用者與系統執行其特定授權任務所必需的最低權限。
多重認證 (MFA)	一種安全流程，要求使用者提供兩種或更多不同的驗證因素來確認其身分，從而顯著強化安全性。
知情權限原則	一項安全原則，規定僅限於因工作需要而有正當理由查閱或使用資訊的個人，方可獲取該資訊。
入職程序	一套標準化且預先定義的流程，用於在新生（例如教師、學生）加入學校時，授予其一套基礎的存取權限。
一次性驗證碼	發送至使用者裝置（例如透過簡訊或驗證器應用程式）的臨時一次性代碼，用作第二重驗證因素。
獨立於主要驗證通道之外的通訊管道	一種與主要驗證通道分離的通訊管道（例如：在手機上接收驗證碼，而非透過正在登入的工作電子郵件接收）。
權限過高	指使用者帳戶擁有的存取權限超過其角色所需，從而造成重大安全風險的狀態。
私密金鑰	儲存在使用者裝置上的機密密碼匙，用於公開密碼學加密以驗證身分，通常用於安全的 SSH 連線或搭配客戶端憑證。
公開金鑰	與私密金鑰相對應的密碼匙，公開分享並由伺服器用於驗證持有相應私密金鑰之用戶的身分。
審查觸發條件	一組預先定義的事件或情況（例如：角色變更、員工離職或安全事件），會自動觸發對使用者存取權限的審查。
基於角色的存取控制 (RBAC)	一種存取管理方法，將權限分配給預先定義的角色（例如「教師」、「管理員」），而非個別使用者，從而簡化管理流程。
職責分離	一項旨在防止詐欺與誤差控制的安全原則，透過確保沒有任何單一人員能掌控關鍵任務的所有環節來達成。通常與「角色分離」相關。
角色分離	指針對不同職能使用獨立帳戶的做法，特別是要求管理員在執行日常任務時使用標準使用者帳戶，而在執行管理職責時則使用獨立的特權帳戶。
SSH（安全殼層）	一種加密規約，用於在不安全的網路環境中安全地運作網路服務，通常用於遠端命令列管理。

術語	定義
票務系統	一種用於管理與追蹤使用者請求的軟體系統，包含針對系統或數據存取的正式申請。
TLS（傳輸層安全性）	一種加密規約，為透過網路傳輸的資料提供端對端安全性，例如當密碼從瀏覽器傳送至伺服器時。

《密碼政策管理實用指南》

版本 1.0

本文件旨在作為實用指南，僅供參考。學校應審閱相關建議，並根據自身環境、資源及需求進行調整。作者對基於本指南所採取的任何行動概不負責。

目錄

1. 前言 4
2. 制定密碼政策 5
2.1. 最低要求 5
2.2. 密碼複雜度與長度 5
2.3. 禁止使用的密碼與密碼共享 6
2.4. 密碼變更頻率 6
2.5. 管理員與技術帳戶密碼 7
2.6. SaaS 解決方案與第三方應用程式 8
3. 實施密碼管理規範 9
3.1. 政策執行（一般方法） 9
3.2. 安全儲存密碼 9
3.3. 處理忘記密碼與重設密碼 10
3.4. 帳戶鎖定與恢復 10
4. 強化安全性 11
4.1. 多重認證 (MFA) 11
4.2. 顯示器顯示弱密碼或遭洩露的密碼 11
5. 事件應變 12
5.1. 處理遭入侵的帳戶 12
5.2. 溝通與升級處理 13
5.3. 必要時進行升級 13
5.4. 事件文件編製 13
6. 檢討與改善 14
6.1. 定期政策檢討 14
6.2. 因應新威脅與新技術 14
6.3. 進行改進 14
附錄 15
術語表 15

1. 前言

1.1. 目的與範圍

本指南為全港學校的密碼管理提供實用建議及基本標準，旨在協助教育機構建立安全、一致且有效的密碼管理措施，以保護學校系統及敏感資料。

本指南的範圍涵蓋密碼政策制定、技術控制措施、帳戶管理程序及使用者支援。其設計旨在能適應不同規模的學校、系統類型及可用資源。

1.2. 目標讀者（資訊科技管理員及技術人員）

本指南適用於資訊科技管理員、技術人員，以及任何負責管理學校環境中用戶帳戶或資訊科技系統的人員。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，IT 團隊將能更有效地：

- 制定並執行有效的密碼政策，
- 實施安全的儲存與驗證方法，
- 應對與密碼相關的事件，
- 向終端使用者提供密碼最佳實務的支援，
- 維持符合相關數據保護規範。

鼓勵各校根據自身技術環境與營運需求，適配這些建議。

2. 制定密碼政策

本節概述了學校強效密碼政策的核心要素。請將這些建議作為基礎，並根據貴校的系統、使用者群組及可用資源進行調整。強效的政策能同時保護一般使用者與關鍵管理員帳戶，使其免受常見威脅的侵害。

2.1. 最低要求

制定所有使用者在建立及保護密碼時必須遵循的明確基本規則。

典型的最低要求包括：

- 所有可存取學校資訊系統或敏感資訊的用戶帳戶，均須設定密碼。
- 預設或臨時密碼必須在首次使用時立即變更。
- 密碼不應書寫下來，或以明文形式儲存於他人可接觸之處。

調整建議：

- 學校可針對特定角色增設要求（例如，對可存取行政系統的職員制定更嚴格的規則），或根據不同平台的敏感程度進行調整。
- 針對年幼學生，建議採用易於記憶的密語而非複雜密碼，並為教師提供教室帳戶管理的指導。

2.2. 密碼複雜度與長度

強密碼較難被猜中或破解。建議如下：

- **長度：**一般使用者至少 8 – 12 個字符（若系統允許，越長越好）。
- **複雜度：**混合使用大寫與小寫字母、數字及符號。
- **避免簡單模式：**勿使用易被猜中的單字或模式（例如「password」、「1234」、學校名稱）。

適用建議：

- 對於難以記憶複雜密碼的年輕使用者，可考慮使用密語（多個無關的單字）。應根據不同年齡層或使用者角色，適度調整複雜度要求。

2.3. 禁止使用的密碼與密碼共享

預防常見的密碼錯誤以降低風險。

- **封鎖常見／遭洩露的密碼：**避免使用已知弱點或遭洩露的密碼（例如「123456」、「qwerty」）。
- **禁止共用密碼：**使用者不得共用密碼，即使是在教職員或學生群體內亦然。
- **專用密碼：**請勿在不同的學校系統中使用相同的密碼。

實用建議：

- 盡可能利用工具或目錄設定，自動封鎖常見密碼。透過定期提醒與培訓，強化這些規則的執行。
    - *在 Google Workspace for Education 中，管理員可於管理主控台的「安全性 > 密碼管理」中設定最低密碼長度與複雜度要求。*
    - *在 Microsoft Active Directory 中，請使用群組原則物件 (GPOs) 來強制執行密碼複雜度與長度要求。*

2.4. 密碼變更頻率

過於頻繁地變更密碼可能會導致密碼強度降低。最佳實務建議：

- **僅在必要時要求變更：**若懷疑帳戶遭入侵或其他安全事件發生時，才應變更密碼。
- **針對敏感帳戶設定定期變更：**對於關鍵系統，建議每 6 至 12 個月強制變更一次。
- **發生資料外洩後的強制措施：**一旦發生任何疑似資料外洩或風險事件，務必要求重設密碼。

實務建議：

- 根據您的環境調整變更頻率——除非絕對必要，否則應避免頻繁重設密碼，特別是針對學生。
    - 利用使用者目錄或帳戶管理系統，標記可能遭入侵的帳戶，並強制其重設密碼。
    - 發生釣魚攻擊事件後，請透過管理工具（例如 Google 管理主控台、AD 使用者與電腦）為受影響的使用者批量重設密碼。

2.5. 管理員與技術帳戶密碼

具備管理員或系統級存取權限的帳戶，需實施更嚴格的存取控制措施，以保護關鍵基礎設施及敏感數據。

- **更長的密碼：**要求至少 14–16 個字符，最好使用密語（例如：Sunny!Beach_Chair7Horse）。
- **獨特且複雜：**每個管理員帳戶都應擁有自己獨特且強大的密碼——絕不在不同系統間重複使用。
- **使用密碼管理工具：**部署信譽良好的密碼管理工具（例如 Bitwarden、LastPass 或 KeePass），以安全地生成並儲存複雜的密碼。
- **啟用多重認證 (MFA)：**務必為管理員及特權帳戶啟用 MFA。
- **禁止共用管理員帳戶：**為每位員工分配獨立的管理員帳戶；切勿共用登入資訊。
- **定期檢視：**定期審核管理員帳戶，移除不必要或未使用的帳戶。

實用建議：

- 若資源有限，請優先為管理員帳戶設定較長且複雜的密碼，並至少為所有雲端或關鍵系統帳戶啟用 MFA。
    - 要求 Google Workspace 或 Microsoft 365 中的所有管理員帳戶必須使用 MFA（透過管理主控台或 Azure AD 強制執行）。
    - 使用具備共享存取控制功能的密碼管理器儲存庫供 IT 團隊使用（例如 Bitwarden Organizations）。
    - 透過從目錄平台匯出使用者清單，並停用閒置帳戶，安排定期審查所有管理員帳戶（例如每季一次）。

- **強效管理員密碼範例：**
    - Sunlight$Giraffe!82_Rain
    - Puzzle#Leaf_Train!934
    - Ocean_Cable2!BridgeMoon

2.6. SaaS 解決方案與第三方應用程式

許多學校使用線上平台和應用程式進行教學、行政管理及溝通。即使無法控制每個設定，您仍可推廣強密碼慣例並管理風險。

- **檢視密碼選項：**只要有可能，請為 SaaS 平台（例如 Google Workspace、Microsoft 365、學習管理系統、圖書館系統）中的使用者帳戶設定強密碼政策。
- **強制實施多重認證 (MFA)：**在任何支援 MFA 的 SaaS 解決方案中，為教職員／管理員帳戶啟用 MFA。同時鼓勵教職員為其個人學校帳戶開啟 MFA。
- **各平台使用不同密碼：**要求使用者（尤其是教職員）為每個 SaaS 或第三方應用程式設定專屬密碼。例如：教職員不應將學校電子郵件密碼用作 Zoom、圖書館或線上學習入口網站的密碼。
- **使用單一登入 (SSO)：**若條件允許，請透過 SSO 將 SaaS 應用程式與學校的主要目錄（例如 Google、Microsoft Azure AD）整合。此舉可集中化驗證流程並簡化密碼管理。
- **密碼管理工具：**鼓勵教職員使用密碼管理工具來追蹤第三方平台的登入憑證，特別是當他們必須使用多種不同服務時。
- **供應商溝通：**採用新的 SaaS 或第三方應用程式時，應向供應商詢問其密碼政策、多因素驗證 (MFA) 支援狀況，以及他們如何保護使用者憑證。

實用建議：

- 有限的 IT 資源：應著重於使用者教育，並盡可能採用 SSO，以減少教職員與學生必須記住的密碼數量。
- 進階 IT 部門：標準化 SaaS 應用程式的入職/離職流程，並建立正在使用的平台清單，包括誰擁有管理員權限。

3. 實施密碼管理實務

本節說明如何透過技術控制與作業程序，將密碼政策落實於日常運作中。內容包含常見學校系統的範例，以及將這些措施適配您的環境的建議。

3.1. 執行政策（一般方法）

技術性執行：利用目錄服務或雲端管理主控台，強制執行密碼長度、複雜度及變更要求。*範例：在 Microsoft Active Directory 中，使用群組原則物件 (GPOs) 進行強制執行；在 Google Workspace 中，則透過管理主控台調整密碼設定。*

- **使用者教育：**在新人入職培訓及定期安全宣導活動中，提供關於密碼規則的明確指引與提醒。
- **定期稽核：**定期檢視帳戶及政策遵循狀況。*範例：執行報表以識別密碼強度不足或不符合規範的帳戶（若您的系統支援此功能）。*

實用建議：

- 若缺乏技術工具，請著重於使用者教育與定期提醒。

3.2. 安全儲存密碼

- **切勿以明文儲存：**請勿將密碼保存在試算表、電子郵件或紙本筆記中。
- **使用密碼管理工具：**為員工及 IT 管理員提供或推薦安全的密碼管理工具（例如 Bitwarden、KeePass）。
- **系統儲存：**確保任何儲存密碼的應用系統（例如自建應用程式）使用加密且帶有鹽值的雜湊演算法，而非明文或簡單加密。

實務範例：

- 使用 Bitwarden 或 LastPass 來儲存員工和管理員的密碼。
- 對於內部開發的應用程式，請您的 IT 供應商確認其密碼儲存機制採用強效的業界標準加密技術（例如 bcrypt）。

3.3. 處理忘記密碼與重設密碼

- **自助重設：**啟用具備安全身分驗證（例如備用電子郵件或簡訊驗證碼）的自助密碼重設功能。
- **服務台流程：**若使用者必須聯繫 IT 部門進行重設，請要求進行身分驗證（例如出示員工證或回答安全問題）。
- **密碼重設連結：**發送在短時間內（例如 30 – 60 分鐘）即失效的密碼重設連結。

實用建議：

- 為 IT 人員有限的學校制定簡單且安全的重設程序。

實務範例：

- Google Workspace 和 Microsoft 365 為已設定密碼恢復資訊的用戶提供自助式密碼重設選項。
- 針對低年級學生，可由班級教師在完成身分驗證後協助處理密碼重設事宜。

3.4. 帳戶鎖定與恢復

- **多次登入失敗後的鎖定：**配置系統在達到指定次數的登入失敗後（例如 5 至 10 次嘗試）鎖定帳戶。
- **通知使用者與管理員：**當帳戶遭鎖定時，應立即通知使用者與 IT 人員，以偵測可能的攻擊。
- **恢復程序：**提供經文件編製的流程，用於驗證身分並解鎖帳戶。

實務範例：

- 在 Active Directory 中，透過群組原則設定帳戶鎖定政策。
- 在 Google Workspace 中，顯示登入警示以偵測可疑活動。

4. 強化安全性

除了基本的密碼規則外，採取額外的安全措施能大幅降低帳戶遭入侵的風險。本節重點介紹每所學校都應考慮採用的進階做法，以保護使用者及敏感系統。

4.1. 多重認證 (MFA)

- 在所有支援多重因素驗證的系統上，要求員工/管理員帳戶必須啟用 MFA。在可行情況下，強烈建議所有使用者啟用 MFA。

4.2. 顯示器顯示弱密碼或遭洩露的密碼

- 利用可用工具檢查是否存在弱密碼、重複使用的密碼或已遭洩露的密碼。

實作建議：

- IT 資源有限：優先為管理員帳戶啟用 MFA，採用簡單但安全的密碼重設與恢復程序，並著重於使用者教育。
- 較先進的 IT 環境：自動化政策執行、使用密碼管理工具，並實施定期監控與報告機制。
-

實務範例：

- 在 Microsoft 365 中，透過 Azure AD 安全性預設值強制實施 MFA。
- 使用 Google 的「密碼警示」擴充功能，當使用者在非 Google 網站輸入學校密碼時發出警告。
- 使用資料外洩監控工具（例如 Have I Been Pwned），若員工的憑證出現在公開的資料外洩事件中，即向其發出警示。

5. 事件應變

本節說明若密碼遭洩漏或懷疑帳戶遭入侵時應採取的措施。迅速且有條不紊的應對措施可將損害降至最低，並保護學校數據。

5.1. 處理遭洩露的帳戶

1. **立即採取的行動**

- 停用或鎖定帳戶：暫時封鎖存取權限，以防止進一步的濫用。
- 重設密碼：在恢復存取權限前，必須設定新的強密碼。
- 強制登出：確保遭入侵的帳戶已從所有連線及裝置中登出。
- 啟用多重認證（若尚未啟用）：新增多重認證以提供額外保護。

實務範例：

- 在 Google Workspace 中，使用管理主控台重設使用者的密碼，並將其從所有裝置登出。
- 在 Microsoft 365 中，使用 Azure AD 重設憑證並撤銷存取憑證。

2. **調查事件**

- 檢查帳戶活動：檢視最近的登入紀錄、密碼變更及已發送的電子郵件，以確認是否有可疑活動。
- 釐清入侵手法：確定帳戶遭入侵的具體原因（例如：網路釣魚、弱密碼、惡意軟件等）。
- 掃描裝置：在發生入侵的電腦上執行防毒/反惡意軟體掃描。

3. **遏制與修復**

- 重設其他受影響的憑證：若該密碼亦用於其他地方，請一併重設。
- 更新並修補系統：確保系統保持最新狀態，以封堵任何漏洞。

5.2. 溝通與升級處理

1. **通知關鍵人員**

- 將所有疑似或已確認的資料外洩事件通報至貴校的 IT 部門或指定安全聯絡人。
- 若涉及敏感數據或多個帳戶，請通知管理層。

2. **通知受影響的使用者**

- 告知用戶其帳戶已遭入侵，並提供後續處理指引（例如：重設密碼、裝置掃描）。
- 僅向需要知悉的人員通報細節，在透明度與機密性之間取得平衡。

5.3. 必要時向上級通報

- 若敏感數據遭存取，或數據外洩可能影響眾多使用者，請依照法律或政策規定，將事件上報至學區資訊科技部門、法務部門或數據保護主管機關。
- 針對重大事件（例如學生數據外洩），請遵循貴校的數據外洩通報程序。

實務範例：

- 若洩露事件涉及學生個人資料，請通知貴校的數據保護主任，並遵循香港《個人資料（私隱）條例》（PDPO）的通報規定。

5.4. 事件文件編製

- 進行事件文件編製，記載事件詳情、已採取的行動及汲取的教訓。
- 在解決事件後，檢視事件經過，並視需要加強政策、培訓或技術控制措施。

6. 檢討與改進

6.1. 定期政策檢討

設定提醒，至少每年一次，或在資訊科技系統有所變更時，檢視貴校的密碼政策。應讓資訊科技人員與教學／行政同仁共同參與，以收集有用的回饋意見。

6.2. 因應新威脅與技術

隨時掌握可能影響學校的新型網路威脅，例如網路釣魚詐騙或密碼外洩。同時，也應留意可能提供更佳密碼保護方式的新技術或軟體更新，例如雙因素驗證。

6.3. 進行改進

每次檢討後，請視需要更新密碼政策。將任何變更清楚地告知教職員與學生，並提供簡易的操作指引或舉辦工作坊，協助所有人遵循新規則。

附錄

術語表

術語	定義
密碼政策	學校內建立及管理密碼的規則。
密碼管理工具	用於儲存及管理密碼的安全工具。
多重認證 (MFA)	一種需要兩種或更多身分驗證方式才能登入的安全機制。
網路釣魚	透過偽造電子郵件等手段，誘使人們洩露密碼的騙局。
數據外洩	未經授權存取敏感資訊的情況。
管理員帳戶	具備更高層級系統控制權限的用戶帳戶。
密碼重設	用於變更遺忘或遭洩露密碼的流程。
遭入侵的帳戶	遭未經授權者存取的帳戶。
加密	將資訊編碼為密碼以防止未經授權的存取。

維護與修補程式管理實用指南

版本 1.0

本文件旨在作為實用指南，僅供參考。各校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及需求。作者對基於本指南所採取的任何行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 前言 5
2. 建立修補程式管理生命週期 6
2.1. 漏洞識別與評估 6
2.2. 修補程式取得與驗證 7
2.3. 測試 7
2.4. 部署與回滾 7
2.5. 驗證與文件編製 8
3. 建立變更管理生命週期 9
3.1. 變更管理整合 9
3.2. 測試 9
3.3. 部署與回滾 9
3.4. 驗證與文件編製 10
4. 檢討與改進 11
4.1. 定期政策檢討 11
4.2. 因應新威脅與新技術 11
4.3. 持續改進 11
附錄 12
術語表 12

1. 前言

1.1. 目的與範圍

本指南為全港學校的系統維護及修補程式管理提供實用建議及基準標準。其目的是協助教育機構管理資訊科技更新與變更，重點在於透過安全的測試及部署程序，落實修補程式管理與變更管理。

本指南的範圍涵蓋變更管理與修補程式管理的生命週期，遵循包含申請、影響評估及測試的正式流程，並設有回滾程序以確保安全部署。 該生命週期亦涵蓋透過學校設定的定期檢討，以持續改進相關流程。本指南設計上可適應不同規模的學校、系統類型及可用資源。這些指引源自多個經認可的來源，包括香港教育局（EDB）以及互聯網安全中心，兩者均提供了作為本指南基礎的指導方針與資源。

1.2. 目標讀者（IT 管理員與技術人員）

本指南適用於資訊科技管理員、技術人員，以及任何負責學校環境中資訊科技系統軟體與修補程式管理的人員。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，資訊科技團隊將能更有效地：

- 透過定期掃描及監控威脅情報，並運用 CVSS 分數，主動識別系統漏洞
- 透過在隔離環境中進行測試，並搭配回滾程序部署，以確保系統穩定性，從而安全地部署與驗證修補程式
- 執行驗證掃描，以確認漏洞已修補或排除
- 透過定期檢討政策，實現持續改進並因應不斷演變的網路威脅

鼓勵各校根據自身技術環境與運作需求，適配這些建議。

2. 建立修補程式管理生命週期

本節詳述建立結構化生命週期的指引，涵蓋修補程式的取得、測試、部署及驗證，以將漏洞風險降至最低。學校應參照此指引，確保修補程式能系統化地套用，並在緊急性與系統穩定性之間取得平衡。

2.1. 漏洞識別與評估

學校應考慮採取以下措施，以掌握漏洞與修補程式資訊：

- **制定掃描時程**：定期對系統及一般網路／裝置執行自動化漏洞掃描，並配合學期行事曆以避免干擾。
- **監控威脅情報**：訂閱 HKCERT/GovCERT.HK 及廠商（例如 Microsoft、Google）的每日警示，以追蹤影響學校軟體（例如瀏覽器、作業系統）的高嚴重性問題。
- **風險評估流程：**參閱 CVSS 分數及可利用性與影響指標（例如：資料外洩風險）；針對高風險項目（例如：分數 >7）設定優先級，以採取立即行動。
- **定義回應時間：**設定必須修補漏洞的時間框架。此時間框架可視漏洞的嚴重程度而定。
- **文件編製與審查**：將發現結果記錄於漏洞登記表（例如：試算表）中，包含受影響資產、嚴重程度及負責人；每季進行審查以識別趨勢（例如：反覆出現且未修補的軟體）。

調整建議：

- 制定掃描時程表時，應配合學校行事曆，以避免造成潛在干擾。
- 可考慮依據漏洞的 CVSS 分數/評級建立兩級應對機制（例如：高風險項目需立即處理；中低風險漏洞則納入常規修補流程中處理）

實務範例：

- 使用 Nessus Community 進行漏洞掃描。若掃描目標數量受限，應優先處理關鍵系統並輪流掃描網路設備。

2.2. 修補程式取得與驗證

學校應僅從官方供應商來源下載修補程式，並驗證下載檔案的完整性。以下列出學校從互聯網取得修補程式時應高度考量的程序：

- 若官方修補程式發布來源不明，應聯繫軟體／硬件供應商尋求指引。
- 在下載及瀏覽官方網站以取得修補程式時，請確保使用適當的 TLS 連線。
- 應在與內部網路隔離的虛擬機器中下載修補程式。
- 驗證下載檔案的校驗和。校驗和應來自官方來源（例如：官方網站）。

實務範例：

- 確認網站用於生成校驗和的雜湊算法，然後在虛擬機器中計算下載檔案的雜湊值。常見的雜湊算法包括 MD5、SHA-1-384/SHA-2-256/SHA-3 等。

2.3. 測試

在隔離的測試環境（例如虛擬機器或隔離的實體機器）中套用修補程式，以檢查功能性問題。具體程序可能因軟體類型（軟體、作業系統修補程式、固件等）而異

- 測試環境應盡可能模擬生產環境，且測試案例應盡可能貼近實際使用情境。
- 測試環境應與內部網路隔離。

實務範例：

- 針對網路設備的新固件，應使用雙引導程序功能，以便在測試失敗時能輕鬆回滾。
- 在虛擬機器中進行應用程式更新的測試。
- 在與校內其他工作站規格及驅動程式版本相同的實體機器上，進行作業系統修補程式的測試。

2.4. 部署與回滾

部署前，請做好緊急回滾的準備。這包括以下準備工作：

- 通報系統停機時間與變更事項。這可能導致需在非工作時段進行部署，以避免中斷服務。

- 通報錯誤回報方法。
- 確定觸發更新回滾的條件。
- 若觸發回滾，應遵循的回滾程序及其相關先決條件。

調整建議：

- 若部署與回滾作業繁瑣，建議在全面部署前先進行小規模分批部署。

實務範例：

- 針對關鍵系統（例如網頁伺服器）的變更，請在部署前製作完整的磁碟克隆，以便輕鬆回滾。例如，使用 dd 命令克隆所有磁碟。回滾程序：關閉機器、移除所有磁碟、插入所有克隆磁碟，然後重新開機。
- 針對網路設備的新固件，請使用雙系統引導程序，以便測試失敗時能輕鬆回滾。
- 從任何配置備份中還原，以便網路設備的配置能保持一致。

2.5. 驗證與文件編製

重新掃描已部署的系統，以驗證修補程式是否已成功套用。詳情請參閱第 2.1 節。套用修補程式後，請更新相應的資產清單。

3. 建立變更管理生命週期

本節詳述建立結構化生命週期的指引，以確保對學校基礎設施進行變更時能保持可靠性。各校應參考並根據實際情境調整相關變更。

3.1. 變更管理整合

為與現有的變更管理程序整合（該程序定義了實施任何變更前的流程），應考慮以下事項：

- **正式申請與核准**：透過預先確定的溝通管道與流程，申請變更核准。
- **影響評估**：評估擬議變更對學校運作的影響（例如：停機時間、已知風險等）
- **資產管理**：將所有資產採購記錄於資產清單中。

3.2. 測試

如同套用修補程式一般，測試應在隔離的測試環境（例如虛擬機器或隔離的實體機器）中進行，以檢查功能性／相容性問題。

- 測試環境應盡可能模擬生產環境，且測試案例應盡可能模擬實際使用案例。
- 測試環境應與內部網路隔離。

適應建議：

- 所有測試的目的是將部署後流程無法運作的風險降至最低，儘管無法完全消除此類風險。 因此，學校應針對測試架設所需投入的資源進行風險評估。例如，若某系統允許停機且非關鍵系統，則可認為僅需進行基本功能測試即可；反之，若為備份系統，則可能需要更全面的測試，以在部署前盡可能找出潛在問題。
- 功能測試通常比可靠性測試更容易。
- 對於關鍵資產，應考慮進行測試部署（例如公開第二階段測試版），以模擬實際情境。

3.3. 部署與回滾

在部署前應做好緊急回滾的準備，這與套用修補程式時相同。第 2.4 節中的所有條款均適用，並需配合以下考量：

- 鑑於關鍵資產的複雜度較高，我們建議在對其進行變更前，先進行文件編製，記載逐步的回滾程序。
- 在測試版階段部署新服務會增加複雜度，若日後需要回滾，將導致數據遷移問題。
- 此外，可能存在更多觸發回滾的因素，例如負面使用者回饋。

- 對於任何新系統，請確定、文件編製並設定日誌服務以供監控。

3.4. 驗證與文件編製

持續監控日誌，以偵測任何可疑行為更新資產清單，以反映最近的部署狀況。

4. 檢討與改進

4.1. 定期政策檢討

設定提醒，至少每年一次，或在 IT 系統有所變更時，檢視貴校的資料處理與標籤標準。應邀請 IT 人員及教學／行政同仁共同參與，以收集有用的回饋意見。

4.2. 因應新威脅與新技術

隨時掌握可能影響學校的新型網路威脅，例如網路釣魚詐騙或密碼外洩。同時，也應留意可能提供更佳密碼保護方式的新技術或軟體更新，例如雙因素驗證。

4.3. 持續改進

每次審查後，請視需要更新您的密碼政策。請向教職員與學生清楚說明任何變更，並提供簡易的操作指引或舉辦工作坊，協助所有人遵循新規。

附錄

術語表

術語	定義
變更管理	一種結構化的流程，用於管理 IT 基礎架構的所有變更，從最初的請求和批准，到部署和驗證，以將中斷和風險降至最低。
校驗和	從檔案計算得出的唯一數位指紋（例如 MD5、SHA-256），用於驗證檔案的完整性，並確保其在下載過程中未遭損毀或竄改。
嚴重性	系統或漏洞的重要性等級，用以決定修補程式與應對措施的緊急程度及優先順序。
CVSS（通用漏洞評分系統）	用於評估電腦系統安全漏洞嚴重性的產業標準，透過數值評分協助設定應對措施的優先順序。
部署	將修補程式、更新或新系統安裝或部署至實際運作環境的過程。
雙系統引導程序	某些網路設備或電腦具備的一項功能，可儲存兩種不同的作業系統或固件版本，若更新失敗時，可快速回滾至前一版本。
完整磁碟複製	對整個硬碟（包含作業系統、應用程式及所有數據）進行逐位元精確複製，作為可靠的備份以利輕鬆還原系統。
雜湊算法	用於從一段數據中產生校驗和或雜湊值的特定數學函數（例如 MD5、SHA-256）。
影響評估	評估擬議變更或修補程式對學校運作、系統及使用者可能產生的正面與負面影響之過程。
隔離測試環境	一個獨立且隔離的網路或系統（例如虛擬機器），用於測試修補程式和變更，同時不影響實際運作環境。
公開測試	在正式上線前，新系統或重大變更的可用性將提供給更廣泛的真實使用者群體，以識別問題並收集回饋的測試階段。
修補程式	旨在更新電腦程式或其支援數據以進行修復或改進的軟體元件，包括修復安全漏洞及其他錯誤。
修補程式管理	為維持系統安全與穩定，針對作業系統及應用系統進行修補程式取得、測試、部署與驗證的完整生命週期。
生產環境	指學校日常運作所處的實際 IT 環境，有別於測試或發展環境。
回應時間	預先定義的時間框架，在此期間內必須處理或修補已發現的漏洞，通常依據其嚴重性等級而定。
風險評估	識別、分析及評估與漏洞相關風險的流程，包括其可利用性與潛在影響。
還原程序	一套預先規劃的步驟，用於在修補程式或變更部署失敗或出現問題後，將系統還原至先前狀態。
測試案例	一套特定條件或變數，測試人員將據此判斷系統是否運作正常，其設計旨在模擬實際使用情境。
威脅情報	針對威脅組織之潛在或現行攻擊所彙整、分析及精煉的資訊，通常來自 HKCERT 等資訊源。
TLS（傳輸層安全性）	一種加密規約，可在瀏覽網站或下載檔案時確保安全、加密的連線，以保護傳輸中的資料。

術語	定義
漏洞登記冊	用於追蹤已識別安全漏洞的記錄或文件（例如試算表），內容包含漏洞的嚴重性、受影響資產、狀態及負責人。
漏洞掃描	利用軟體工具自動掃描網路與系統，以識別已知安全弱點及未修補軟體的流程。

《數據備份與復原實用指南》

版本 1.0

本文件旨在作為實用指南，僅供參考。各校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及需求。作者對任何基於本指南所採取的行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 前言 5
2. 建立標準備份程序 6
2.1. 備份的頻率與範圍 6
2.2. 備份保留 6
2.3. 異地與冗餘備份 7
2.4. 備份加密 7
2.5. 備份完整性 8
2.6. 備份儲存媒體處理 8
3. 建立資料恢復程序 8
3.1. 定義恢復時間目標 8
3.2. 復原文件編製 9
3.3. 定期還原演習 10
4. 檢討與改善 11
4.1. 定期政策檢討 11
4.2. 因應新威脅與新技術 11
4.3. 進行改善 11
附錄 12
術語表 12

1. 前言

1.1. 目的與範圍

本指南為全港學校提供有關管理數據備份及恢復程序的實用建議和基本標準。其目的是協助教育機構在安全備份數據方面維持一致的基準，並建立一系列步驟來管理數據恢復的步驟和程序，以及對數據進行標籤和保護，確保學校系統和敏感資訊得到安全處理。

本指南的範圍涵蓋資料備份標準、備份的技術程序以及生命週期管理。其設計旨在能適應不同規模的學校、系統類型及可用資源。這些指引源自多個經認可的來源，包括香港教育局（EDB）以及互聯網安全中心（CIS），兩者均提供了作為本指南基礎的指引與資源。

1.2. 目標讀者（資訊科技管理員及技術人員）

本指南適用於資訊科技管理員、技術人員，以及任何負責管理學校環境中用戶帳戶或資訊系統的人員。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，資訊科技團隊將能更有效地：

- 建立標準化的備份流程，明確規定備份頻率、範圍及資料保留政策
- 透過安全資料處理框架進行系統化運作；包含加密實務、敏感資料儲存規範，以及限制將數據上傳至第三方服務
- 制定數據生命週期與刪除政策，以將潛在的數據外洩風險降至最低
- 根據營運需求，為各類數據定義具體的保存職責
- 安全刪除數據，確保資訊永久無法復原

鼓勵各學校根據自身技術環境與營運需求，適配這些建議。

2. 建立標準備份程序

本節概述了備份例行程序的核心組成部分，學校在建立備份程序時應考慮這些部分，以確保備份程序能夠有效運作。

2.1. 備份的頻率與範圍

為所有運作數據定義明確的備份間隔（例如：每日、每週等）。

若學校決定執行全磁碟備份，應將備份頻率記錄於備份程序中。若學校決定針對不同數據設定不同的備份頻率，則備份頻率應與對應數據的變更頻率相符。在此情況下，應彙整一份清單，記錄每項備份任務的範圍與頻率。

實務建議：

- 基於檔案的備份可在不同營運資料間提供備份頻率的靈活性；全磁碟備份雖能減少管理負擔，但需犧牲儲存空間。
- 我們強烈建議對所有經常修改的運作數據進行每日備份。
- 我們強烈建議導入自動化軟體來管理本地備份。

實務範例：

- 建立一份清單，記錄待備份的檔案及其備份頻率。請確保該清單涵蓋所有營運數據。

2.2. 備份保留

請在本地端保留至少 3 個版本的備份，以便在需要時能存取較舊的版本。

在制定保留政策時，我們強烈建議學校考慮以下事項：

- 若有助於管理作業，可考慮保留 7 或 5 個版本（例如：每週一覆寫前一週一的備份）。
- 可考慮將特定備份保留更長時間（例如：每週／每月／每年的首次備份）。

實用建議：

- 將備份保留政策與數據生命週期及刪除政策相互配合。

2.3. 異地與冗餘備份

我們建議建立多個備份副本，若可行，應包含一份異地副本。否則，請將冗餘備份存放於遠離原始備份的位置，或考慮採用雲端方案。

實務範例：

- 每週製作一份當前備份的完整磁碟副本。將硬碟存放在學校辦公室內的上鎖櫃中，並遠離備份伺服器。

2.4. 備份加密

備份應視為「靜態數據」，因此須依照《資料處理與數據保護指南》進行加密。

加密金鑰應以密碼加密，並存放在獨立的裝置、USB 隨身碟或 TPM 中。

適用建議：

- 密碼長度應至少為 15 個字符，並遵循管理員密碼政策。

實務範例：

- 將加密金鑰儲存於具備 TPM 輔助全磁碟加密功能的裝置中，例如 BitLocker。
- 使用存檔工具建立加密存檔（例如 7zip），並妥善管理密碼。

2.5. 備份完整性

將每次備份的校驗和儲存於獨立位置，以便在需要還原時檢查備份的完整性。

2.6. 備份儲存媒體處理

請考量以下事項，以安全的方式儲存備份：

- 將備份存放在物理上安全的場所。詳情請參閱《實用物理與環境安全指南》。
- 處於斷電狀態的 USB 隨身碟、SSD 及 HDD 應至少每年連接電源一次，以防止因位元翻轉導致數據遺失。對於 USB 隨身碟和 SSD 等快閃記憶體裝置，請供電至少一小時；對於 HDD，則需連接電源一天。

實務範例：

- 對於支援 SMART 功能的磁碟機，請使用 SMART 報告工具檢查其健康狀態。
- 若磁碟顯示老化跡象或達到預設的更換閾值，請透過「硬件資產稽核」標記為故障並更換磁碟，詳見指南

3. 建立資料恢復程序

本節概述學校在建立有效復原程序時必須考量的核心要素。這些措施將確保在發生事故時，能執行順暢且可追蹤的數據復原程序。

3.1. 定義恢復時間目標

將復原時間目標 (RTO) 定義為系統中斷後，恢復特定系統所能接受的最長時間。復原程序應是一份可在該復原時間目標內完成的指示清單。

實務建議：

- 應根據數據的重要性及對業務的影響來定義復原時間目標。例如，在發生事故時，允許某項資源（如網頁伺服器）停機的時間長度。
- 若任何恢復程序無法在 RTO 時限內完成，各校應考慮修改恢復程序，必要時亦應調整備份程序。
- 資源可劃分為不同層級，並針對各層級定義相應的 RTO。
- 若發生事故，RTO 亦可作為團隊的復原優先順序。

實務範例：

- 為不同的學校資源（例如網頁伺服器、檔案伺服器、雲端平台）定義 RTO。
- 每個資源可能包含子元件，相關內容可於《復原文件編製》中說明。

3.2. 復原文件編製

為每個資源建立逐步的復原指南。某個資源（例如特定伺服器）的典型復原指南包含以下內容：

- **初步評估：**關於評估影響範圍的指引——例如，確定受影響的系統（如學生數據庫與電子郵件），使用 RPO 指標估算資料損失，並隔離問題以防止擴散（例如，對疑似勒索軟體的系統斷開數據網絡連接）。包含用於記錄事件時間戳記、症狀及潛在原因的檢查清單。

- **備份選取與準備：**選擇最新可用備份的指示（例如，基於 RTO 目標，如在 4 小時內恢復關鍵系統）。詳述驗證步驟，例如掃描檢查數據損毀或惡意軟件，以及準備復原環境（例如，使用沙箱伺服器以避免覆寫即時數據）。
- **逐步還原流程**：針對數據還原的編號程序，包括：
    - 存取備份（例如：透過雲端入口網站或異地儲存裝置，以及解密程。
    - 還原流程，包含針對不同元件還原順序的特殊考量。
    - 工具與指令（例如：附帶螢幕截圖說明的特定軟體）。
- **驗證與測試**：關於執行還原後檢查的指南，例如用於驗證數據完整性的完整性測試（例如針對學生紀錄的樣本查詢），以及功能測試（例如確保評分軟體正常運作）。

- **回滾程序**：若還原失敗時的應變計畫，例如還原至較早的備份，或切換至備援站點／災難復原計畫。
- **文件編製與日誌**：要求記錄所有操作（例如：誰執行了什麼操作、何時執行），以供稽核之用。包含用於記錄結果的表單。

適應性建議：

- 將這些流程與《事件應變手冊》對齊，以確保沒有衝突。

3.3. 定期還原演習

復原演習旨在測試系統的可復原性，並驗證是否符合復原時間目標 (RTO)。因此應定期進行復原演習。

實務建議：

- 可考慮將復原演習納入事件應變演習之中。
- 主要應衡量的兩項指標為「復原成功率」以及「是否符合 RTO」。
- 演習結束後，應檢視是否有任何流程可進行優化。
- 切勿盲目調整 RTO。若 RTO 已達標，應預留緩衝空間；僅在優化後仍難以達成 RTO 時，才應提高 RTO 標準。

實務範例：

- 請在未連接到生產系統的備用伺服器上進行演習。

4. 檢討與改善

4.1. 定期政策檢討

設定提醒，至少每年一次，或在 IT 系統有變更時，檢視貴校的備份標準。應讓 IT 人員與教學／行政同仁共同參與，以蒐集有用的回饋意見。

4.2. 因應新威脅與新技術

請隨時掌握可能影響學校的新型網路威脅，例如網路釣魚詐騙或密碼外洩。此外，也請留意可能提供更佳密碼保護方式的新技術或軟體更新，例如雙因素驗證。

4.3. 進行改善

每次檢討後，請視需要更新您的密碼政策。將任何變更清楚地告知教職員與學生，並提供簡易的操作指引或舉辦工作坊，協助所有人遵循新規定。

附錄

術語表

術語	定義
備份加密	將備份資料進行編碼的過程，使其僅能透過特定的解密金鑰存取，即使儲存媒體遭竊，也能防止未經授權的存取。
備份完整性	衡量備份完整性與準確性的指標，確保數據未遭損毀或竄改，且能成功還原。
備份保留	一項政策，用以定義應保留多少個版本（世代）的備份，以及在刪除前應保留多長時間。
備份例行程序	一套標準化且排程化的程序，用於建立、儲存及管理學校數據的備份。
[二進制]數元翻轉	數位儲存中的一種數據劣化現象，指單一數據數元會自發性地改變其狀態，這可能隨時間推移導致檔案損毀，特別是在未供電的儲存媒體上。
校驗和	由檔案或備份生成的獨特數位指紋，用於透過檢查數據是否遭竄改或損毀來驗證其完整性。
靜止數據	指未在網路或裝置間主動傳輸，而是儲存於硬碟、固態硬碟（SSD）或備份磁帶等媒體上的數據。
數據關鍵性	衡量特定數據或系統對學校運作的重要性，有助於確定復原的優先順序與目標。
數據生命週期	數據從建立到刪除所經歷的完整過程，包括其活躍使用、儲存及最終處置。
加密金鑰	一種由算法用於加密和解密數據的機密資訊（例如密碼或數位檔案）。
基於檔案的備份	一種備份方法，透過複製個別檔案和資料夾，提供備份內容與頻率的靈活性。
備份世代	隨時間保存的不同備份版本（例如，週一、週二和週三的每日備份即為三個不同的備份世代）。
事件應變手冊	一套文件編製的程序，用於指導如何應對安全事件，例如資料外洩或系統故障。
異地備份	將備份數據儲存於與主系統不同的實體位置，以防範火災、水災或竊盜等本地災難。
營運數據	學校日常運作所需的即時數據，例如學生紀錄、財務資訊及教學材料。
復原文件編製	詳細說明如何從備份中還原特定系統或數據的逐步指南。
恢復點目標 (RPO)	以時間為單位衡量，可接受的最大數據遺失量。它定義了備份必須執行的頻率（例如，RPO 為 24 小時即要求至少每日執行一次備份）。
恢復時間目標 (RTO)	系統或服務在發生中斷後，可接受的最長離線時間，在此時間內必須恢復至運作狀態。
冗餘備份	備份資料的多份副本，通常儲存於不同地點或不同媒體上，以提高可靠性。

術語	定義
還原演習	定期、按計劃進行的測試，在受控環境中將數據和系統從備份還原，以驗證程序是否有效且能滿足 RTO 要求。
回滾程序	一種應急計畫，用於將失敗或出現問題的還原嘗試回滾至先前穩定的狀態。
沙箱伺服器	一種隔離的測試環境，讓 IT 人員能在不影響實際生產系統的情況下，測試軟體或執行復原演習。
SMART（自我監控、分析與報告技術）	內建於硬碟與 SSD 中的監控系統，可偵測並回報有關磁碟機健康狀態與可靠性的各項指標。
TPM（可信平台模組）	裝置主機板上專用的硬件晶片，提供安全的硬件級安全功能，例如儲存加密金鑰。
全磁碟備份	一種備份方法，會建立整個硬碟的完整副本（映像檔），包含作業系統、應用程式及所有數據。

《資料處理、標籤與數據保安實務指南》

版本 1.0

本文件旨在作為實用指南，僅供參考。各校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及要求。作者對基於本指南所採取的任何行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 前言 5
2. 建立數據標籤標準 6
2.1. 數據分類規則 6
2.2. 數據標記程序 6
2.3. 數據標籤審計 7
3. 制定數據處理準則 8
3.1. 安全數據傳輸 8
3.2. 安全數據儲存 8
4. 建立數據生命週期與刪除政策 9
4.1. 數據保留規則 9
4.2. 刪除數據 10
5. 檢討與改進 11
5.1. 定期政策檢討 11
5.2. 因應新威脅與技術 11
5.3. 持續改進 11
附錄 12
術語表 12

1. 前言

1.1. 目的與範圍

本指南為全港學校提供數據標記的實用建議及基本標準。其目的是協助教育機構在數據標記及保障方面維持一致的基準，確保學校系統及敏感資料得以安全處理。

本指南的範圍涵蓋資料標記標準、技術程序、安全的資料儲存與共用，以及資料生命週期管理。本指南的設計旨在適應不同規模的學校、系統類型及可用資源。這些指引源自多個經認證的來源，包括香港教育局（EDB）以及互聯網安全中心（CIS），兩者均提供了作為本指南基礎的指引與資源。

1.2. 目標讀者（資訊科技管理員及技術人員）

本指南適用於資訊科技管理員、技術人員，以及任何負責管理學校環境中用戶帳戶或資訊科技系統的人員。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，資訊科技團隊將能更有效地：

- 根據數據的重要性、敏感度及所需的安全等級，對數據進行分類
- 遵循與檔案／文件數據類別相關的統一標籤程序
- 透過一系列簡單且能維持一致安全性的步驟，安全地儲存及傳送敏感數據
- 理解數據生命週期，並掌握在數據不再需要時最佳的移除／銷毀方式

鼓勵各學校根據自身技術環境與運作需求，適配這些建議。

2. 建立數據標籤標準

本節概述了應遵循的資料標記標準的核心組成部分。此類規範可將數據分組為數據類別，以便更輕鬆地執行管控。請將這些建議作為基礎，並根據貴校的使用情境、使用者群組及可用資源進行調整。

2.1. 數據分類規則

根據數據外洩事件的影響程度，制定明確的基礎規則，將數據分類為 3 個等級。這些數據類別可用於定義適用於特定類別數據之共享與儲存的控制措施。

典型數據類別包括：

- 公開：公眾已知的知識，或即使意外洩露也不會造成危害的數據。
- 內部：任何包含非公眾所知資訊的數據，且若遭洩露將導致外部方獲取不符合公關策略的資訊。
- 機密：若遭洩露將可能造成嚴重聲譽損害，或引發合規或法律後果的數據。機密數據的常見範例為個人識別資訊（PII），即任何與在世個人相關且可推斷其身分的資訊。

應用建議：

- 學校可根據營運需求增設額外的數據類別。
- 針對儲存於不同媒介（例如紙本與電子檔）的數據，管控措施可能有所不同，但數據分類規則應保持一致。

2.2. 數據標記程序

應制定統一且簡明的程序，分別針對電子檔案與紙本文件標註數據。若使用者能辨識文件所屬的數據類別，即視為數據已標籤，但通常仍以統一性為佳。設計此類程序時，請考量以下事項：

- **程序的簡便性：**冗長的程序可能導致遵循意願降低。
- **辨識便利性：**資料標籤應易於員工辨識，以避免因不知情而導致的違規情況。

實務建議：

- 確保所有員工皆熟知數據標籤程序及數據分類規則。可考慮在員工休息室張貼海報以供快速參考。
- DLP 解決方案可能提供自動分類功能。請諮詢 IT 部門，以確保手動與自動流程之間保持一致。

實務範例：

- 手動為所有檔案添加標籤，並在文件上添加浮水印。若數位副本未含浮水印，可考慮在紙本上加蓋印章。例如，在文件名稱前添加標籤，如 [機密] Student_Data.txt。
- 可考慮開發自動化工具，例如將同一資料夾內所有文件標籤為具有機密性的工具。

2.3. 數據標籤審計

定期檢視數據及其標籤，以偵測標籤與數據間的錯位。

實務範例：

- 使用資料探索掃描器等工具，有助於定位敏感數據，從而快速列出需標籤為具有機密性的數據清單。閱讀其數據標籤以檢查是否存在不一致。

3. 制定數據處理準則

本節針對上述三種數據標籤提供控制措施範例。請將這些建議作為基礎，並根據貴校的使用情境、使用者群組及可用資源進行調整。

3.1. 安全數據傳輸

- **分享時進行加密：**將標籤為「機密」的所有檔案以密碼加密後再傳送給他人，並將密碼另行傳送。
- **限制接收者：**標記為具有機密性的數據的檔案不應上傳至任何第三方伺服器，包括生成式 AI 服務。

調整建議：

- DLP 解決方案可能提供即時監控功能，並可作為技術控制措施 s。
- 透過簡單的流程實現操作，無需專用工具，在透過檔案權限設定分享敏感資料時，設定安全的預設配置，包括將連結有效期限預設為分享後 24 小時內，並規定組織成員處理機密檔案時僅限「唯讀」權限
- 分享一份簡單易懂的單頁檢查清單，供員工安全地分享機密文件和資料，確保符合安全數據傳輸的慣例

3.2. 安全數據儲存

- **限制資料外洩：**避免 將 機密資料儲存於個人或未經批准的裝置中，除非已獲授權且經過加密。一旦不再需要，應立即從裝置中移除機密資料。
- **加密靜止數據：**除全磁碟加密外，應採用最先進的加密方案，對靜止狀態下的敏感數據進行加密。

實務範例：

- 為學校設備啟用 BitLocker。
- 使用由安全密碼生成的金鑰，以 AES256-CBC 形式加密所有備份。作為緊急備用方案，請將密碼寫在紙上，並存放於實體受控區域的保險箱中。

4. 建立數據生命週期與刪除政策

資料生命週期政策規定特定類型的数据應保留多久，以及之後應如何刪除，以將資料外洩風險降至最低。

4.1. 數據保留規則

文件編製：記錄學校所含的數據類別。針對每個類別，依據使用情境或任何合規要求定義保留期間。數據類別可能包括但不限於：

- 學生數據（人口統計數據、學業表現、醫療紀錄等）
- 學校流程數據（活動與考試日程、部門會議、會議記錄等）
- 教學資料
- 通訊紀錄 （發送給學生及教職員的公告與通訊，以及與第三方（包括政府部門、學校組織等）之間的其他往來）

調整建議：

- 若數據量過大以致無法人工審查（例如缺乏技術性控制措施），請優先處理包含個人識別資訊（PII）的文件 。
- 保存期限可採條件式設定，而非固定時限，例如：學生／教職員離校後 3 個月、供應商協議終止／到期後 1 年、資產處置後 1 年內之紀錄等。

實務範例：

- 使用 Microsoft Purview 等程式，該程式可追蹤文件的最後存取時間，並發出警示或刪除數據。

4.2. 刪除數據

請遵循《學校資訊保安——建議實務》（2019 年 9 月）第 6.3.5 節中的表格。

媒體類型	**重複使用（包括轉移以供重複使用）**	**處置（包括以舊換新及更換故障媒體）**
硬磁碟、軟磁碟、磁帶等非揮發性磁性媒體	覆寫	覆寫、消磁器或物理銷毀
非揮發性固態記憶體，例如 USB 隨身碟、記憶卡、固態磁碟 (SSD) 等	覆寫	覆寫或物理銷毀
光學媒體 - 只寫一次的媒體，例如 CD、DVD、藍光光碟等	不適用	物理銷毀
光學媒體 - 可重複寫入，例如 CD、DVD、藍光光碟等	覆寫	物理銷毀
智慧型裝置，例如 PDA、手機、平板電腦等	覆寫	覆寫、消磁器或物理銷毀

實務範例：

- 使用 Windows 中的 sdelete 等程式，透過覆寫方式安全刪除檔案。
- 考慮在重新使用前，使用 Autopsy 等鑑識工具檢查數據痕跡。

5. 檢討與改進

5.1. 定期政策檢討

設定提醒，至少每年一次，或在資訊科技系統有所變更時，檢視貴校的資料處理與標籤標準。邀請資訊科技人員及教學／行政同仁共同參與，以蒐集有用的回饋意見。

5.2. 因應新威脅與技術

隨時掌握可能影響學校的新型網路威脅，例如網路釣魚詐騙或密碼外洩。同時，也應留意可能提供更佳密碼保護方式的新技術或軟體更新，例如雙因素驗證。

5.3. 持續改進

每次檢討後，請視需要更新密碼政策。將任何變更清楚地告知教職員與學生，並提供簡易的操作指引或舉辦工作坊，協助所有人遵循新規則。

附錄

術語表

術語	定義
存取控制	用於限制僅授權使用者才能存取資訊科技系統、數據或地點的流程與技術。
人工智能	能夠執行通常需要人類智慧的任務（例如學習或解決問題）的電腦系統或軟體。
資產	學校擁有或管理的任何裝置、軟體、數據或系統，包括硬件、軟體及雲端服務。
備份	為防止數據遺失或損毀而另行儲存的數據副本，以便進行復原。
自攜設備	使用個人擁有的裝置（例如筆記型電腦、智慧型手機）進行學校活動或存取學校系統。
雲端服務	由第三方主機託管並透過互聯網存取的線上服務（例如：儲存空間、應用程式、平台）。
機密數據	必須防止未經授權存取的資訊，例如學生紀錄或個人數據。
網絡安全事件	任何企圖或實際發生的未經授權存取、使用、揭露、干擾、修改或破壞資訊或資訊系統之行為。
數據加密	將數據轉換為編碼形式以防止未經授權存取的過程。
數據外洩防護 (DLP)	旨在防止敏感資訊遭未經授權分享或遺失的工具或流程。
數據保護	為保護個人、敏感或機密資訊免遭未經授權的存取、揭露、竄改或破壞而採取的措施。
終端裝置	任何連接至學校網路的裝置（例如：電腦、平板電腦、智慧型手機）。
防火牆	一種安全系統（硬件或軟體），根據預先設定的規則監控並控制進出網路的流量。
事件	任何可能危及學校資訊或系統機密性、完整性或可用性的事件。
IT 協調員	負責監督學校資訊科技系統、安全及合規事宜的人員或職位。
日誌	用於監控與追蹤責任的事件記錄，例如系統存取或數據變更。
流動裝置管理 (MDM)	用於監控、管理及保障學校運作中所使用行動裝置的工具或流程。
多重認證 (MFA)	一種安全流程，要求使用者提供兩項或更多獨立的憑證以驗證其身分。
網路分段	將電腦網絡劃分為多個子網路，以提升安全性與效能。
修補程式管理	透過套用修補程式（patches）來解決漏洞或錯誤，以保持軟體最新狀態的流程。
個人數據／個人可識別資訊（PII）	任何與已識別或可識別之個人相關的資訊，例如姓名、身分證號碼或聯絡方式。
實體存取控制	用於限制進入建築物、房間或其他敏感區域的措施。

術語	定義
權限／特權存取	授予需執行管理或敏感任務之用戶的較高層級系統存取權限。
勒索軟體	一種惡意軟體，會鎖定或加密受害者的數據，並要求支付贖金以解鎖數據。
遠端存取	指從學校實體場地外部存取學校 IT 系統或數據的能力，通常透過 VPN 或安全連線實現。
敏感數據	一旦洩露可能對個人或學校造成損害的數據，例如健康紀錄或紀律處分報告。
供應商	向學校供應貨品或服務的任何第三方供應商或服務提供者，尤其是那些能夠存取數據或系統的供應商。
使用者	任何獲授權使用學校資訊科技資源的教職員、學生或其他人士。
漏洞	系統、軟體或流程中的弱點，可能被利用以危害安全性。
無線安全	為保護無線（Wi-Fi）網路免受未經授權的存取或攻擊而實施的存取控制措施與實務做法。

電子郵件安全實用指南

版本 1.0

本文件旨在作為實用指南，僅供參考。各校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及需求。作者對任何基於本指南所採取的行動概不負責。

版本歷史

版本日期	版本號	變更說明	作者

目錄

1. 簡介 5
2. 針對資訊科技部門的建議 6
一般建議 6
2.1. 隱藏電子郵件地址 6
2.2. 防範詐騙與釣魚攻擊 6
針對本地郵件伺服器的建議 8
2.3. 郵件伺服器防護 8
2.4. 防轟炸/防垃圾郵件措施 9
雲端郵件服務建議 9
2.5. 防轟炸/防垃圾郵件措施（雲端） 9
3. 給終端使用者的建議 11
3.1. 安全處理電子郵件 11
3.2. 可疑電子郵件的常見徵兆 12
術語表 14

1. 簡介

1.1. 目的與範圍

本指南為全港學校提供電子郵件安全的實用建議及基本標準，旨在協助教育機構建立安全、一致且有效的電子郵件管理措施，以降低學校系統及敏感資料遭入侵的風險。

本指南的範圍涵蓋垃圾郵件及釣魚防護措施、郵件伺服器管理、雲端管理郵件服務的技術控制，以及針對可疑電郵的通報與處理之用戶支援。本指南設計上可適應不同規模的學校、系統類型及可用資源。

1.2. 目標讀者（資訊科技管理員及技術人員）

本指南適用於資訊科技管理員、技術人員，以及任何負責管理學校環境中用戶帳戶或資訊科技系統的人員。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，IT 團隊將能更有效地：

- 在校園內全面實施嚴格的電子郵件安全措施，無論是處理收件或發件皆然。
- 啟用防詐騙及防釣魚措施。
- 維護郵件伺服器的安全與防護，包括雲端託管及自行架設的電子郵件伺服器。
- 分享安全處理電子郵件的通用做法與安全程序，並提供有關識別可疑電子郵件及採取應對措施的資訊與培訓。

鼓勵各校根據自身技術環境和運作需求，適配這些建議。

2. 針對資訊科技部門的建議

一般建議

2.1. 隱藏電子郵件地址

電子郵件地址也是密碼驗證的一部分。隱藏電子郵件地址意味著攻擊者將更難取得登入憑證。

- 為外部電子郵件配置基於角色的別名，以盡量減少個人地址的曝光。
- 設定複雜且難以預測的電子郵件名稱。

實務範例：

- 設定基於角色的別名，例如「外部通訊」，讓教師在回覆外部電子郵件時，可使用此別名取代個人電子郵件地址。
- 建議採用非直觀的姓名組合，例如使用「axc362@mail.com」而非「alice.chan@mail.com」

2.2. 防範詐騙與釣魚攻擊

- 準備有關識別及通報釣魚攻擊的培訓資料，並制定釣魚攻擊通報程序。
- 探索開源的釣魚偵測／分析軟體，並針對詐騙模式（例如：緊急關鍵字）配置伺服器過濾器。

實用建議：

- 製作培訓材料時，建議參考第 3 節的內容。
- 盡可能簡化網路釣魚通報程序。
- 開源的網路釣魚與垃圾郵件偵測技術，能提供值得探索的技術管控措施，而非僅仰賴終端使用者的通報。

實務範例：

- 開源建議：Apache SpamAssassin 用於過濾，ThePhish 用於自動化釣魚報告分析。

針對本地郵件伺服器的建議

本節概述了保障本地郵件伺服器安全的流程。請將這些建議作為基礎，並根據貴校的需求與限制進行調整。

2.3. 郵件伺服器防護

保護電子郵件的第一步，是保護郵件伺服器本身。以下提供一些通用建議，說明如何降低本地部署郵件伺服器的攻擊面。

- 部署防火牆，將 SMTP 流量限制在受信任的學校 IP 位址範圍內。
- 配置伺服器，從回應標頭中移除內部網路相關資訊。
- 對更新/修補程式進行盡職審查。詳情請參閱《維護與修補程式管理指南》。

實用建議：

- 若需外部存取，請使用 VPN，並在防火牆中將該 VPN 的 IP 範圍加入白名單。
- 若存在無法採用 IP 白名單的應用情境，請考慮使用黑名單，依據地區限制存取權限。

實務範例：

- 將學校無往來往的地區（例如北韓和伊朗）的 IP 加入黑名單。

2.4. 防轟炸/防垃圾郵件措施

本節建議採取措施，旨在偵測並過濾不受歡迎的電子郵件活動，包括濫發電郵、轟炸式發送及惡意郵件（例如病毒）。

- 實施記錄/入侵偵測機制，以自動封鎖可疑 IP，並針對此類事件設定行動裝置警示。
- 僅允許經過真確性驗證的使用者進行郵件中繼。
- 實施大小和速率限制，以防止資源耗盡。
- 對附件部署病毒掃描，並在檢測出病毒時將電子郵件隔離。

適應性建議：

- 設定閾值時請留意流量模式，因為在註冊期間或活動期間可能會出現電子郵件流量激增的情況。
- 考慮與現有的 IT 儀表板進行整合。

實務範例：

- 使用如 Fail2Ban 等工具進行入侵偵測並封鎖 IP 位址。
- 在中午 12 點至凌晨 6 點期間設定較低的閾值，因為此時預期流量較低，畢竟終端使用者應已入睡。

雲端郵件服務建議

本節 概述了在雲端郵件服務（例如 Outlook、Gmail）上保護電子郵件的安全流程。請將這些建議作為基礎，並根據貴校的需求與限制進行調整。

2.5. 防轟炸/防垃圾郵件措施（雲端）

多數雲端郵件服務預設已啟用垃圾郵件過濾器，並允許透過管理後台進行 配置。請檢查以下配置：

- 配置日誌記錄以進行異常偵測。

- 在設定中啟用寄件者驗證。
- 透過政策設定大小與頻率限制。

實用建議：

- 大多數雲端郵件服務供應商都內建了垃圾郵件/網路釣魚/病毒偵測功能。
- 建議尋找可將日誌匯出至本地端電腦的 API，以便整合第三方異常偵測系統。

3. 給終端使用者的建議

終端使用者（包括教師和學生）應考量以下事項，以最大限度地降低電子郵件攻擊媒介的危害性。請將本指南作為製作培訓材料的參考，或作為所有教師內部指引的範本。

3.1. 安全處理電子郵件

一般預防措施

- **驗證寄件者身分**：務必檢查寄件者的電子郵件地址的真確性。偽造的地址看似合法，但可能存在細微差異（例如：不尋常的網域）。如有疑慮，請根據您手邊的聯絡資訊致電給寄件者。
- **避免開啟來自未知寄件者的電子郵件**：請勿開啟或回覆未經請求的電子郵件。將其標記為垃圾郵件以改善過濾效果。
- **謹慎對待連結**：點擊前請將滑鼠懸停於超連結上，檢視目標網址。若網址看似可疑或不符，請避免點擊。
- **限制電子郵件地址的公開範圍**：將電子郵件用途限於工作相關。避免使用學校電子郵件註冊任何個人服務或帳戶（例如新聞訂閱），並避免在網路上公開電子郵件地址（例如網誌）。

處理附件

- **僅從可信來源下載附件**：僅限從已知聯絡人或經核實的組織下載附件。開啟前請使用最新的防毒軟體掃描所有附件。
- **安全管理加密附件**：若密碼出現在同一封電子郵件中，或信息源不明，請勿解密附件。應透過非同頻道（例如：電話或安全通訊應用程式）索取密碼，以確認其合法性。

應對可疑活動

- **刪除並通報可疑電子郵件**：立即刪除任何看似詐騙、包含緊急要求或索取敏感資訊的電子郵件。向您的 IT 部門或電子郵件服務供應商通報，以便進行調查。
- **切勿分享敏感資訊**：絕不要透過電子郵件提供個人、財務或登入詳細資訊，即使該郵件聲稱來自可信機構。請透過官方或非電子郵件管道（例如電話或安全通訊應用程式）核實相關請求。

實用建議：

- 讓教師知悉指定的通報管道，並持續提醒他們。
- 考慮製作海報，以持續提醒教師。

3.2. 可疑電子郵件的常見徵兆

寄件者與信頭異常

- **發件人地址仿冒或不符：**電子郵件看似來自可信實體（例如銀行或同事），但實際地址卻不熟悉或存在細微差異（例如「support@bankk.com」而非「support@bank.com」）。
- **來源出乎意料或未經請求：**來自未知寄件者或您先前未曾有過往來之組織的電子郵件，尤其是聲稱具有緊急性的郵件。

內容與語言指標

- **緊急或威脅性語言：**要求立即採取行動的措辭，例如「您的帳戶將被暫停」或「立即點擊以避免處罰」，旨在製造恐慌並繞過批判性思考。
- **索取敏感資訊：**以驗證或更新為名，要求提供密碼、財務數據或個人數據。合法組織極少透過電子郵件索取此類資訊。
- **語法、拼寫或格式錯誤：**存在錯誤、措辭生硬或品牌形象不一致（例如標誌或字體不符），偏離專業標準。
- **通用或非個人化的問候語：**使用「親愛的用戶」或「尊貴的客戶」而非您的姓名，顯示為大量發送的詐騙郵件。

連結與附件

- **可疑超連結：**連結內容與顯示文字不符（例如，將滑鼠懸停其上會顯示不同的網址）、導向不熟悉的網域，或包含常見網域的變體（例如 www.gmaiI.com 而非 gmail.com）。
- **意外的附件：**來源不明且副檔名異常（例如 .exe、.zip）的檔案，可能含有惡意軟件。若同一封電子郵件中包含加密附件，且密碼亦載於該郵件內，此類情況尤需提高警覺。

其他警示徵兆

- **承諾獎勵或獎品：**提供金錢、禮物或機會，但條件好得令人難以置信，通常需要點擊連結或提交數據。

- **情境不符：**提及您未曾發起的交易、未知帳戶，或您未曾參與的事件。

術語表

術語	定義
本地郵件伺服器	由學校自行管理、部署於校內網路或資料中心（而非公有雲）的電子郵件伺服器。
雲端郵件服務	由雲端服務供應商（例如 Microsoft 365、Google Workspace）主機及管理，並透過網頁控制台進行管理的電子郵件平台。
基於角色的別名	代表某個職能或團隊（例如 admissions@）的電子郵件地址，用於降低個人電子郵件地址的曝光風險，並簡化職務交接流程。
不可預測的電子郵件地址格式	一種命名規範，旨在避免易被猜中的模式（例如使用隨機字串取代 firstname.lastname），以阻礙帳戶猜測。
網路釣魚	一種社會工程學電子郵件攻擊，意圖誘騙收件人洩露憑證、數據或執行有害操作。
電子郵件詐騙	旨在謀取金錢利益或竊取數據的詐騙信息（例如：緊急付款通知、禮品卡索取、冒充 VIP）。
垃圾郵件	未經請求或大量發送的電子郵件，會佔用收信箱空間，且可能包含惡意連結或附件。
郵件轟炸	一種拒絕服務攻擊手法，透過發送極大量電子郵件來淹沒郵箱或伺服器。
發件人偽造	偽造「寄件者」地址或顯示名稱，使信息看似來自可信的寄件者。
寄件者驗證	透過技術或政策檢查確認寄件者是否合法，以減少偽造及冒充行為。
隔離區	一個暫存區，用以隔離可疑電子郵件以便審查，之後才會釋放到收信箱中。
附件惡意軟件掃描	自動分析附件檔案，以偵測並阻擋惡意程式碼。
連結保護 / URL 重寫	一種控制機制，會掃描並重寫連結，使連結的目標在點擊時經過塊核對，以阻擋惡意網站。
異常偵測	監控可能顯示濫用或遭入侵的異常電子郵件或登入模式（例如：流量激增、非典型 IP）。
防火牆	一種依據規則過濾網路流量的裝置／服務，用於限制 SMTP 並保護郵件系統。
SMTP（簡易郵件傳輸協定）	用於在伺服器之間，以及從客戶端傳輸至伺服器的電子郵件傳輸協定。
IP 允許清單（白名單）	一份允許存取服務的可信 IP 位址清單；預設情況下，其他所有 IP 位址均被封鎖。
IP 封鎖清單（黑名單）	因濫用、威脅或違反政策而被明確封鎖的 IP 位址清單。
速率/大小限制	用於限制特定時間段內的信息數量或大小，以防止資源耗盡及郵箱轟炸。
Fail2Ban	一款開源工具，可解析日誌並在偵測到重複的可疑活動後自動封鎖 IP 位址。

Apache SpamAssassin	一個開源電子郵件過濾框架，會針對垃圾郵件指標對信息進行評分，並啟用過濾動作。
ThePhish	一款開源工具，用於分析通報的網路釣魚電子郵件，協助自動進行分流與分類。
沙箱／隔離環境	一種受控的虛擬機器/容器，用於開啟或分析高風險檔案，同時避免危及生產系統。
標頭淨化	一種配置，用於從外發電子郵件的標頭中移除內部路由/系統詳細資訊，以避免洩露網路資訊。
帶外驗證	透過獨立的可信通道（例如電話通話）確認請求，以降低網路釣魚風險。
TLS（傳輸層安全性）	當系統支援並強制執行時，用於保護電子郵件客戶端與伺服器之間傳輸中數據的加密協定。
經認證的中繼限制	一項僅允許經過真確性驗證的使用者進行電子郵件中繼的規則，以防止開放中繼遭濫用。
管理主控台 / 儀表板	用於配置郵件安全設定、政策、日誌及警示的管理界面。
釣魚模擬	一項受控的測試活動，透過發送逼真的測試電子郵件，訓練使用者辨識並回報可疑信息。
公共 Wi-Fi 注意事項	向使用者提供指引，提醒除非已採取保護措施（例如透過 VPN 或預先加密的檔案），否則應避免透過開放式無線上網熱點存取敏感數據。

《流動裝置管理實用指南》

版本 1.0

本文件旨在作為實用指南，僅供參考。學校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及需求。作者對基於本指南所採取的任何行動概不負責。

目錄

1. 前言 4
2. 學校管理裝置之管控建議 5
若 MDM 解決方案的可用性高 5
2.1. 透過 MDM 解決方案實施的技術管控 5
2.2. 《可接受使用政策》附錄 7
若 MDM 解決方案的可用性不足 8
2.3. 無需 MDM 解決方案的替代技術管控措施 8
2.4. 與其他程序的整合 10
3. 關於處理自攜設備（BYOD）的建議 11
3.1. 網路分段與設定 11
3.2. BYOD 設備清單與核准 12
3.3. BYOD 設備清單審查 12
附錄 13
術語表 13
學校自有裝置可接受使用政策範本 17
自帶設備（BYOD）可接受使用政策範本 21

1. 前言

1.1. 目的與範圍

本指南為全港學校的流動裝置管理提供實務建議及基本標準。其目的是協助教育機構實施安全的管理措施，以保護在校園環境中使用，以及用於學校教育／行政目的的流動裝置。

本指南的適用範圍涵蓋學校無論是否已採用流動裝置管理（MDM）解決方案之情況，針對流動裝置的合宜使用提供技術管控措施與指引。此外，亦包含針對學校目前尚未採用 MDM 解決方案時，如何實施替代性技術管控措施的章節，以及將這些管控措施與其他安全措施整合的最佳實踐——請配合其他實用指南一併參閱。 本指引內容蒐集自多個經認可的來源，包括香港教育局（EDB）及互聯網安全中心（CIS），兩者所提供的指引與資源均構成本指引的基礎。

1.2. 目標讀者（IT 管理員與技術人員）

本指南旨在供資訊科技管理員、技術人員，以及任何負責管理學校環境中用戶帳戶或資訊科技系統的人員參考。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，IT 團隊將能更有效地：

- 透過 MDM 解決方案在行動裝置上實施技術管控
- 制定《可接受使用政策》，以規範校園環境中的行動裝置使用
- 透過將相關管控措施與其他程序整合，以支援 MDM 解決方案
- 在無法立即取得流動裝置管理工具的情況下，管理其他流動裝置管理解決方案
- 制定「自攜設備」（BYOD）政策，規範設備的網路隔離
- 建立 BYOD 裝置的功能清單，並制定審批與審查政策

鼓勵各校根據自身技術環境與運作需求，適配這些建議。

2. 針對學校管理裝置的管控建議

本節說明學校如何有效管理共享的「學校管理裝置」（例如學生平板電腦／筆記型電腦）的安全性。本節假設這些裝置屬於學校財產，且學校對其擁有完全控制權。

注意：MDM 註冊

我們強烈建議學校考慮採用專為教育領域設計的免費或低成本 MDM 解決方案。MDM 提供技術管控機制，可作為耗費大量人力進行政策管控的替代方案，從而節省大量人力資源。部分 MDM 供應商會為學校提供大幅折扣。

本指南的以下章節將分為兩種不同情境：第一部分將探討 MDM 解決方案的應用，另一部分則說明在未採用 MDM 解決方案時可實施的管控措施。

若 MDM 解決方案的可用性高

2.1. 透過 MDM 解決方案實施技術管控

本節列出學校可透過 MDM 針對共用裝置實施的建議管控措施。

2.1.1. 密碼政策執行

透過 MDM 執行密碼政策。
有關密碼政策的詳細資訊，請參閱《安全性配置檢查清單》。

2.1.2. 應用程式管理

建立一份明確的允許與禁止應用程式清單。

根據需求配置應用程式加入白名單或黑名單（若白名單限制過嚴，則改為黑名單）

調整建議：

- 定期（例如每年）檢視應用程式清單及對應的 MDM 控制設定，確保清單仍符合需求

2.1.3. 內容過濾

配置 MDM 以執行內容過濾政策。

實務範例：

- 針對所有經核准的教育資源採用白名單機制。若此方式過於嚴格，GitHub 提供大量由社群維護的有害內容網域黑名單。

2.1.4. 裝置加密

在裝置設定期間透過 MDM 啟用裝置加密。

實用建議：

- 請留意 MDM 軟體所採用的加密方案。應避免使用 DES 和 3DES 等弱加密演算法，以及 ECB 等弱區塊加密形式。

2.1.5. 遠端清除

透過 MDM 實施遠端清除功能，以防裝置遭竊或遺失。

實作建議：

- 在部署前應對遠端清除功能進行功能測試。
- 了解遠端清除功能的限制：某些實作方案需要被盜裝置具備互聯網連通性。

2.1.6. 定期更新

在裝置設定期間，透過 MDM 啟用裝置加密。

實用建議：

- 請留意 MDM 軟體所採用的加密方案。應避免使用 DES 和 3DES 等弱加密演算法，以及 ECB 等弱區塊加密形式。

2.1.7. 裝置使用後

當重新分配裝置用途時（例如指派給另一位學生），請透過 MDM 解決方案清除裝置數據。部分 MDM 系統允許自動執行數據清除，並重新啟用所有安全控制措施。

實務建議：

- 重新配置裝置時，請遵循《數據處理實務指南》中記載的正確程序。

2.2. 《可接受使用政策》附錄

MDM 解決方案可能會收集使用者活動以進行異常偵測。務必在裝置使用前告知使用者。若 MDM 解決方案會收集任何數據，以下說明應新增至《學校裝置可接受使用政策》的條款。

- **使用者活動監控：**告知終端使用者其裝置活動將受到監控。
- **資料蒐集與使用聲明：**列出 MDM 解決方案為監控目的將蒐集的使用數據，並聲明終端使用者同意《可接受使用政策》即表示接受此類數據的蒐集。MDM 解決方案常見的蒐集數據包括：
  - **應用程式使用與活動**：追蹤已安裝及正在使用的應用程式，以及其消耗的時間或數據量，包括列入黑名單或未經授權的應用程式。
  - **網路與數據使用**：顯示網路狀態、應用程式流量消耗及整體數據模式，以偵測異常或過度使用情況。
  - **位置與移動**：透過即時位置追蹤與地理圍欄技術，顯示裝置（進而延伸至使用者）所在位置，並常在進入未授權區域時觸發警示。
  - **使用者日誌與行為模式**：記錄使用者操作、會話日誌及行為異常，例如嘗試存取受限資源，或未經授權的網路存取等可疑活動。
  - **合規性與政策違規**：顯示組織政策的遵循情況，包括安全設定、軟體更新，以及來自用戶行為（如越獄或不符合規範的配置）的潛在威脅。

- **裝置使用模式**：裝置的整體使用模式，包括電池續航力、儲存空間及連線時長，這些可間接反映使用者的習慣。

實用建議：

- 不同 MDM 解決方案所收集的數據會有所差異。請在起草《可接受使用政策》時調整相關項目。

若 MDM 解決方案的可用性不高

本節列出學校在無需依賴 MDM 解決方案的情況下，除《可接受使用政策》外可考慮實施的替代管控措施。我們將先介紹技術管控措施，再提供《可接受使用政策》作為備用方案。

2.3. 無需 MDM 解決方案的替代技術管控措施

在缺乏流動裝置管理（MDM）解決方案的情況下，可實施替代性技術管控措施。然而，可擴展性仍是關鍵考量因素。雖然我們可以利用 Active Directory 群組原則來集中執行管控，但對於每台獨立運作或非網域裝置，仍須個別且在地地套用這些管控措施。

實作建議：

- 為簡化獨立裝置的部署流程，可先將一臺裝置配置為包含所需設定的「黃金映像」，再將其複製到其他類似裝置上。請注意，不同的控制措施組合將需要各自獨立的黃金映像。
- 無論採用何種方法，都應始終限制終端使用者對管理權限的存取，以維護安全性並防止未經授權的變更。

2.3.1. 密碼原則強制執行

- **已加入網域的 Windows 裝置**：設定「預設網域原則」以建立密碼原則。若要對低年級學生群組套用不同規則，請使用「細粒度密碼原則」。
- **獨立運作的 Windows 裝置**：使用「本機安全性原則編輯器」設定密碼原則。

- **macOS：**使用 Apple Configurator 建立定義密碼規則的 .mobileconfig 檔案。在裝置的初始設定過程中傳輸並安裝這些檔案。

有關密碼政策的詳細資訊，請參閱《安全性配置檢查清單》。

2.3.2. 應用程式管理

建立一份明確的允許與禁止應用程式清單。

不同作業系統皆內建用於將應用程式列入黑名單或白名單的工具，例如 Windows 的 AppLocker 及 macOS 的 Apple Configurator。

實用建議：

- AppLocker 規則是根據特定執行檔的發行者、路徑或雜湊值來設定的。這對於建立一份詳盡的黑名單而言可能頗具挑戰性。因此建議採用白名單。
- Apple Configurator 透過應用程式包識別碼 (bundleID) 來識別應用程式，使黑名單功能更為強大。

2.3.3. 內容過濾

在校園內實施全網內容過濾（例如 DNS 代理伺服器和防火牆規則）。

實務範例：

- 針對所有經核准的教育資源採用白名單。若此方式過於嚴格，GitHub 上有許多由社群維護的有害內容網域黑名單可供參考。
- 可考慮採用 OpenDNS 或 Pi-Hole 作為主要的免費選項。

2.3.4. 裝置加密

只要設定了密碼，現代的 Android 和 iOS 裝置都會對系統檔案進行加密。

針對 Windows 和 macOS 筆記型電腦，應部署管控措施以強制實施 BitLocker 和 FileVault。

- **已加入網域的 Windows 裝置：**建立 BitLocker 磁碟加密的群組原則。

- **獨立的 Windows 和 macOS 裝置：**逐一配置加密設定。由於這涉及整合 TPM 的全磁碟加密，直接克隆會引發注意事項。建議使用 USB 上的自動化腳本以簡化流程。

2.3.5. 裝置使用後清除

當設備轉作其他用途時，請手動清除設備數據。詳情請參閱《資料處理實務指南》。

2.4. 與其他流程的整合

- 請參閱《資產管理實務指南》，以獲取裝置分發的相關指引。
- 請參閱《實務指南：實體安全》，以獲取關於學校自有裝置安全儲存的指。

3. 關於處理自攜設備（BYOD）的建議

採用自帶設備（BYOD）對學校構成獨特的安全威脅，因為這本質上意味著允許外部設備存取學校資源。在教師和學生的設備上部署行動裝置管理（MDM）解決方案並不可行，且由於缺乏遵守意願，多數政策將難以奏效。

3.1. 網路隔離與設定

將所有自帶設備（BYOD）視為外部裝置。透過與學校基礎設施在物理或邏輯上均已隔離的存取點提供互聯網存取。

確保存取點的密碼安全。有關強密碼的定義，請參閱《安全檢查清單》。

確保學校無線存取點的協定版本為最新，例如使用支援 WPA3 的無線存取點。

若需存取內部網路，請考慮要求使用者憑證才能連線至存取點，或評估是否確實需要設置該存取點。

適應性建議：

- 對於需要透過自帶裝置 (BYOD) 存取內部數據的群組，應為每個群組設置獨立的存取點，並在邏輯上將這些存取點彼此隔離，同時與內部數據網絡隔離（例如透過防火牆/通訊閘）。如此即可實施存取控制。

實務範例：

- 假設教師無需透過自帶設備存取內部伺服器，請為內部互聯網存取與自帶設備/訪客互聯網存取分別使用兩家不同的互聯網服務供應商，並確保子網之間不存在任何實體連結。
- 假設教師需要存取內部資源，但學生則不需要。請建立總共 3 個子網——內部網路、教師 BYOD 及學生 BYOD。透過通訊閘/防火牆將教師 BYOD 與內部網路隔離，並為學生 BYOD 選用另一家互聯網服務供應商。

3.2. 自帶設備清單與審核

針對每台需連線至內部網路的自帶設備（BYOD），建立一套審核流程。

自帶設備清單

針對所有獲准存取內部資源的 BYOD 裝置，建立詳細的清單，內容包含使用者資訊、裝置詳細資料、已安裝應用程式清單以及核准日期。

核准

存取控制的核准應由 IT 部門負責，該部門應透過比對裝置與《BYOD 裝置使用規範》（AUP）中的技術管控措施，評估裝置是否符合規範。

若裝置符合規範，IT 部門可在終端使用者簽署《BYOD 裝置可接受使用政策》後，授予其存取所需資源的權限。

實務範例：

- 在終端使用者簽署《可接受使用政策》後，可透過根據 MAC 位址設定防火牆規則來授予存取權限。
- 授予存取權限時，僅應授予其所需的必要權限。

3.3. BYOD 設備清單審查

針對 BYOD 設備清單中的存取需求，定期（例如每年）進行審查。若使用者不再需要存取權限，應撤銷其存取權限。

附錄

術語表

術語	定義
學校管理的裝置	由學校擁有並完全掌控的裝置（例如：學生共用平板電腦／筆記型電腦），學校可對其強制執行設定、安裝軟體並限制使用。
流動裝置管理 (MDM)	一種平台，可集中註冊、配置及管理裝置，執行安全政策、部署應用程式、監控合規性，並能遠端定位或清除裝置資料。
MDM 註冊	將裝置註冊至 MDM 的流程，使其能接收並執行學校的政策與配置。
可接受使用政策 (AUP)	一套規範，用以界定使用學校裝置、網路及數據時，哪些行為屬可接受範圍，哪些則不可接受。
使用者活動監控	收集並檢視裝置／使用者活動（例如應用程式使用、網路使用、位置資訊），以偵測不當使用、政策違規或安全問題。
數據蒐集與使用聲明	AUP 中的一項聲明，說明 MDM 收集哪些數據、收集的原因，以及數據將如何被使用。
異常偵測	識別裝置或使用者行為中可能顯示濫用、遭入侵或違反政策之異常模式。
地理圍欄	一種基於位置的控制機制，透過虛擬邊界，在裝置進入或離開定義區域時觸發動作或警示。
使用記錄	帶有時間戳記的裝置與使用者操作記錄（例如登入、應用程式啟動、網路連線），用於監控與調查。
合規性監控	檢查裝置是否符合所需的安全設定與政策，以確保其持續符合規範。
政策違規	任何用戶或裝置未遵循既定學校政策或安全要求的狀況。
遠端清除	發送至裝置的指令，用於清除數據並將裝置恢復至出廠或基準狀態，通常在裝置遺失或遭竊時使用。
裝置加密	透過將裝置上儲存的數據轉換為無法讀取的形式，除非提供正確的金鑰或密碼，否則無法讀取，藉此保護裝置上儲存的數據。
全磁碟加密 (FDE)	一種加密技術，用於保護整個儲存磁碟，確保在裝置遺失或遭竊時，數據仍無法被讀取。
BitLocker	Microsoft Windows 的全磁碟加密技術，用於保護靜止狀態下的數據，通常會使用 TPM。
FileVault	Apple macOS 的全磁碟加密技術，用於保護靜止狀態下的數據。
可信平台模組 (TPM)	一種硬件晶片，用於安全儲存密碼匙，並支援裝置完整性檢查與磁碟加密。
密碼政策	用於建立、變更及管理密碼的規則（例如：長度、複雜度、鎖定）。

強密碼	符合或超過政策要求（例如：長度足夠、獨特且難以猜測）的密碼，用以抵禦暴力攻擊與猜測攻擊。
細粒度密碼政策	Active Directory 功能，允許針對不同使用者群組設定不同的密碼規則（例如：低年級學生與教職員）。
預設網域原則	與網域連結的基準群組原則物件，通常定義組織層級的設定，例如密碼原則。
本機安全性原則	用於在獨立（非網域）裝置上強制執行安全性配置的 Windows 本地端配置（secpol.msc）。
Apple Configurator	Apple 工具，用於建立和部署配置檔、管理裝置，以及在 iOS/iPadOS/macOS 裝置上安裝應用程式。
.mobileconfig	Apple 配置檔檔案，用於將設定（例如：密碼規則、Wi-Fi）套用至 Apple 裝置。
應用程式管理	控制哪些應用程式可以安裝或執行，以及應用程式在裝置上的部署與更新方式。
白名單 (允許清單)	一種控制方法，僅允許已核准的應用程式、網站或網域；其餘項目預設皆被封鎖。
黑名單 (封鎖清單)	一種控制方法，預設允許其他項目，同時封鎖特定的應用程式、網站或網域。
AppLocker	Windows 的一項功能，可根據發行者、路徑或雜湊規則，限制可執行的執行檔、腳本及封裝應用程式。
BundleID	Apple 生態系統中分配給應用程式的唯一識別碼，用於鎖定或控制特定應用程式。
內容過濾	基於類別、白名單或黑名單來限制對網頁內容或網域的存取控制。
DNS 過濾	透過控制 DNS 查詢來過濾網路存取，在建立連線前即封鎖或允許特定網域。
OpenDNS	一款基於雲端的 DNS 服務（Cisco），可提供基於類別的網頁過濾與安全防護。
Pi-hole	一款開源的 DNS 沉洞服務，可阻擋廣告與追蹤程式，並可用於網路上的基本網域層級內容過濾。
黃金映像	一種標準化且預先配置的系統映像，用於將一致的設定與軟體複製到多台裝置上。
克隆（磁碟映像）	將已配置裝置的映像檔建立並部署至其他裝置，以加速設定並確保一致性。
已加入網域的裝置	已連接到 Active Directory 網域的電腦，可進行集中式驗證與政策執行。
獨立裝置	未加入網域的裝置；由裝置本身進行本地端管理。
Active Directory (AD)	微軟目錄服務，用於管理整個組織中的使用者、群組、裝置、驗證及原則。
群組原則 (GPO)	Active Directory 機制，用於集中強制執行使用者與電腦的配置及安全性設定。
網路分段	將網路或使用者群組劃分為獨立區段以降低風險並限制存取的作法（例如：內部網路與自帶裝置（BYOD））。

子網	網路的邏輯子區段，擁有專屬的 IP 位址範圍，通常用於分離流量並實施不同的控制措施。
防火牆	一種根據預設規則允許或阻擋網路流量的安全設備或軟體。
通訊閘	一種網路裝置（通常為路由器或防火牆），用於連接不同網路，並在它們之間執行路由與存取控制。
存取點 (AP)	一種為用戶端裝置提供無線（Wi-Fi）網路存取的裝置。
WPA3	當前的 Wi-Fi 安全協定，其加密與驗證強度高於 WPA2。
憑證式驗證	利用數碼證書對連線至網路或服務的裝置或使用者進行驗證，通常用於確保 Wi-Fi 存取的安全性。
MAC 位址	網路界面的唯一硬件識別碼，有時用於存取控制清單或防火牆規則。
自攜設備	一種允許使用者在特定條件下，將個人裝置連線至學校網路或資源的作法。
BYOD 設備清單	記錄獲准存取內部資源的個人裝置清單，包含所有者、裝置詳細資訊、應用程式及核准日期。
核准流程	IT 部門用於審查、授權並授予裝置存取特定資源權限的步驟與標準。
合規性檢查	在授予或保留存取權限前，針對裝置進行的評估，以確認其是否符合所需技術控制措施及《使用者行為準則》（AUP）標準。
使用後裝置清除	在將裝置重新指派給另一位使用者之前，清除使用者數據並恢復基準配置的流程。
安全銷毀/清除	在重新配置或報廢裝置時，永久清除數據以確保無法復原。
數據處理實務指南	一份內部參考文件，其中定義了安全處理數據、清除數據以及重新配置裝置的程序。
資產管理實務指南	一份用於分配、追蹤及維護學校所有設備的內部參考文件。
實務指南：實體安全	一份關於裝置實體安全（例如：儲存、存取控制）的內部參考文件。
加密演算法	用於加密與解密數據的算法；其強度會影響整體安全性。
DES	一種過時的對稱加密演算法，現已被視為不安全，且不適合用於現代數據保護。
3DES	一種將 DES 演算法應用三次的舊式加密演算法；現已被視為安全性不足，正逐步淘汰。
ECB（電子密碼本）	一種不安全的區塊加密形式，會暴露數據中的模式，應避免使用。
內容白名單	一份列出使用者獲准存取之網站或網域的清單；其餘皆遭封鎖。
網域黑名單	一份禁止的網站或網域清單，用戶不得存取；其餘網站仍可存取。
DNS 代理	一種代表客戶轉發 DNS 查詢的伺服器或服務，並能執行過濾與記錄政策。

互聯網服務供應商 (ISP)	提供互聯網連通性服務的公司；可使用不同的 ISP 來隔離內部網路與自帶裝置（BYOD）／訪客網路。
越獄	移除裝置（例如 iOS）上製造商或作業系統限制的行為，此舉允許未經授權的應用程式或設定，並削弱安全性。
不符合規範的配置	指裝置狀態不符合所需的安全政策（例如：作業系統過時、加密功能已停用，或安裝了禁止的應用程式）。

學校自有裝置可接受使用政策範本

學校自有裝置之可接受使用政策 (AUP)

前言

本《可接受使用政策》（AUP）概述了將學校所有設備（如筆記型電腦和平板電腦）用於教育目的的準則。這些設備旨在支援學生與教師的學習、教學及與學校相關的活動。 所有使用者必須負責任地使用這些裝置，以保護學校數據、確保安全，並遵守法律與道德標準。使用學校所有裝置即表示您同意遵守本政策中概述的所有規則。違反規定可能導致紀律處分，例如喪失裝置使用權、留校察看（針對學生），或由學校行政部門決定的其他後果。

本政策涵蓋裝置使用、安全及維護等關鍵領域。所有使用者均應詳閱並遵守這些指引。

安全 Wi-Fi 使用

為保護學校資訊及個人資料，連接安全網路至關重要。

- 當存取重要學校資訊（例如學生紀錄或成績）時，請僅連接安全且由學校提供的 Wi-Fi 網路。這些網路旨在確保您的資訊隱私與安全。
- 除非您使用經學校核准的虛擬私人網路（VPN），否則請避免在公共無線上網熱點（如咖啡廳或購物中心）進行與學校相關的工作。公共網路通常不安全，可能會使您的資訊面臨風險。
- 若您不確定某個 Wi-Fi 網路是否安全或合法，請向學校的 IT 人員求證。

安全數據處理

安全地處理學校數據對於維護隱私及防止未經授權的存取至關重要。

- 管理敏感資訊（例如學生證號、個人資料）時，請僅使用經學校核准的應用程式或平台。這些經核准的工具（例如安全的雲端儲存服務）均配備端對端加密功能，以保護您的資料。
- 切勿在未經加密或未經學校核准的應用程式或網站上輸入敏感資訊。請確認網站網址中是否包含「https://」，這表示該連線是安全的。
- 若您對應用程式或網站連通性的安全性有任何疑慮，請諮詢學校的資訊科技人員。

數據備份與同步

定期備份課業資料有助於防止資料遺失，並確保您的學習進度得以保存。

- 請使用學校提供的工具（如 Google Drive 或 OneDrive）來儲存和同步所有學習檔案。請務必依照學校指示啟用加密功能。
- 請定期將作業儲存至學校認可的雲端儲存服務。此做法對於防止作業與專案遺失至關重要。
- 請向 IT 人員確認您的備份設定是否符合學校的安全與加密要求。

裝置儲存

- 當裝置未使用時，請將其存放於安全處所，例如上鎖的櫃子或書包內。當您身處校外時，這點尤為重要。
- 避免在公共場所或未受保護的區域將裝置置於無人看管之處。

遵守登入與密碼政策

遵循登入與安全規範，可保護您的裝置、帳戶及學校網路。

- 請依照資訊科技部門的要求，建立並維持強密碼。何謂強密碼，請參閱《安全配置檢查清單》。切勿將密碼透露給任何人。
- 若發現登入或自動鎖定設定有任何問題，請立即向 IT 人員通報。此舉可確保您的裝置安全無虞。

密碼管理

- 請勿將學校電子郵件、網路登入或其他帳戶的密碼直接儲存於裝置中。
- 在首次設定裝置時，請停用網頁瀏覽器或應用程式中的自動儲存密碼功能。
- 請將密碼記在腦中，或若學校提供經核准的密碼管理工具，請使用該工具。

裝置歸還與數據清除

- 在處置裝置或將其轉交給其他學生之前，請先將裝置交還給 IT 人員進行數據清除。請勿嘗試自行從裝置中清除數據。

設備清點報告

- 若裝置發生任何狀態變更（例如遺失、損壞或重新分配給他人），請立即向 IT 人員通報。此舉有助於學校維持準確的資產清單紀錄。

一般使用準則

除上述以安全為核心的規定外，以下準則旨在確保師生能負責任且有效地使用校方設備：

- **允許用途**：裝置僅限用於與學校相關的活動，包括課堂作業、家庭作業、備課、批改作業、研究及專業發展。有限度的個人用途（例如查看天氣或使用教育類應用程式）在不妨礙學校職責或違反本政策的前提下，是被允許的。
- **禁止活動**：
    - 未經資訊科技部門批准，擅自安裝未經授權的軟體、應用程式或擴充功能，此舉可能引入安全風險或違反授權協議。
    - 存取、下載或散佈不當、非法或受版權保護的資料，包括但不限於暴力、歧視性或露骨的性內容。
    - 將裝置用於遊戲、社群媒體（除非經學校核准用於教育目的），或任何會分散學習或教學注意力的活動。
    - 修改裝置設定、硬件或軟體，超出資訊科技部門明確允許的範圍。
    - 透過學校裝置或帳戶進行霸凌、騷擾或發送不當信息。
- **互聯網與電子郵件使用**：為確保安全及符合規範，所有透過學校裝置進行的互聯網及電子郵件活動均受監控並記錄。請僅將學校電子郵件用於教育相關通訊。請尊重智慧財產權，並避免透過未加密的管道分享機密資訊。
- **設備保養與維護**：請小心使用設備以避免損壞。如有任何硬件問題（例如螢幕破裂、電池故障），請立即向 IT 部門通報。請勿自行嘗試維修。
- **遠端存取與校外**使用：在校外（例如在家中）使用裝置時，請確保處於安全的環境中。啟用所有必要的安全功能，例如閒置後自動鎖定及全磁碟加密。學生在家中使用裝置時，應視情況接受家長監督。
- **監控與隱私**：學校保留監控裝置使用情況的權利，包括檔案、電子郵件及瀏覽紀錄，以確保遵守規定。使用者對校方所有裝置不應期待隱私權。

違反規定的後果

違反本《使用規範》可能導致：

- 學生：喪失裝置使用權、留校察看、通知家長，或其他校方紀律處分。
- 針對教師：暫時停用裝置、強制再培訓、績效考核，或其他行政處分（最高可包含解僱）。
- 若違規涉及非法活動或數據外洩，將採取法律行動。

學校將迅速且公正地調查所有通報之違規行為。

《可接受使用政策》（AUP）確認書

理解並同意學校的裝置使用規則是必經步驟。

- 在開始使用學校裝置之前，請審閱並簽署由 IT 人員提供的確認表格（紙本或電子表格）。此表格確認您已理解這些準則。未滿 18 歲的学生，其父母或監護人亦須簽署。
- 若《可接受使用政策》（AUP）或安全提醒的任何部分有不明之處，請聯繫 IT 人員以求澄清。

透過簽署，您確認已閱讀、理解並同意遵守本《可接受使用政策》。本政策可能隨時更新；如有變更，將通知使用者，並視需要要求重新確認。

使用者簽名：_____ **日期：**_____

姓名（正楷）：_____ **身分（學生／教師）：**_____

配發裝置： _____

家長／監護人簽名（若學生未滿 18 歲）：_____ **日期：**_____

如有疑問或需要支援，請聯絡學校的 IT 人員，聯絡資訊為 [插入資訊]。

自帶設備（BYOD）合宜使用政策範本

自攜設備可接受使用政策

前言與目的

本《可接受使用政策》（AUP）概述了個人行動裝置（BYOD），例如智慧型手機、平板電腦及筆記型電腦，在連線至學校網路及資訊系統時的使用準則。本政策旨在確保安全、受保護且高效能的學習環境，同時保護學校資料、網路及資源免受未經授權存取、資料外洩、惡意軟件及敏感資訊遺失等風險。

本政策參照教育局（EDB）的《學校資訊保安 — 建議做法（2019 年 9 月）》制定，特別是第 5 章（存取控制）、第 7 章（網絡與通訊安全）及第 9 章（行動裝置與行動應用程式保護）。 本政策提倡「最小權限」、「知情需要」及「負責任使用」的原則，以符合相關法例，包括《個人資料（私隱）條例》。

本校鼓勵為教育目的使用自帶設備（BYOD），但保留在政策遭違反時限制或撤銷存取權限的權利。

適用範圍

本政策適用於：

- 所有使用個人裝置連線至學校 Wi-Fi 網路、有線連接或任何學校 IT 資源的學生、教職員及訪客。
- 自帶設備（BYOD）涵蓋任何能具有學校網路連通性的個人行動裝置（例如：iOS/Android 手機/平板電腦、筆記型電腦）。
- 校方自有設備雖受其他資訊科技政策規範，但在與自帶設備（BYOD）併用時，仍須遵循類似的安全標準。

基於無障礙需求，經資訊科技主管批准後，可獲豁免。

可接受使用準則

使用者可將自帶設備用於：

- 教育活動，例如存取學習管理系統、學校電子郵件或經核准的線上資源。
- 行政任務（限教職員），包括協作工具及文件共享。
- 在非教學時間內進行有限度的個人使用，但前提是不得干擾學校活動或違反本政策。

所有使用行為均須符合學校的使命與價值觀，且使用者必須尊重他人的權利（例如：不得進行騷擾、霸凌或侵犯智慧財產權）。

禁止活動

當個人自備裝置（BYOD）連線至學校網路時，嚴禁進行以下行為：

- 存取、下載或散佈非法、有害或不當的內容（例如：色情內容、仇恨言論、未經許可的版權材料）。
- 安裝或執行未經授權的軟體，包括惡意軟件、病毒或來自不可信來源的應用程式。僅允許使用來自官方商店（例如 Apple App Store、Google Play）或學校核准清單中的應用程式。
- 分享學校憑證（例如：使用者名稱、密碼）或使用共享／群組帳戶進行 BYOD 存取。
- 對裝置進行越獄/取得 root 權限，或利用作業系統漏洞。
- 透過不可信或已遭入侵的裝置（例如未安裝最新安全修補程式）連線至學校網路。
- 將自帶設備（BYOD）用於商業活動、遊戲，或會消耗過多帶寬的串流媒體。
- 規避學校安全措施，例如使用 VPN 繞過防火牆或存取受限網站。
- 未經同意擅自錄製、拍攝或錄影學生、教職員或學校設施。

裝置的安全要求

欲連線至學校網路，自帶裝置（BYOD）必須符合以下最低安全標準。學校可在可行情況下使用流動裝置管理（MDM）工具來確保合規：

- **裝置配置：**
    - 啟用強效鎖定畫面：密碼/PIN 碼長度至少 8 個字符，且須包含混合字符（字母、數字、符號）；閒置 5 分鐘後自動鎖定。
    - 安裝並保持最新版本的抗惡意程式軟件，並啟用即時掃描功能。
    - 啟用全裝置加密（例如 macOS 上的 FileVault、Windows 上的 BitLocker，以及 iOS/Android 上的內建加密功能）。
    - 確保作業系統及所有應用程式皆已安裝最新的安全性修補程式。
    - 停用密碼自動儲存功能，且勿在裝置上儲存學校的登入憑證。

- **網路存取：**
    - 僅透過學校的安全 Wi-Fi 連線（需具備驗證功能的 WPA2/WPA3-Enterprise）。訪客網路為隔離網路，無法存取內部資源。
    - 存取任何敏感的內部系統時，請使用學校提供的 VPN；禁止使用個人 VPN。
    - 處理學校數據時，請避免連接公共 Wi-Fi；如有必要，請使用加密的行動數據。
- **核准與清點：**
    - 裝置必須向 IT 部門註冊（例如透過 MDM 註冊）並經核准後，方可獲准存取內部網路。
    - 學校將維護已連線自帶裝置（BYOD）的清單，其中包含使用者詳細資料及已安裝的應用程式。
- **數據處理：**
    - 盡量減少在個人裝置上儲存敏感的學校數據（例如學生紀錄）；請使用學校提供的加密雲端儲存服務。
    - 透過 MDM 啟用遠端清除功能，以因應裝置遺失或遭竊的情況。
    - 使用加密工具備份數據；在處置或重複使用裝置前，請清除所有學校數據。

使用者有責任確保裝置的實體安全（例如：勿將裝置置於無人看管之處），並在裝置遺失或遭竊時立即向資訊科技主管通報。

使用者責任

- **監控同意：**使用者確認學校可能基於安全目的（例如偵測未經授權的存取或惡意軟件）監控網路流量、裝置日誌及活動。
- **公共使用：**在校外使用自帶設備（例如做作業）時，請避免在未建立安全連線的情況下處理敏感資料；使用藍牙/NFC 時請謹慎，以防止資料遭竊聽。

網路保護措施

學校實施以下措施以保障網路安全：

- 防火牆、網絡入侵偵測系統（IDS）及區域隔離，以將自帶裝置（BYOD）的流量與關鍵系統隔離。

- 定期稽核非法存取點並執行漏洞掃描。
- 記錄所有存取嘗試。
- 實施帶寬管理以防止濫用。

將自帶設備（BYOD）的流量進行隔離（例如劃分為訪客／教職員／學生網域），並透過過濾機制阻擋惡意網站。

監控、執行與後果

- 資訊科技部門將透過日誌、掃描及隨機稽核來顯示器合規狀況。異常活動（例如偵測到惡意軟件）可能會觸發調查。
- 違規行為將依循漸進式處置：
    - 首次違規：警告及強制重新培訓。
    - 重複或嚴重違規（例如：數據外洩）：暫時或永久撤銷網路存取權限；紀律處分（例如：學生停學、職員解僱）。
    - 涉及法律違規：將依規定向主管機關通報。
- 可於 7 天內向校長提出申訴。

確認聲明

使用者將自備裝置（BYOD）連接至學校網路，即表示同意遵守本《網路使用規範》（AUP）。未滿 18 歲之學生須由家長／監護人共同簽署。確認方式可透過簽署表格、電子郵件確認或 MDM 註冊完成。

聯絡方式：如有疑問，請聯絡資訊科技主管 [電子郵件/電話]。本政策將依照教育局指引，每年或視需要進行檢討。

《網路管理與無線安全實用指南》

版本 1.0

本文件旨在作為實用指南，僅供參考。學校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及需求。作者對任何基於本指南所採取的行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 前言 5
2. 網路安全管理 6
2.1. 維護網路清單 6
2.2. 內部網路設計 6
2.3. 網路存取控制 6
3. 網路技術控制措施 7
3.1. 存取控制 7
3.2. 網頁過濾 7
3.3. 監控工具 7
4. 強化伺服器與網路設備 8
4.1. 強化管理員連線安全性 8
4.2. 服務與應用程式的安全性 8
5. 無線網路 8
5.1. 無線網路驗證 9
5.2. 無線網路協定 9
5.3. 無線網路隔離 9
6. 驗證 10
6.1. 埠掃描 10
6.2. 漏洞掃描 10
7. 檢視與改善 11
7.1. 定期政策檢討 11
7.2. 因應新威脅與技術 11
7.3. 持續改進 11
附錄 12
術語表 12

1. 前言

1.1. 目的與範圍

本指南為全港學校提供數據標籤的實用建議及基準標準。其目的是協助教育機構在保護其網絡方面維持一致的基準，並為學校提供一種安全的無線網絡安全實施方式。

本指南的範圍涵蓋網路技術管控、強化伺服器與網路設備，以及無線網路防護措施。其設計旨在適應不同規模的學校、系統類型及可用資源。這些指引源自多個經認可的來源，包括香港教育局（EDB）以及互聯網安全中心（CIS），兩者均提供了作為本指南基礎的指導方針與資源。

1.2. 目標讀者（資訊科技管理員及技術人員）

本指南適用於資訊科技管理員、技術人員，以及任何負責管理學校環境中用戶帳戶或資訊科技系統的人員。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，資訊科技團隊將能更有效地：

- 在伺服器及網路設備上實施強化防護措施
- 實施強效通訊協定（如 WPA3）、嚴謹的驗證方法及嚴格的網路隔離
- 透過埠口掃描與漏洞掃描定期驗證，以識別並修復弱點
- 透過年度檢討及因應新威脅的調整，持續迭代並改進這些流程

我們鼓勵各校根據自身技術環境與營運需求，適配這些建議。

2. 網路安全管理

本節闡述學校在設計與維護安全網路架構時應參考的核心要素。

2.1. 維護網路清單

- 對於所有連接內部網路的網路設備和終端點，應記錄其 IP 位址（如適用）和配置。
- 應維護網路圖，並在內部網路新增設備或淘汰舊設備時進行更新。

實務範例：

- 使用試算表或數據庫表格進行資產清單追蹤。使用數據庫可與現有的資產管理清單進行整合。

2.2. 內部網路設計

- **不可路由 IP：**為內部系統設計網路時，應採用私有 IP 位址，並指派不可路由的 IP 範圍（例如 192.168.x.x），以防止外部存取。
- **網路分段：**使用子網作為資源與機器的高階分組，以便進行存取控制。預設情況下禁止跨子網通訊。
- **DMZ：**若需對內部資源（例如網頁伺服器）開放公眾存取，應將該資源置於非軍事區（DMZ）內。

實務範例：

- 使用 192.168.0.0 IP 範圍，並設定通訊閘，以建立 3 個虛擬子網，分別供外部裝置、內部裝置及檔案伺服器使用。
- 或者，可選用另一家互聯網服務供應商為外部裝置提供互聯網連通性，藉此將外部裝置與內部網路進行物理隔離。

2.3. 網路存取控制

規劃終端點與資源的存取需求。考慮採用基於群組的存取管理，這意味著該規劃應列出所有群組及其存取權限，以及每個群組中的所有成員。

群組的範例包括：

- 機器群組（例如：教職員室電腦、教室電腦等）
- 連接至特定存取點群組的裝置

- 內部資源群組（例如：所有備份伺服器）

為配合營運需求，請制定申請、授予及撤銷存取權限的政策。

適應性建議：

- 預設將所有行動裝置視為外部裝置。
- 請注意，在某些情況下，邏輯網路存取控制可能會被繞過。若要徹底拒絕對內部資源的存取，請考慮實施實體網路隔離。儘管如此，邏輯網路存取控制對於網路安全仍至關重要。

3. 網路技術控制措施

本節列出可在設計完善的網路中實施管控的技術措施。請將以下建議作為貴校的參考依據。

3.1. 存取控制

- **存取控制清單 (ACL)：**在防火牆和路由器上設定 ACL，透過定義僅允許必要埠號與通訊協定的規則來限制流量（例如：阻擋除核准服務以外的所有傳入流量）。遭拒絕的存取嘗試可轉送至入侵偵測系統進行審查。

實務建議：

- 若配合適當的網路分區措施，學校可基於子網實施白名單機制。
- 我們強烈建議採用白名單策略，並預設將所有流量列為明確拒絕。

3.2. 網頁過濾

- **網頁代理伺服器：**可利用網頁代理伺服器封鎖惡意 IP、網路釣魚網站及非教育性內容。部分代理伺服器能對 TLS 連線進行中間人攻擊並讀取網頁內容。被拒絕的存取嘗試可轉送至記錄系統。
- **DNS 代理：**DNS 代理無法讀取網頁內容，但可透過阻擋 DNS 查詢來阻止存取惡意網頁。

3.3. 監控工具

在關鍵瓶頸點（如通訊閘）後方或 DMZ 內部部署入侵偵測系統 (IDS)，並針對可疑活動建立警示系統（例如電子郵件、簡訊）。

實務範例：

- 將一台電腦重新配置，安裝輕量級作業系統，然後部署如 Wazuh 般的開源 IDS 工具。在通訊閘上建立網路 Tap 或鏡像埠，使流量被鏡像至 IDS。
- 調整偵測簽名與模式，以將誤報降至最低。分析初始日誌以識別常見的誤報；接著調整閾值或排除特定的流量模式。

4. 強化伺服器與網路設備

許多應用程式和網路設備為確保相容性，預設配置存在安全漏洞。學校應注意以下事項，並撤銷其設備和應用程式上的不安全配置。

4.1. 強化管理員連線安全性

- **加密連線：**許多網路設備（如路由器和防火牆）的管理會話預設使用未加密的 HTTP 連線。請改用 HTTPS。
- **憑證管理：**許多網路設備使用自簽名憑證。請將此憑證匯出，並安裝至用於存取管理界面的設備之信任儲存庫中，如此一來，在正常情況下將不會出現 TLS 錯誤，但若攻擊者試圖偽造管理會話，則會觸發憑證錯誤。
- **IP 白名單：**透過限制可存取管理界面的 IP 位址，來限制對管理界面的存取權限。應透過 DHCP 預留及／或為用於存取管理界面的裝置設定靜態 IP 來實現此措施。
- **安全密碼：**變更預設密碼，並嚴格遵循《安全配置檢查清單》中的管理員密碼政策。

4.2. 服務與應用程式的安全性

- **服務管理：**停用伺服器上所有未使用之服務。訂閱修補程式通知以及時套用修補程式。
- **應用程式強化：**遵循廠商或第三方（例如 CIS）的強化指南（例如停用預設功能），強化應用程式配置並安裝安全性修補程式。應用程式流量應使用加密通訊協定。
- **管理員存取權限：**在 SSH 連線中啟用憑證驗證。停用密碼登入。

5. 無線網路

眾所周知，無線網路的安全性較有線網路為弱。一般而言，所有連線至具有相同 SSID 之存取點的裝置，在網路存取控制模型中應被視為一個獨立的群組。

5.1. 無線網路驗證

請將存取點視為一個集線器，只要使用者能通過存取點的驗證，即可將纜線插入其中。因此，存取點的驗證方法必須具備高度安全性。

對於用於向公眾提供互聯網存取的存取點，請使用符合密碼政策的強密碼。

對於用於提供內部資源存取的存取點，請實施以下其中一種方式：

- 使用客戶端憑證進行真確性驗證。
- 停用 DHCP，並採用 MAC 位址與 IP 位址白名單機制。
- 使用具備加密級熵值的長密碼（例如：25 個隨機的英數字數字與符號），並制定政策禁止共用密碼。

否則，請使用 VPN 進行內部存取。

5.2. 無線網路協定

使用支援 WPA2/WPA3 協定的存取點。在存取點中停用 WPA/WEP 協定。

實用建議：

- WPA2 的安全性極度取決於密碼的強度。新款存取點雖支援 WPA3，但為維持反向兼容性，通常仍同時支援 WPA2，這可能導致依實作方式而異的下行攻擊。請使用強密碼。

5.3. 無線網路隔離

請透過邏輯或物理方式將無線網路與內部網路隔離。物理隔離通常更為安全，建議用於無需提供內部網路存取權限的無線存取點。

若不希望為實體隔離而建置另一套網路基礎架構（例如：用於內容過濾的另一台 DNS 代理伺服器），請採用邏輯存取控制，並透過通訊閘或防火牆實施嚴格的存取控制。

實務範例：

- 請透過另一套互聯網方案提供互聯網存取，最好選用不同的互聯網服務供應商，以確保公共互聯網存取與內部網路完全隔離。
- 為教師與行政人員設置不同的存取點，因為他們對內部資源的存取需求不同。

6. 驗證

本節概述驗證網路安全性的措施，應定期執行（例如每年一次）。

6.1. 埠掃描

使用埠掃描工具來驗證存取控制的實施情況。在不同的子網中執行埠掃描，並將報告與存取控制圖進行交叉比對（參見第 2.3 節）。

如有任何不一致之處，請檢視防火牆規則。

實務範例：

- 使用 nmap 掃描開放埠。使用 -p 0-65535 參數掃描所有開放埠。
- 預期僅會看到防火牆規則中允許的埠號。

6.2. 漏洞掃描

使用漏洞掃描工具，找出運行中服務因缺少修補程式所導致的任何漏洞。檢視報告，若漏洞適用於伺服器/網路設定，請套用相關修補程式。

實務建議：

- 將掃描器置於具備完整網路存取權限的子網中。防火牆會因掃描範圍受限而影響掃描準確性。

7. 檢視與改善

7.1. 定期政策檢討

設定提醒，至少每年一次，或在資訊科技系統有所變更時，檢視貴校的資料處理與標籤標準。邀請資訊科技人員及教學／行政同仁共同參與，以蒐集有用的回饋意見。

7.2. 因應新威脅與技術

隨時掌握可能影響學校的新型網路威脅，例如網路釣魚詐騙或密碼外洩。同時，也應留意可能提供更佳密碼保護方式的新技術或軟體更新，例如雙因素驗證。

7.3. 持續改進

每次檢討後，請視需要更新密碼政策。將任何變更清楚地告知教職員與學生，並提供簡易的操作指引或舉辦工作坊，協助所有人遵循新規則。

附錄

術語表

術語	定義
存取控制清單 (ACL)	一套適用於防火牆和路由器等網路設備的規則集，根據 IP 位址、連接埠和通訊協定等因素，指定允許或拒絕哪些流量。
應用程式強化	透過套用安全性修補程式、停用不必要的預設功能，並遵循供應商的安全性建議（例如 CIS 指南），來強化應用程式安全性的過程。
DHCP 預留	一種網路配置，指示 DHCP 伺服器根據特定裝置的 MAC 位址，始終為該裝置指派相同的特定 IP 位址。
DMZ（非軍事區）	位於內部網路與公共互聯網之間、獨立且隔離的網路區段，用於主機如網頁伺服器等對外公開的服務，以保護內部網路。
DNS 代理	一種透過攔截 DNS 查詢，並在建立連線前阻擋對惡意或受限網域的請求，從而過濾網頁存取的工具。
降級攻擊	一種攻擊手法，黑客迫使系統放棄安全的連線（如 WPA3），轉而採用較舊且安全性較低（如 WPA2）的連線方式，以便更容易進行攻擊。
系統強化	透過縮小系統的攻擊面來強化系統安全性的過程，通常包括停用不必要的服務、變更預設密碼，以及套用安全的配置。
網絡入侵偵測系統 (IDS)	一種監控網路流量以偵測可疑活動或政策違規的系統，並在偵測到潛在威脅時發出警報。
IP 白名單	一種安全措施，將對系統或界面的存取權限限制在預先核准的 IP 位址清單內。
邏輯網路分割	利用虛擬區域網路（VLAN）和防火牆規則等軟體控制措施，將網路劃分為較小且相互隔離的區段（子網）的做法。
MAC 與 IP 白名單	一種無線認證方法，僅允許具備預先核准 MAC 位址及對應靜態 IP 位址的裝置進行連線。
網路存取控制	定義哪些使用者、裝置或群組可存取特定網路資源的政策與技術規則。
網路拓撲圖	學校網路的視覺化呈現，顯示裝置之間的互連方式及其位置。
網路清單	所有網路裝置與終端設備的完整記錄，包含其 IP 位址、配置，以及實體／邏輯佈局。
網路分段	將網路劃分為較小且相互隔離的區段（子網）的作法，用以控制流量並限制潛在安全威脅的擴散。
網路監聽埠 / 鏡像埠	一種應用於網路交換機的方法，用於將一個或多個埠的網路流量複製到指定的監控埠，使入侵偵測系統（IDS）能在不介入流量路徑的情況下進行流量分析。
不可路由 IP 位址	專門保留供內部網路使用的 IP 位址（例如 192.168.x.x 範圍），這些位址無法直接從公共互聯網存取。
物理網路隔離	透過物理上分離的硬件（例如不同的交換機、路由器，甚至不同的互聯網服務供應商）來隔離網路，以防止任何直接通訊。
埠掃描	探測伺服器或主機上開放的網路埠，用以識別正在運行的服務，並驗證防火牆規則是否按預期運作。

術語	定義
自簽名憑證	一種未經受信任的核證機關簽署，而是由其創建者（例如網路裝置本身）自行簽署的 SSL/TLS 憑證。
SSID（服務集識別碼）	使用者在搜尋 Wi-Fi 連線時所看到的無線網路公開名稱。
子網	較大網路的邏輯子網，可實現更高效的流量管理並應用細粒度的安全政策。
漏洞掃描	一種自動化的掃描流程，用於檢查系統、網路及應用系統，以識別已知的安全漏洞，例如缺少修補程式或不安全的配置。
網頁代理伺服器	作為 Web 請求中介的伺服器，讓學校能過濾內容、封鎖惡意網站並顯示流量。
白名單策略	一種安全策略，預設會阻擋所有網路流量，僅明確允許特定核准的流量通過。
WPA2 / WPA3	適用於無線網路的現代化安全協定，提供強大的加密與驗證功能。WPA3 是最新且最安全的標準。

實用物理與環境安全指南

版本 1.0

本文件旨在作為實用指南，僅供參考。學校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及要求。作者對基於本指南所採取的任何行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 前言 5
2. 場地準備 6
    2.1. 校園分區與資源分配 6
    2.2. 災害防範 6
    2.3. 存取控制系統 7
    2.4. 環境控制 8
    2.5. 監控系統部署 8
3. 資產安全與維護 8
    3.1. 資產實體管控 8
    3.2. 人員管控 9
4. 檢討與改進 10
    4.1. 定期政策檢討 10
    4.2. 因應新威脅與新技術 10
    4.3. 進行改進 10
附錄 11
    術語表 11

1. 前言

1.1. 目的與範圍

本指南為全港學校的實體及環境安全維護提供實用建議與基本標準。其目的是協助教育機構維持一致的基準，以確保校園安全，並保護校園環境免受實體及環境威脅。

本指南的範圍涵蓋環境隔離措施，以及在學校環境的不同位置提供安全措施與資源。其設計旨在適應不同規模的學校、各類教育體系及可用資源。這些指引源自多個經認證的來源，包括香港教育局（EDB）以及互聯網安全中心，兩者均提供了作為本指南基礎的指導方針與資源。

1.2. 目標讀者（IT 管理員與技術人員）

本指南旨在供 IT 管理員、技術人員，以及任何負責管理學校環境中使用者帳戶或資訊系統的人員參考。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，IT 團隊將能更有效地：

- 將校園區域劃分為公共、受保護及限制區域，並加強安全防護
- 透過專用防護系統的安裝指引，降低火災、水患、颱風等環境災害的風險
- 選用合適的存取控制系統，並落實實體與環境管控措施
- 實施實體管控措施以保護及維護資產，建立主動式系統，協助建立多層次防禦機制以應對實體與環境風險

鼓勵各校根據自身技術環境與營運需求，靈活適配這些建議。

2. 場地準備

本節闡述為防範實體與環境安全威脅而進行校園場地準備的核心要素。若本指南適用於現有校舍，請確認是否已處理以下事項。

2.1. 校園分區與資源分配

將校園劃分為公共、受保護及限制區域。範例：

- **公共區域：**走廊、餐廳等
- **受保護區域：**教室、圖書館等
- **限制區域：**伺服器室、教職員休息室等

將分類整理成清單，並為每個受保護區域及限制區域分配足夠的資源以確保安全。

實務建議：

- 用於保障各區域安全的資源可包含人力配置（例如：監督）、即時監控（例如：閉路電視系統）、存取控制系統（例如：鎖與鑰匙、通行證）以及其他適當的措施與政策。

實務範例：

- 為確保伺服器機房的安全，某所學校決定透過政策實施人員監督，並安裝閉路電視系統及感應卡進出系統。

2.2. 災害防範

應針對火災、水患及颱風風險實施防護措施，特別是在伺服器機房等管制區域。

防火措施：

- 安裝如 VESDA（雷射煙霧偵測系統）及熱感應器等偵測系統，以便在火災發生前偵測到煙霧或溫度異常。
- 依照常規防火規範，定期測試偵測與警報系統。
- 採用氣體滅火系統或滅火器，而非水，以避免損壞 IT 設備。

防洪措施：

- 定期檢查屋頂、平台、平屋頂、地下室及排水系統，確保排水管與檢修井無阻塞。

- 將伺服器機房設置於洪水淹沒區之上，並將設備架高以防潛在的水流侵入。

防颱措施：

- 在伺服器機房門上加裝防風條，或在伺服器機房前方增設隔間。
- 請勿在伺服器機房增設窗戶，以防因窗戶滲漏或破損導致雨水滲入。

停電防範措施：

- 為伺服器安裝專用電路，以避免因其他電器故障導致斷路器跳閘而中斷供電。
- 為伺服器安裝不斷電系統（UPS），以便在停電時有足夠時間進行有序關機。

適應性建議：

- 某些 UPS 可在電源中斷時，透過網路界面傳送訊號以關閉伺服器。在此情況下，請特別注意遠端關機服務的配置。應使用物理隔離的網路，並在伺服器端將關機訊號加入 IP 白名單。

2.3. 存取控制系統

以下列出學校在選用常見存取控制系統時應特別注意的事項。

門扇：

- 應選用配備安全鉸鏈的門，當鉸鏈被拆下時，門會自動鎖定。
- 選用配備死鎖機構的門，並搭配門上隨附的門閂板使用。切勿使用門閂孔徑過大、無法與門閂吻合的門閂板。
- 檢查門框與門體是否密合，並加裝防風條，以增加攻擊者利用工具撬動的難度。

傳統鎖具：

- 選用具備防撬功能的鎖具，例如安全銷、防撬桿及限制型鑰槽。
- 將鑰匙收好，避免被他人透過照片複製鑰匙。
- 檢查鑰匙上是否有任何鐫刻或印製的數字。若鑰匙上的數字長度較短（例如 4 位數），該鑰匙的熵值可能不足，且可能被重複用於同一鎖款的其他批次中。

RFID 門禁系統：

- 應採用具備安全通訊協定、不易遭受未經授權讀取與仿真攻擊的 RFID 系統。過時的實作方案（如 Mifare Classic）往往容易遭受此類攻擊。目前 Mifare Desfire 除 UID 之外，普遍被認為是安全的。

生物特徵鎖：

- 生物特徵鎖容易遭受偽造攻擊。應選用具備活體偵測機制（如脈搏與熱感應）的生物特徵鎖，或採用多模態鎖具（例如結合生物特徵與 PIN 碼）。

PIN 碼鎖：

- 長期使用相同的 PIN 碼可能會形成磨損痕跡，從而暴露 PIN 碼組合。請定期輪替包含不同數字的 PIN 碼。

磁力鎖／電動門釋放機構：

- 門鎖釋放裝置應採用有線按鈕。此類線纜應從門鎖釋放按鈕直接連接至門體本身。門鎖釋放裝置不應涉及任何無線通訊。
- 請勿在公共區域將按鈕至門體的線纜外露。
- 請注意，這些裝置需持續供電才能保持上鎖狀態。請檢查電池壽命，以確認斷電時門能維持上鎖狀態的時間長度。

2.4. 環境控制

- 請在 IT 區域維持最佳環境條件，例如溫度介於 20-25°C 之間，濕度為 50-80%，以防止硬件過早故障。
- 為環境控制系統的冷卻電源增加冗餘設計，確保伺服器在維護期間仍能不中斷地運行。
- 制定維護時程表，確保定期進行維護，同時確保總製冷能力足以應付伺服器的散熱需求。

2.5. 監控系統部署

- 選擇能在可見光不足時，同時具備可見光與紅外線錄影功能的攝影機。
- 部署前，請先根據校園平面圖規劃攝像頭的設置位置及監控死角。確保所有重要區域均已納入監控範圍。
- 若條件允許，應將監控網路與內部網路及互聯網進行物理隔離。

3. 資產安全與維護

本節列出可用於實體保護資產的技術管控措施。請將以下建議作為貴校的參考依據。

3.1. 資產實體管控

- 針對位於公共區域的資產，部署資產鎖（例如 Kensington 鎖），以防止遭竊。確認鎖具已牢固地固定於某個永久性結構上，且未解鎖時無法移除。
- 在可接觸區域的網路線路上部署線纜鎖，以防止未經授權的網路存取或竊聽。

- 將存取點等資產放置於物理上難以觸及的位置，例如天花板或上鎖的機櫃內。

3.2. 人員管控

- 使用授權人員清單，並為員工、訪客及承包商配發不同顏色編碼的證件。
- 制定政策，要求員工若在受保護區域發現任何可疑人員，應立即向保安人員通報。

實務建議：

- 在授權人員名單中明確標示承包商可進入的區域，以便安保人員透過監控系統進行監控。

實務範例：

- 訪客使用紅色徽章，承包商使用黃色徽章。要求員工向保安部門通報任何未佩戴徽章或佩戴紅色徽章的人員。

4. 檢討與改進

4.1. 定期政策檢討

設定提醒，至少每年一次，或在資訊科技系統有所變更時，檢視貴校的資料處理與標籤標準。邀請資訊科技人員及教學／行政同仁共同參與，以蒐集有用的回饋意見。

4.2. 因應新威脅與新技術

隨時掌握可能影響學校的新型網路威脅，例如網路釣魚詐騙或密碼外洩。同時，留意可能提供更佳密碼保護方式的新技術或軟體更新，例如雙因素驗證。

4.3. 進行改進

每次檢討後，請視需要更新密碼政策。將任何變更清楚地告知教職員與學生，並提供簡易的操作指引或舉辦工作坊，協助所有人遵循新規則。

附錄

術語表

術語	定義
存取控制系統	用於管理及限制進入實體區域的硬件（鎖具、感應卡讀卡機）與政策之集合。
資產鎖	如 Kensington 鎖等實體安全裝置，透過纜繩將設備（例如筆記型電腦、顯示器）固定於固定物體上，以防止竊盜。
授權人員名單	一份正式記錄，列出獲准進入特定受控區域的個人（員工、訪客、承包商），通常與通行證配合使用。
生物特徵鎖	一種利用獨特生物特徵（如指紋或面部特徵）進行身份驗證的鎖具。
纜線鎖	用於將網路線纜固定於裝置或連接埠上的實體鎖具，以防止未經授權的斷線或網路竊聽。
校園分區	根據敏感度及進出要求，將學校的實體場地劃分為不同區域（公共區、受保護區、限制區）的做法。
防反鎖裝置	一種鎖具機制，可防止門閂被工具（如信用卡）推回，從而增強對簡單繞過技術的防禦能力。
專用電路	專門為單一電器或特定設備組（例如伺服器）供電的電路，使其與其他電路的故障隔離。
環境控制	用於在裝有敏感 IT 設備的區域維持最佳環境條件（例如溫度、濕度、空氣品質）的系統與程序，以防止硬件故障。
氣體滅火系統	一種不使用水，而是利用化學劑或惰性氣體來撲滅火勢的滅火系統，藉此保護電子設備免受損壞。
人員管控	依賴人員與政策的安全措施，例如使用顏色編碼的證件進行身分識別，以及培訓員工通報可疑人員。
紅外線（錄影）	一種攝影機功能，透過偵測熱能訊號，可在低光或無光環境下進行錄影。
活體檢測	生物特徵系統中的一項安全功能，透過驗證活體存在（例如偵測脈搏或熱能），以防止使用假指紋或照片進行冒充。
磁力鎖	一種利用強磁場來確保門鎖安全的電磁鎖，需持續供電才能保持上鎖狀態。
Mifare Classic / Desfire	RFID 通訊協定類型。Mifare Classic 為較舊且安全性較低的標準，而 Mifare Desfire 則是現代且安全性更高的通訊協定，建議用於存取控制系統。
PIN 鎖	一種需輸入數字個人識別碼（PIN）方可進入的存取控制鎖。
受保護區域	學校內指定區域，例如教室或圖書館，僅限學生及教職員等授權群體進入。
公共區域	學校內的區域，例如走廊或餐廳，通常對所有學生、教職員及訪客開放，無需特別的存取控制。
限制區域	高度安全的區域，例如伺服器機房或校長室，僅限少數經特別授權的人員進入。
限制性鑰槽	鎖具的一項功能，採用獨特的鑰匙設計，防止一般鎖匠擅自複製鑰匙。

術語	定義
RFID 感應卡系統	一種存取控制系統，利用內含無線射頻識別（RFID）晶片的卡片或鑰匙圈，在對準讀卡機時授予進入權限。
安全鉸鏈	門鉸鏈設計有安全銷釘，可與門框進行聯鎖，即使鉸鏈銷釘被拔出，也能防止門被拆下。
防盜銷釘	鎖芯內部的特殊銷釘，透過卡住或阻擋開鎖工具，使撬鎖行為更加困難。
監控盲區	監控系統視野字段內，任何攝影機均無法捕捉的區域，形成盲點。
UPS（不斷電系統）	一種電池備份設備，可在停電期間為連接的設備提供緊急電源，使其能安全且有序地關機。
VESDA（超早期煙霧偵測裝置）	一種採用雷射技術的高度敏感煙霧偵測系統，能識別微小的煙霧微粒，在火災完全發展前提供早期預警。
氣密條	一種用於密封門窗周圍縫隙的材料，以防止水、風和灰塵等外界因素侵入。

監控與記錄實用指南

版本 1.0

本文件旨在作為實用指南，僅供參考。各校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及需求。作者對基於本指南所採取的任何行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 前言 5
2. 建立日誌記錄標準 6
2.1. 記錄範圍 6
2.2. 日誌的集中式儲存 6
2.3. 日誌傳輸 6
2.4. 日誌分類與保留 7
3. 日誌記錄的實施 8
3.1. 作業系統 8
4. 監控系統的建置 10
4.1. 建立監控指標 10
4.2. 建立正常行為基準 10
4.3. 配置警示 11
4.4. 需審查的觸發條件 11
4.5. 監控工具 12
5. 檢討與改進 13
5.1. 定期政策檢討 13
5.2. 因應新威脅與技術 13
5.3. 進行改進 13
附錄 14
術語表 14

1. 前言

1.1. 目的與範圍

本指南為全港學校提供數據標記的實用建議及基準標準，旨在協助教育機構建立結構化的日誌記錄與監控標準，以強化其網絡安全紀錄與實務。本指南以「集中且安全的日誌儲存」為核心原則，並介紹了一套分級日誌政策及其實際實施步驟。

本指南的範圍涵蓋實施一套有效的監控系統，將收集到的日誌轉化為可執行的情報。此目標可透過建立典型運作期間的正常網路及系統行為基準來達成。本指南的設計旨在適應不同規模的學校、系統類型及可用資源。 本指南的指引內容源自多個經認可的來源，包括香港教育局（EDB）以及互聯網安全中心（CIS），兩者均提供了用於編製本指南的指導方針與資源。

1.2. 目標讀者（IT 管理員與技術人員）

本指南適用於資訊科技管理員、技術人員，以及任何負責管理學校環境中用戶帳戶或資訊科技系統的人員。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，資訊科技團隊將能更有效地：

- 參考 ISO 27002 標準，涵蓋關鍵事件，例如存取嘗試、權限使用及配置變更。
- 根據作業系統實施並適配分層日誌保留政策及實作方法，並針對 Windows、macOS 和 Linux 提供具體配置。對於缺乏原生記錄功能的軟體，亦提供額外步驟。
- 利用資源使用狀況與登入時間，建立基準運作示意圖，藉此制定追蹤不同 IT 系統典型運行時間的時程表。

鼓勵各校根據自身技術環境與營運需求，適配這些建議。

2. 建立日誌記錄標準

本節詳述建立結構化記錄標準的指引，以確保記錄實施的完整性。各校應參考並根據自身情境進行調整。

2.1. 記錄範圍

ISO 27002 標準定義了 10 種需記錄的關鍵活動類型，以確保問責制，學校應參考這些類型來決定應記錄哪些內容。

- **系統存取嘗試：**成功與失敗的系統存取嘗試，包括登入與登出。
- **權限使用：**使用提升權限或管理員權限執行的操作（例如修改使用者權限）。
- **系統配置變更：**對系統配置的修改，例如防火牆規則或軟體配置的變更。
- **應用程式進程啟動與停止：**應用程式或服務的啟動或終止。
- **系統故障與錯誤：**可能暗示安全問題的系統異常運作、當機或誤差信息。
- **資訊保安事件：**與安全相關的事件，例如惡意軟件偵測或未經授權的存取嘗試。
- **保護系統的啟用與停用：**啟用或停用安全工具，例如防毒軟體、防火牆或入侵偵測系統。
- **資訊存取：**與敏感數據的互動，包括讀取、修改或複製檔案。
- **資訊刪除：**移除或刪除檔案或數據，尤其是被歸類為敏感的項目。
- **使用者存取權限變更：**修改使用者權限或存取層級，例如授予或撤銷存取權限。

實作建議：

- 預設的記錄行為通常不足以記錄上述所有事件。請參閱後續章節的實作範例。
- 若具備技術能力與資源，學校可考慮新增更多事件記錄，例如自訂異常偵測。

2.2. 日誌的集中式儲存

儲存在本地主機內的日誌，在發生本地權限提升後容易遭到破壞。因此，日誌應儲存於集中式儲存系統中，並將日誌匯出至具備適當存取控制的集中式伺服器。

建立日誌集中儲存機制，對於有效監控事件及偵測異常狀況亦至關重要。

2.3. 日誌傳輸

日誌應透過安全加密通道進行傳輸，以避免遭竊聽。

2.4. 日誌分類與保留

《香港政府資訊科技保安指引》（G3）**附錄 C** 根據機密性、完整性及可用性（CIA）原則，為資訊系統定義了三級分類：

- **第 1 級（低影響）**：公開或非敏感數據（例如學校網站內容）。若發生遺失或外洩，影響極輕微。
- **第 2 級（中等影響）**：敏感但非高度機密性之數據（例如：教職員電子郵件、學生出勤紀錄）。若數據外洩，可能造成中度干擾或隱私疑慮。
- **第 3 級（高／關鍵影響）**：高度機密性或關鍵數據（例如：學生個人資料、考試成績、財務紀錄）。若數據外洩，可能導致重大的法律、聲譽或營運損害。

日誌依據其所屬的系統或數據進行分類，保存期限則與等級掛鉤（例如：第 1 級為 6 個月，第 2/3 級為 12 個月）。

實作建議：

- 系統的分類應在資產採購階段即完成，並記錄於資產清單中。

3. 日誌記錄的實施

為確保操作記錄具備足夠細節，學校必須將系統與應用系統的配置調整至超出預設值。本節列出學校可參考的關鍵 IT 元件配置步驟，涵蓋記錄與匯出日誌的整體流程。

注意：所有裝置的時鐘應保持同步。這通常透過 NTP 伺服器來實現。

3.1. 作業系統

Windows

在「群組原則」中啟用進階稽核（例如：電腦設定 > 原則 > Windows 設定 > 安全性設定 > 進階稽核配置）。啟用以下類別：

- 登入/登出（用於系統存取嘗試）。
- 權限使用（用於管理操作）。
- 物件存取（針對檔案存取/刪除）。
- 系統（用於配置變更與故障）。

設定事件記錄轉發至集中式伺服器以進行彙整。

Linux

修改 /etc/rsyslog.conf 或 /etc/syslog-ng.conf，以包含有關驗證 (auth.*)、系統變更 (cron.*) 及安全事件的詳細記錄。使用 auditd 進行詳細審計追蹤（例如，使用 auditctl -w /path/to/grading_files -p wa 來監控寫入/存取）。

編輯設定檔中的規則，將日誌匯出至集中式伺服器或檔案伺服器。

macOS

透過 log config 指令啟用記錄功能（例如：sudo log config --形式 "level:debug"）。

編輯設定檔中的規則，將日誌匯出至集中式伺服器。

3.2. 網路裝置

設定路由器和防火牆（例如 pfSense、Cisco）以記錄流量（入站/出站）、存取嘗試以及配置變更。啟用將 syslog 輸出至中央伺服器（例如，透過 Cisco 裝置上的 logging host <SERVER_IP>）。

3.3. 應用程式

本地應用程式

各應用系統的配置方式不盡相同。學校應針對每項應用系統探索其日誌記錄功能。應用系統日誌通常會與系統日誌整合，若設定得當，系統日誌應已匯出至中央伺服器。

企業級應用程式通常具備強大且可自訂的記錄功能。例如，Google Workspace 的管理主控台會記錄使用者操作、檔案存取及配置變更，而 Microsoft 365 的稽核記錄則會擷取類似事件。學校可透過設定啟用這些功能，但可能需要調整預設值以獲得更細緻的記錄層級。

雲端應用程式

學校應深入了解雲端應用程式的記錄功能及其匯出功能。建議將記錄匯出至集中式記錄伺服器。

不具備原生記錄功能的應用程式

針對日誌記錄功能不足或完全缺乏日誌記錄的應用程式，學校可採取以下策略：

- **透過系統層級記錄進行補充：**配置作業系統稽核功能，監控應用程式儲存數據的目錄（例如學生紀錄）。
- **透過網路層級記錄進行補充：**將應用程式流量導向代理伺服器，以記錄 HTTP/HTTPS 請求。

4. 監控系統的建置

本節提供有效監控系統建置的高階概覽，供學校參考。

4.1. 建立監控指標

以下是可能預示資料外洩、惡意軟件或未經授權存取等威脅的要素。請根據學校的使用情境考慮監控這些項目。關鍵領域包括：

- **進出流量**：透過防火牆或通訊閘監控網路流量，以偵測異常模式，例如數據外洩至外部 IP，或來自已知惡意來源的掃描攻擊。
- **關鍵資源存取**：監控對敏感系統的登入行為，例如學生資訊系統或學習管理系統（如 Google Classroom 或 Canvas）。
- **配置檔**：密切關注系統配置的變更，例如防火牆規則或使用者權限，以防止遭篡改。範例：偵測 Linux 伺服器上 /etc/passwd 檔案或 Windows 登錄檔中未經授權的編輯行為，此類行為可能開啟後門。
- **安全工具日誌**：彙整來自防毒、反惡意軟件或端點偵測工具的警示。
- **資源使用狀況**：追蹤 CPU、記憶體、磁碟及帶寬使用情況，以偵測資源密集型活動。

實務範例：

- 監控 HTTP/HTTPS 流量中的上傳/下載突增現象，這可能表示勒索軟體正在加密並傳送學生檔案。
- 顯示登入失敗嘗試並標記 IP 位址。
- 根據 IP 位址顯示來自校區地理範圍外的存取行為。
- 監控對重要設定檔或登錄檔金鑰的編輯或修改嘗試。

4.2. 建立正常行為基準

在學校正常運作期間，收集 2 至 4 週的數據以定義基準線。隨後可在即時監控中將這些基準線進行比對，以偵測異常情況。

每個衡量指標都需要有基準值，這些基準值應隨時間形成模式。

請注意，由於學校內可能發生重大事件（例如考試期間），數據可能會出現劇烈波動，進而觸發誤報。因此，若發生此類事件，應適時檢視並調整基準值。

實務範例：

- 常規模式：團隊從日誌中觀察到每天上午 8 點登入量達到高峰，並判定這是因師生到校所產生的正常行為。此行為隨後被進行文件編製，並將此期間觸發警告的閾值設定得較高。
- 突發高峰：考試期間前夕，因需列印試卷，印表機使用量可能驟增。
- 低谷期：深夜時段的存取量會急遽下降，甚至降至零。

4.3. 配置警示

根據觀察到的模式和基準設定即時警示規則。整合可發送電子郵件、簡訊或推播通知的工具，或 Slack/Telegram/Discord 機器人。

調整建議：

- 警報規則清單可能冗長繁瑣，且需耗時調整，請參閱《待檢視觸發條件》。

實用範例：

- 在非工作時間，若實驗室電腦的 CPU 使用率持續高於基準值，即觸發警示。
- 當來自特殊國家（例如伊朗或北韓）的網路流量突然激增時觸發警示。
- 若觸發任何自動防護措施（例如因登入嘗試失敗而封鎖 IP 位址），請發出警示。

4.4. 需審查的觸發條件

- **誤報**：警報應觸發應變程序。任何事件應變程序均包含對潛在事件的驗證，以 確認警報的有效性。若警報屬誤報，應調查誤報原因，並調整閾值／基準模式以符合新的觀察結果。
- **閾值設定過高**：若閾值顯然設定在遠高於正常使用水準的範圍，應考慮調低閾值以符合實際使用情境。若預留了因應特定時間或事件所致流量激增的緩衝空間，則應考慮針對正常時段與繁忙時段實施不同的規則。

4.5. 監控工具

以下列出學校可考慮用於即時監控的工具清單（非詳盡列表）。

- 網絡**入侵偵測系統 (IDS)**／網絡**入侵防禦系統 (IPS)**：針對網路監控，Snort 是一款基於 Linux 的開源工具，可用於配置規則以監控傳入流量。可與 Barnyard2 整合以進行數據庫記錄，並搭配 Snorby 作為網頁界面來檢視警示。
- **主機端監控**：OSSEC 是一款免費監控工具，可安裝於 Windows/Linux 機器上，並配置為監控檔案完整性（例如，在學生數據庫檔案發生變更時發出警示）。此外，亦可針對目錄配置作業系統層級的日誌，並透過集中式日誌監控進行監控。
- **檔案完整性監控**：Tripwire（提供開源版本）會掃描關鍵目錄（例如網頁應用程式的 /var/www），並執行每日檢查。若配置檔案發生意外變更，系統將透過 syslog 發出通知，使用者可將其路由至您的警示系統。
- **帶寬與資源監控**：PRTG Network Monitor 提供最多 100 個感測器的免費版本。可安裝於 Windows 伺服器上，為實驗室電腦的 CPU 及路由器的帶寬新增感測器，並配置 SMS 通知。
- **集中式日誌監控：**Greylog 是一款開源記錄管理平台，能即時收集、索引及分析日誌。對於需要可擴展解決方案來監控網路流量、安全事件及資源使用情況的學校而言，此工具是理想選擇。

5. 檢討與改進

5.1. 定期政策檢討

設定提醒，至少每年一次，或在 IT 系統有所變更時，檢視貴校的數據處理與標籤標準。邀請 IT 人員以及教學／行政同仁共同參與，以蒐集有用的回饋意見。

5.2. 因應新威脅與技術

隨時掌握可能影響學校的新型網路威脅，例如網路釣魚詐騙或密碼外洩。同時，也應留意可能提供更佳密碼保護方式的新技術或軟體更新，例如雙因素驗證。

5.3. 進行改進

每次檢討後，請視需要更新密碼政策。將任何變更清楚地告知教職員與學生，並提供簡易的操作指引或舉辦工作坊，協助所有人遵循新規則。

附錄

術語表

術語	定義
進階稽核	Windows 群組原則中的一項功能，可詳細配置要記錄哪些特定系統事件，例如權限使用或物件存取。
異常偵測	識別異常模式或偏離既定正常行為基準的過程，這可能預示著安全威脅。
Auditd	Linux 稽核守護程式，一種用於建立系統呼叫與檔案存取之詳細、核心層級審計追蹤的系統元件。
基準線（正常行為）	經過一段時間建立的正常系統與活動網絡標準或模式，用作偵測異常及安全威脅的參考依據。
日誌集中儲存	將來自多個系統與裝置的日誌匯出並儲存至單一安全伺服器的做法，旨在防止篡改並便於分析。
CIA 三元組（機密性、完整性、可用性）	一種用於分類資訊系統的安全模型，基於三大核心原則：防止資料遭未經授權洩露（機密性）、確保資料準確性（完整性），以及確保在需要時能存取資料（可用性）。
數據外洩	將數據從電腦或數據網絡未經授權地傳輸或複製至外部位置的行為。
誤報	在實際未發生安全事件時，錯誤地指出已發生安全事件的警報，通常由合法但異常的活動觸發。
檔案完整性監控 (FIM)	一種用於監控和偵測關鍵系統或配置檔案變更的流程或工具，並在發現潛在未經授權的修改時向管理員發出警示。
群組原則	Microsoft Windows 中的功能，用於管理使用者和電腦的配置，包括在整個網路中啟用進階安全性與記錄設定。
主機端監控	專注於個別裝置（主機）上發生的活動與事件（例如檔案變更、日誌記錄或程序執行）的安全監控。
IDS/IPS（網絡入侵偵測/防禦系統）	一種用於監控網路流量以偵測惡意活動或政策違規的系統，可向管理員發出警示（IDS），或主動阻擋威脅（IPS）。
ISO 27002	一項國際標準，為資訊保安控制措施提供框架與指引，包含事件記錄與監控的最佳實務。
日誌分類與保留	根據日誌所涉及系統的敏感程度對日誌進行分類，並定義這些日誌必須保留的具體期間的流程。
日誌傳輸	將日誌資料從來源系統（如伺服器或防火牆）傳送至集中式儲存伺服器的流程，此傳輸應透過安全且經過加密的通道進行。
監控指標	用於追蹤系統或網路效能並偵測潛在安全威脅的具體、可量測的系統或網路活動指標（例如：CPU 使用率、登入失敗次數）。
NTP（網路時間協定）	一種用於透過電腦網絡同步電腦系統時鐘的協定，對於在不同事件記錄間準確關聯事件至關重要。
代理伺服器（用於記錄）	一種可路由應用程式流量的中介伺服器，使其能記錄請求，並補充缺乏原生記錄功能的應用程式的記錄能力。
即時警示	當監控系統偵測到符合預定義規則、且可能表示潛在安全事件的事件時，會立即發送的自動化通知。

術語	定義
資源使用狀況	一種監控指標，用於追蹤 CPU、記憶體、磁碟及網路帶寬等系統資源的消耗狀況，以偵測異常或資源密集型活動。
Syslog	一種標準協定，用於將系統日誌或事件信息傳送至特定伺服器（稱為 syslog 伺服器），以便進行集中式收集與分析。
分級分類（系統）	一種根據資訊系統對機密性、完整性及可用性的影響，將其劃分為不同層級（例如第 1、2、3 層）的方法，進而據此制定日誌保留政策。
過低閾值	設定過高或靈敏度不足的警示閾值，導致無法偵測到低於觸發閾值、但潛在惡意的細微活動。

供應商關係實務指南

版本 1.0

本文件旨在作為實務指南，僅供參考。各校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及需求。作者對任何基於本指南所採取的行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 前言 5
2. 與供應商協商 6
2.1. 供應商安全實務評估 6
2.2. 協議中的安全要求 6
2.3. 退出策略與合約終止 7
3. 效能評估 7
3.1. 效能指標 7
3.2. 客戶端監控 8
4. 涉及供應商的事故管理 8
4.1. 事件通報程序 8
4.2. 整合事件應變程序 8
5. 檢討與改進 9
5.1. 定期政策檢討 9
5.2. 因應新威脅與技術 9
5.3. 持續改進 9
附錄 10
術語表 10

1. 前言

1.1. 目的與範圍

本指南為管理供應商關係提供實用建議及基本標準，特別適用於全港各學校。其目的是協助教育機構在第三方管理方面維持一致的基準，使學校能夠與相關第三方建立安全的工作關係。

本指南涵蓋評估供應商資安措施的最佳方法，以及將明確的資安要求納入合約的相關內容。其設計旨在適應不同規模的學校、系統類型及可用資源。這些指引源自多個經認可的來源，包括香港教育局（EDB）以及互聯網安全中心（CIS），兩者均提供了作為本指南基礎的指引與資源。

1.2. 目標讀者（資訊科技管理員及技術人員）

本指南適用於資訊科技管理員、技術人員，以及任何負責管理學校環境中用戶帳戶或資訊科技系統的人員。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，資訊科技團隊將能更有效地：

- 評估供應商是否符合 ISO 27001 等公認標準
- 在供應商合約中明確界定安全要求，包括數據處理、所有權、終止合約後的歸還/刪除、備份時程表及事件通報流程
- 運用重要指標顯示供應商表現，以評估其對客戶端工具的使用情況
- 建立清晰的溝通管道，並將供應商程序整合至學校自身的事件應變計畫中

鼓勵各校根據自身技術環境與營運需求，適配這些建議。

2. 與供應商協商

本節闡述在訂閱供應商服務前應注意及值得核實的常見事項。學校應將此清單作為參考，並配合自身情況加以採用。

2.1. 供應商安全實務評估

- 對供應商的安全措施進行技術審查，例如了解存取控制、加密方法及漏洞管理。
- 透過基本的網路搜尋或供應商提供的報告，識別供應商系統中的風險，例如數據外洩的歷史紀錄。
- 考量與學校 IT 基礎架構的相容性。

調整建議：

- 確認供應商是否符合 NIST 或 ISO 27001 等標準。

審閱供應商提案中關於系統正常運作時間及安全承諾的條款。協商條款時應納入違約罰則，並保留在安全標準未達標時（例如安全稽核未通過或發生已公開的安全事件）終止合約的權利。

2.2. 協議中的安全要求

本節重點在於確保所提供的服務達到特定安全標準，以保障學校的權益。
協議應涵蓋以下安全條款：

- 供應商如何處理數據——數據在刪除前的儲存、傳輸及保留方式。
- 合約終止時數據的所有權、歸還及刪除事宜。
- 供應商的備份時程表及其資料保留方案。
- 服務的正常運作時間，以及服務中斷時的補償措施。
- 持續性安全更新（例如修補程式）的期限、範圍及成本
- 發生網路安全事件時的通報流程。

實用建議：

- 請參照其協議與貴公司的網絡安全政策進行比對，以確認是否需採取進一步措施，或該服務是否適合。

實務範例：

- 假設某雲端儲存服務供應商未對其伺服器上儲存的數據進行加密。學校可以制定政策，要求在上傳前對所有數據進行加密，或者直接放棄使用該服務。

2.3. 退出策略與合約終止

應預先規劃供應商的更換事宜。若因需更換供應商，卻發現所有數據都必須手動匯出，那將是極其糟糕的情況。

- 應在協議中納入退出條款，以確保合約終止時能順利轉移並刪除數據（例如：提供數據匯出工具）。
- 在服務正式上線前，應進行資料匯出功能測試，並定期進行本地備份。相關備份時程應明定於學校的備份政策中。

實務範例：

- 在與雲端服務供應商的協議中確保包含數據匯出功能，並於測試階段驗證其運作。
- 依據《備份與保留政策》，每日匯出數據以建立本地備份。

3. 效能評估

本節闡述用於衡量供應商服務效能的常見指標。學校應參考此清單並配合自身情況調整。請注意，效能監控可能高度取決於供應商的透明度（例如：其服務內建的監控工具）。

3.1. 效能指標

並非所有列出的指標都能輕鬆顯示，這取決於服務供應商。

- **延遲：**衡量處理請求並做出回應所需的時間，有助於找出回應時間的瓶頸。
- **吞吐量：**追蹤每單位時間內處理的請求或操作數量，例如每分鐘的請求數。
- **錯誤率：**顯示失敗請求或操作的百分比，以顯示可靠性問題。
- **資源利用率：**包含 CPU 使用率、記憶體消耗量，以及每秒儲存 I/O 操作次數 (IOPS)，可揭示您的資源配置是否過多或不足。
- **正常運作時間與可用性：**計算服務正常運作的時間百分比，通常與 SLA（服務水準協議）相關。
- **成本相關指標：**計算成本或進行成本效益分析，以確保效能與支出相符。

3.2. 客戶端監控

客戶端監控可消除對供應商的依賴，並提供真實使用者的視角。監控工具包括：

基本命令列工具：

- **Ping**：使用 Windows、macOS 或 Linux 系統內建的 ping 指令，向雲端服務的端點發送封包（例如：ping api.examplecloud.com）。此指令會回報平均往返時間 (RTT) 值（單位為毫秒）。若需持續監控，可使用 MTR（My Traceroute）等工具，結合 ping 與 traceroute 功能，以識別造成延遲的跳躍點。
- **Curl 或 Wget 用於測試吞吐量**：使用 curl 或 wget 測試下載速度。

集中式持續監控：

- **代理伺服器**：可配置代理伺服器以記錄並測量端點的延遲與帶寬，這將反映供應商的效能表現。

4. 涉及供應商的事故管理

本節列出可用於實體保護資產的技術控制措施。請將以下建議作為貴校的參考依據。

4.1. 事件通報程序

應要求供應商在協議中提供明確的事件通報機制，並於評估期間審查其應變計畫。這些機制應包含：

- 供應商端的任何偵測機制（例如：日誌、警示等）
- 學校端的任何通報機制（例如：服務請求單等）

4.2. 整合事件應變程序

- 將供應商的事件通報機制整合至學校監控系統中，利用其儀表板或警示功能以實現快速偵測。
- 制定涉及供應商的事件應變程序，包括向學校領導層升級的流程及聯絡對象。
- 維護供應商支援的聯絡清單。若可行，請定期（例如每年）測試聯絡管道。

5. 檢討與改進

5.1. 定期政策檢討

設定提醒，至少每年一次，或在資訊科技系統有所變更時，檢視貴校的資料處理與標籤標準。邀請資訊科技人員及教學／行政同仁共同參與，以收集有用的回饋意見。

5.2. 因應新威脅與技術

隨時掌握可能影響學校的新型網路威脅，例如網路釣魚詐騙或密碼外洩。同時，也應留意可能提供更佳密碼保護方式的新技術或軟體更新，例如雙因素驗證。

5.3. 持續改進

每次檢討後，請視需要更新密碼政策。將任何變更清楚地告知教職員與學生，並提供簡易的操作指引或舉辦工作坊，協助所有人遵循新規則。

附錄

術語表

術語	定義
客戶端監控	從學校自身網路測量供應商服務表現的做法，藉此從真實使用者的角度獲取延遲和吞吐量等指標。
合約終止	終止與供應商協議的正式程序，應遵循合約中預先定義的條款。
錯誤率	一種追蹤供應商服務中失敗請求或操作比例的效能指標，用以反映其可靠性。
升級流程	預先定義的程序，說明當事件需要升級處理時，應聯繫學校內部（例如：領導層）及供應商組織中的哪些人員。
退出策略	一項預先規劃的流程，用於終止與供應商的合作關係，確保在合約終止時，學校數據能被安全且完整地移轉或刪除。
匯出工具	供應商提供的工具或功能，讓學校能以可用的格式輕鬆從服務中提取其數據。
事件通報機制	供應商協議中定義的正式流程，概述供應商或學校應如何、何時以及向誰報告安全事件。
ISO 27001	一項資訊保安管理國際標準，可用作評估供應商安全態勢與合規性的基準。
延遲	從向供應商服務發送請求到收到回應之間的時間延遲，用於衡量響應速度並識別瓶頸。
NIST	美國國家標準與技術研究院（NIST），提供可用於評估供應商安全實務的網絡安全框架。
績效評估	根據關鍵指標對供應商服務進行量測與評估的流程，以確保其符合學校的營運及合約要求。
資源利用率	一項衡量供應商運算資源（例如 CPU、記憶體）消耗量的績效指標，有助於確保資源配置正確。
資料保留方案	供應商針對學校數據及備份在永久刪除前將儲存多久所制定的政策。
往返時間 (RTT)	數據封包從來源（學校）傳輸至目的地（供應商）並返回所需的總時間；這是衡量延遲的主要指標。
安全條款	供應商協議中的一項具體條款，用以界定與資料處理、儲存、歸還／刪除、備份及事件應變相關的安全義務。
服務水準協議 (SLA)	合約中正式界定供應商預期服務水準的條款，包含正常運作時間、效能的保證，以及未達標時的罰則。
供應商安全實務	供應商用以保護其系統及客戶資料的一套技術控制措施與政策，包括存取控制、加密及漏洞管理。
吞吐量	一種效能指標，用於衡量供應商服務在特定時間單位內所能處理的操作或請求數量（例如：每分鐘請求數）。
正常運作時間與可用性	一種計算供應商服務處於運作狀態且可供使用者存取的時間比例的指標，通常在服務水準協議（SLA）中予以保證。
漏洞管理	供應商用於識別、評估及修復其系統與軟體中安全弱點的流程。

生成式人工智能實用指南

版本 1.0

本文件旨在作為實用指南，僅供參考。學校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及需求。作者對基於本指南所採取的任何行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 前言 5
1.1. 目的與範圍 5
1.2. 目標讀者（資訊科技管理員及技術人員） 5
2. 隱私與數據保安；數據安全 6
2.1. 制定獲准與受限生成式人工智能工具的指引 6
2.2. 探索資料外洩保護 (DLP) 解決方案 7
2.3. 校園人工智能道德原則 7
2.4. 人工智能治理架構：三道防線 7
2.5. 人工智能應用影響評估 7
3. 相關教育 9
3.1. 生成式人工智能簡介 9
3.2. 生成式人工智能的優勢 9
3.3. 生成式人工智能的弱點 9
3.4. 使用生成式人工智能的常見風險與問題 9
3.4a. 人工智能相關罪案及安全風險（深度偽造） 10
3.5. 識別與處理敏感數據 10
3.6. 將內部文件中的數據匿名化的步驟 10
3.7. 識別使用生成式人工智能的服務 11
3.8. 負責任使用的最佳實踐 11
3.8a. 人工智能生成內容的標籤及可追溯性 12
3.9. 法律與政策考量 12
3.10. 案例研究與互動練習 12
3.11. 結論與資源 12
4. 其他 13
4.1. 設定年齡限制 13
4.2. 政策與教學材料的檢視 13
術語表 15

1. 前言

1.1. 目的與範圍

本指南針對學校使用生成式人工智能（GenAI）提供指引，涵蓋可能使用的各類工具，並闡述將這些工具融入校園環境的高階方法。本指南亦將提供實用建議，協助學校識別並應對生成式人工智能的潛在陷阱與風險，使其應用建立在健全的實踐基礎上，從而實現對人工智能的負責任且有效率的運用。

本指南的範圍涵蓋生成式人工智能的優缺點、為確保安全使用而必須管理的潛在隱私及數據管理風險，以及在處理供人工智能使用的數據時，用以減輕常見風險的步驟。 本指南設計上具高度適應性，可配合不同規模的學校、系統類型及可用資源進行調整。這些指引源自多個經認證的來源，包括香港教育局（EDB）以及互聯網安全中心（CIS），兩者均提供了作為本指南基礎的指導方針與資源。

本指南應與教育局《中小學數字教育發展藍圖》（2026 年）及其附篇二《中小學應用人工智能教學指南》一併閱讀，以掌握香港學校運用人工智能的教學原則，以及對教職員／課程的期望。附篇一《中小學人工智能素養學習架構》亦應一併查閱，以了解學生層面的人工智能素養課程內容。

1.2. 目標讀者（資訊科技管理員及技術人員）

本指南適用於資訊科技管理員、技術人員，以及任何負責管理學校環境中用戶帳戶或資訊系統的人員。本指南假設讀者具備資訊科技運作的基本知識。

遵循本文件中的指引，資訊科技團隊將能更有效地：

- 制定一系列關於在校園環境中審批生成式人工智能工具的指引
- 針對生成式人工智能（GenAI）所衍生的風險與問題實施緩解策略
- 分享針對不應公開分享的機密內部文件，進行資料匿名化及數據保護的步驟
- 辨識不同生成式人工智能服務供應商的優缺點
- 在全校範圍內建立負責任使用的最佳實踐

鼓勵各校根據自身技術環境與運作需求，適配這些建議。

2. 隱私與數據保安；數據安全

幾乎所有生成式人工智能服務皆運行於雲端運算，這其實只是指第三方擁有的電腦。本節說明學校可實施哪些管控措施，以確保隱私與數據保安。

2.1. 制定獲准與受限生成式人工智能工具的指引

- **供應商評估**：依據安全認證與數據隱私條款評估供應商，確保僅核准具備明確隱私保障的工具。
- **網路限制**：封鎖未經核准的生成式人工智能工具在學校網路上的存取權限，以維持安全與合規性。
- **簡化審批流程**：建立簡便流程，例如讓教職員透過表單提交工具詳細資訊（如網址），以高效審查並批准新工具。
- **定期政策檢討**：每年檢視供應商政策，以更新生成式人工智能工具的核准狀態，並確保持續符合規範。

建議於供應商評估流程中加入風險分級：不可接受風險／高風險／有限風險／低風險。

- 不可接受風險：例如生成用以假冒教職員／學生的欺騙性材料，或用以操控學生決定／情緒的工具：一律禁止；於校網封鎖。
- 高風險：例如支援評分、分班／收生決定，或學生福祉／行為評估的人工智能：必須人手覆核；備存審核紀錄；須經資訊科技督導小組批准方可使用。
- 有限風險：例如直接與學生互動的人工智能聊天機械人／導師：須公開披露使用人工智能；提供選擇退出機制；記錄使用情況。
- 低風險：例如一般寫作／創意輔助工具（教案草擬）：遵循上述標準審批流程。

實用建議：

- 查核安全合規報告（如 SOC 2（第二類））、ISO/IEC 27001，以及隱私合規報告（如 GDPR 合規性）。
- 雖然作業系統中已內建生成式人工智能工具（如 Copilot 和 Gemini），但截至本文撰寫之日，這些工具僅在使用者主動使用其功能時才會收集數據。

實務範例：

- 在校園範圍內透過 DNS 過濾功能封鎖所有受限的生成式人工智能工具。
- 若需禁止 Copilot，請透過 GPO 或 Intune 設定「關閉 Windows Copilot」政策。

2.2. 探索資料外洩保護 (DLP) 解決方案

建議採用各種數據保護解決方案，以即時監控使用者輸入內容。例如，以瀏覽器擴充功能形式呈現的端點數據保護解決方案，能夠在使用者將內容貼上至特定網站時，自動遮蔽個人識別資訊（PII）；而網路層級的數據保護解決方案（例如代理伺服器），則能掃描 HTTP 請求，並過濾或攔截被標記的請求。

2.3. 校園人工智能道德原則

- 透明及可解釋：機構應確保能夠以清晰及易於理解的方式，向人解釋明白人工智能應用的決策過程。
- 可靠、穩健及安全：人工智能應用的開發應確保能夠透過使用合適的模型和數據集，在長時間內穩定可靠地運作，並抵禦網絡攻擊，維持安全性。
- 公平：人工智能應用所作出的建議或產生的結果，應以公平方式對待相似群體中的每個人，不應偏袒或歧視，亦不應造成或引致傷害。
- 多元與包容：應通過了解和尊重所有受影響的持份者的利益，促進人工智能應用的包容性，並兼顧多元化的使用者需求。
- 人為監督：人工智能應用用於決策或操作過程中所需的人為干預程度，應取決於所涉及的道德問題的嚴重程度（例如評分對學生影響越大，所需人手覆核程度亦應越高）。
- 合法與合規、數據私隱：負責的機構應貫徹依據法律、規例及相關監管制度行事，並須遵守《個人資料（私隱）條例》的保障資料原則。
- 安全、問責、有益的人工智能、合作與開放、可持續性與公正轉型：人工智能應用不應危及學生的身心安全，機構須對其道德影響負責，其發展應促進共同福祉。

2.4. 人工智能治理架構：三道防線

- 第一道防線為項目團隊（校內對應：IT 協調員／提出申請的教師）：負責開發人工智能應用、風險評估、執行風險緩解措施，以及記錄「人工智能評估」工作。
- 第二道防線由項目督導委員會及項目保證小組組成（校內對應：資訊科技督導小組／數據保護主任）：確保項目品質，制定人工智能應用的驗收標準，進行獨立檢視，並於全校推行前批准人工智能應用。
- 第三道防線涉及資訊科技委員會／首席資訊官（校內對應：校長／學校管理委員會），並可選擇由人工智能道德委員會提供支援（校內可設「人工智能諮詢小組」）：負責審核、建議及監管高風險人工智能應用。

2.5. 人工智能應用影響評估

在批准任何新人工智能工具作全校使用前，建議簡略記錄以下組成部分：

- 風險分級準則：根據人工智能應用的特性，確定所需的評估級別。
- 人工智能應用評估問題：評估時應考慮人工智能應用的整個生命週期，每個問題均圍繞一個核心主題。

- 影響考量：識別對特定持份者（例如學生、教職員）的正面及負面影響，以及所需的控制措施。
- 檢討週期：應視乎項目進度定期（例如每年）或在發生重大變更時進行檢視。

3. 相關教育

許多人使用生成式人工智能（GenAI）服務，但鮮少有人了解其中的風險。以下提供一個框架，供資訊科技部門參考，用以製作相關員工培訓教材。學校應根據自身情況修改此清單，以製作更符合需求的教材。

3.1. 生成式人工智能簡介

- 定義與概述：說明何謂生成式人工智能（例如 ChatGPT、DALL-E 或 Midjourney 等工具，可根據提示生成文字、圖像或其他內容）。
- 與教育相關的實際案例（例如：生成教學大綱、摘要文章或製作學習輔助工具）。
- 培訓目的：強調應負責任地使用生成式人工智能，以在學校環境中最大化效益並將風險降至最低。

3.2. 生成式人工智能的優勢

- 效率與生產力：加速諸如腦力激盪、草擬電子郵件或製作教育內容等任務。
- 創造力與創新：協助產生多元觀點、視覺輔助工具或個人化學習材料。
- 可及性：支援多元學習者（例如：語言翻譯、針對不同需求學生提供的簡化說明）。
- 可擴展性：處理重複性任務，為教育工作者和職員節省時間。

3.3. 生成式人工智能的弱點

- 不準確與虛構內容：AI 可能產生看似合理但實際錯誤的資訊；使用者應始終核實輸出結果。
- 缺乏理解力：AI 無法真正理解語境或細微差異，導致回應流於表面或帶有偏見。
- 依賴風險：過度依賴可能阻礙使用者培養批判性思考或發展技能。
- 資源密集型：需具備互聯網連線，且可能對運算資源需求龐大。

3.4. 使用生成式人工智能的常見風險與問題

- 錯誤資訊與事實查核的挑戰：若未經交叉驗證，輸出結果可能傳播錯誤。
- 偏見與公平性問題：以不完善數據訓練的人工智能，可能延續既有偏見或特定觀點。
- 剽竊與智慧財產權疑慮：生成的內容可能侵犯著作權，或未標示來源。
- 安全性漏洞：輸入敏感資訊時，可能導致數據外洩或暴露。
- 倫理困境：例如在學術環境中利用 AI 作弊，或生成有害內容。

3.4a. 人工智能相關罪案及安全風險（深度偽造）

- 深度偽造（Deepfake）：生成式人工智能可製作高度逼真的虛假音訊、圖像或影片，模仿真實人物的樣貌或聲音。在學校環境中，此技術可能被用以假冒學生、教師或家長，捏造有損聲譽的材料，或針對特定學生進行欺凌。
- 學校應向教職員及學生講解如何辨識深度偽造內容，並設立清晰渠道，供人向 IT 協調員／訓導組舉報懷疑深度偽造或假冒事件。
- 模型越獄（Model jailbreaking）：使用者絕對不應嘗試繞過人工智能工具內置的安全過濾機制。任何此類嘗試，或任何顯示已繞過預期安全機制的人工智能產出，均應立即舉報。
- 亦應明確將利用深度偽造技術進行的網絡欺凌，以及「起底」（未經同意披露／分享他人個人資料）列為具體的可舉報濫用情況。

3.5. 識別與處理敏感數據

- 定義：說明機密數據（例如學生紀錄）、內部數據（例如學校政策）及敏感數據（例如姓名、地址或健康資訊等個人識別資訊）。
- 參照資料處理準則：引導使用者查閱學校的特定政策，以了解詳細的分類與合規要求（例如美國的《家庭教育權利與隱私法》（FERPA））。
- 警示訊號：如何在文件、電子郵件或提示中辨識敏感數據（例如：個人識別資訊、財務細節或學校專有資訊）。

3.6. 將內部文件中的數據匿名化的步驟

- 準備工作：在將文件輸入 AI 工具前，先審查文件中的敏感內容。
- 基本技巧：利用文字處理軟體的「尋找/替換」功能，將姓名、日期或地點替換為佔位符（例如，將「John Doe」替換為「學生 A」）。
- 進階方法：遮蔽圖片或表格、彙總數據（例如使用平均值取代具體數字），或使用匿名化軟體／工具。
- 驗證：仔細檢查匿名化版本，確保沒有任何可識別資訊殘留；並使用樣本提示進行測試。
- 最佳實務：避免上傳完整文件；僅萃取必要段落。
- 批改場景特例：教職員如須將學生作業上載至人工智能平台以進行批改或生成評語，須先移除任何可識別個人身分的資料，以確保完全符合《個人資料（私隱）條例》。

實務範例：

- 即使已部署 DLP 防護措施，仍值得對員工進行相關教育，並將 DLP 作為最後一道防線。
- 提醒員工在為生成式人工智能（GenAI）使用而進行數據匿名化時，切勿使用生成式人工智能工具，否則將背離匿名化的初衷。

3.7. 識別使用生成式人工智能的服務

- 常見範例：作業系統中的 AI 助手（例如 Windows 中的 Microsoft Copilot、iOS 中的 Siri 增強功能）。
- 生產力工具：Google Workspace 中的功能（例如 Docs 中的 AI 摘要）、Microsoft Office 中的功能（例如 Word 中的 AI 寫作助手）。
- 教育平台：例如可汗學院的 AI 導師或 Duolingo 的生成式功能。
- 網路服務：網站上的聊天機械人，以及像 Canva 的 Magic Studio 這樣的圖片生成工具。
- 如何確認：尋找「AI 驅動」等標籤，或查閱隱私權政策；在設定中啟用或停用 AI 功能。

適應性建議：

- 若適用，請考慮將此原則延伸至任何其他需輸入數據的第三方雲端服務。推廣「雲端不過是別人的電腦」這個觀念。

3.8. 負責任使用的最佳實踐

- 提示字串設計：撰寫清晰、具體的提示字串，以提升輸出品質並降低風險。
- 驗證與引用：務必將 AI 生成的內容與可靠來源交叉核對，並適當引用。
- 隱私保護：使用具備強大數據保護措施且經學校核准的工具；避免在處理敏感任務時使用免費或公開的 AI 服務。
- 協作與監督：鼓勵同儕審查 AI 產出，並考慮將其整合至學校工作流程中。

3.8a. 人工智能生成內容的標籤及可追溯性

- 任何用於學校官方通訊、證書、宣傳資料，或類似身分證明文件／財務文件的人工智能生成內容，均應清楚標示為「人工智能生成」或「人工智能輔助生成」。
- 如平台支援相關功能，應保留可追溯人工智能生成圖像或文件來源的後設數據／浮水印，以便日後如有爭議時可作追蹤及問責之用。

3.9. 法律與政策考量

- 版權與所有權：理解 AI 生成的內容可能並非完全原創；尊重智慧財產權法規。
- 校方特定規定：概述機構關於 AI 使用的政策（例如：作業中的可接受使用範圍、對特定工具的禁令）。
- 法規遵循：簡要說明相關法律（例如：數據保護法規，如《一般資料保護條例》（GDPR）或針對未成年人的《兒童線上隱私保護法》（COPPA））。
- 問題通報：如何向學校資訊科技部門或行政單位通報與人工智能相關的問題，例如偏見或錯誤。

實務範例：

- 建議教職員使用可檢查潛在侵權問題的工具，例如 Grammarly 剽竊檢測器。

3.10. 案例研究與互動練習

- 真實情境：教育領域中 AI 濫用的案例（例如教師輸入學生數據導致數據外洩），以及成功且負責任的應用實例。
- 實作活動：角色扮演匿名化流程、辨識工具中的 AI 成分，或針對 AI 產出進行準確性與偏見的批判性分析。
- 測驗或討論：鞏固關鍵概念並鼓勵反思。

3.11. 結論與資源

- 重點摘要：總結效益與責任之間的平衡。
- 持續學習：鼓勵透過學校公告或可信來源，隨時掌握 AI 發展動態。
- 支援資源：提供學校指引連結、外部教學資源（例如聯合國教科文組織關於教育中人工智能倫理的指南），或諮詢聯絡資訊。

4. 其他

4.1. 設定年齡限制

一般建議

聯合國教科文組織《教育與研究中生成式人工智能指南》（2023）建議，生成式人工智能服務的年齡限制應設定為至少 13 歲。

生成式 AI 供應商通常會提及其服務的 13 歲年齡要求，而其他供應商則在其服務條款中規定須年滿 18 歲，以避免因可能涉及成人內容而承擔法律責任。

我們的建議

我們建議在小學的學生網路中，採用全網內容過濾機制，例如 DNS 代理伺服器或防火牆。

然而，對於中學，我們認為應由學校自行決定是否實施此類管控措施。

實作建議：

- 透過應用網路分隔的概念，可在學生互聯網存取環境與教職員互聯網存取環境中，分別實施不同的存取控制措施。

按學生年齡及年級的分階段安排：

- 低小階段：學生只應在教師引導下，初步認識／體驗人工智能科技；毋須（亦不要求）獨立操作生成式人工智能工具。
- 高小階段：生成式人工智能工具原則上只應在教師或監護人直接指導下使用，因為該階段的學生尚未能穩妥判斷人工智能生成內容的真確性。
- 中學階段：學生可循序漸進，逐步自主使用人工智能工具（備課、自主探索、朋輩學習），並須負起愈來愈大的責任，核實人工智能產出內容及引用出處。
- 學校應在生成式人工智能供應商自訂的最低年齡要求以外，一併採用上述分階段安排；而上文建議小學階段實施的全網內容過濾措施仍然適用。

4.2. 政策與教學材料的檢視

鑑於生成式人工智能技術（包括模型、工具及相關法規的進展）日新月異，必須定期檢視並更新政策與培訓教材，以確保其準確性與適用性。新功能、倫理考量、法律要求及最佳實踐可能不斷出現，進而影響處理生成式人工智能的相關程序。

我們建議定期（例如每年）重新檢視這些材料，或在人工智能技術、學校政策或適用法律（例如數據保護或著作權法規）有重大更新時進行檢視。請務必參閱特定人工智能工具的最新服務條款以及貴機構的指引，以確保符合規範並掌握最新資訊。

術語表

術語	定義
生成式人工智能 (GenAI)	指利用訓練數據中學習到的模式，根據使用者提示來生成新內容（文字、圖像、程式碼、音訊等）的人工智能系統。
提示	提供給生成式人工智能工具的文字或指示，用以引導其生成的內容。
提示工程	透過設計清晰、具體且結構化的提示，以提升生成式人工智能的輸出品質並降低風險的實踐方法。
經核准的生成式人工智能工具	已通過學校安全、隱私及合規性審查，並獲授權使用的生成式人工智能服務。
受限生成式人工智能工具	因安全、隱私、合規或政策考量而被封鎖或禁止的生成式人工智能服務。
供應商評估	在批准前，對生成式人工智能供應商的安全性、隱私、合規性、可靠性及合約條款進行評估。
簡化核准流程	一種輕量級的提交與審查工作流程（例如：附有工具網址的員工表單），用於高效評估並授權新的生成式人工智能工具。
定期政策審查	針對已核准／受限工具及供應商政策進行定期（例如每年）重新評估，以維持持續合規。
網路限制	用於防止在學校網路中存取未經批准的生成式人工智能服務的存取控制措施（例如：DNS 封鎖、防火牆規則）。
DNS 過濾	一種利用網域名稱系統 (DNS) 政策來封鎖或允許存取特定網站或類別的控制措施（例如：封鎖受限的生成式人工智能工具）。
群組原則物件 (GPO)	一種 Windows/Active Directory 機制，用於在已加入網域的裝置上集中強制執行設定（例如：「關閉 Windows Copilot」）。
Microsoft Intune	一款基於雲端的裝置與應用程式管理平台，可在受管裝置上強制執行政策（例如：停用 Copilot）。
Windows Copilot	整合於 Windows 中的 Microsoft AI 助理，提供由 AI 驅動的協助與內容生成功能。
Google Gemini	Google 的生成式 AI 套件，可用於 Google 各項產品與服務，可協助內容創作與摘要生成。
安全認證	針對供應商安全控制措施的獨立驗證（例如 SOC 2 Type II、ISO/IEC 27001）。
SOC 2 Type II	一份審計報告，用於評估服務組織在特定期間內所實施之控制措施的設計與運作成效。
ISO/IEC 27001	一項規範資訊保安管理系統（ISMS）要求的國際標準。
GDPR	歐盟《一般資料保護條例》，規範個人數據的處理與數據保護。
COPPA	一項美國法律（《兒童線上數據保護法》），規範針對 13 歲以下兒童的線上數據蒐集。

FERPA	美國法律（《家庭教育權利與隱私法》），旨在保護學生教育紀錄的隱私。
數據外洩防護 (DLP)	亦稱為資料外洩防範；指用於偵測並防止敏感數據離開核准範圍的技術與流程。
端點 DLP	部署於使用者裝置上的 DLP 控制措施（例如瀏覽器擴充功能），用於監控並在敏感數據傳送前進行封鎖或遮蔽。
網路 DLP	位於網路層級的 DLP 控制措施（例如代理伺服器），用於檢查網頁/HTTP 流量，並阻擋、隔離或標記敏感數據外洩行為。
代理伺服器	一種用於中介網頁請求的伺服器，可進行檢查、過濾、記錄及執行政策（例如用於 DLP）。
HTTP 請求檢查	對外發出的網頁請求進行分析，以在數據離開數據網絡前偵測敏感內容或政策違規。
剪貼簿資料遮蔽	當使用者將數據貼上（例如貼入網頁表單）時，由 DLP 工具強制執行敏感數據的自動遮蔽或移除。
個人可識別資訊 (PII)	可識別個人身分的數據（例如：姓名、地址、電子郵件、電話號碼、學生證號、健康資訊）。
敏感數據	若遭洩露可能造成危害的數據（例如：個人識別資訊、財務數據、健康數據、內部評估報告）。
機密數據	僅限特定對象查閱的高度受限資訊（例如：學生紀錄、教職員紀律檔案）。
內部數據	供內部使用但未受嚴格限制的非公開資訊（例如：政策草案、內部備忘錄）。
匿名化	移除或轉換識別資訊的過程，以確保無法透過數據重新識別個人身分。
遮蔽	在分享或供人工智能使用前，從文件中移除或遮蔽特定敏感元素（例如：姓名、身分證號碼）的過程。
彙總	將數據整合為摘要（例如平均值、總和），以降低可識別性並保護隱私。
佔位符	用於取代文件或提示語中真實識別碼的通用標籤（例如「學生 A」、「學校 X」）。
匿名化驗證	在匿名化或刪除處理後，進行二次檢查以確保不再存在任何可識別資訊的流程。
數據最小化	僅分享最低限度的必要數據（例如：摘錄而非完整文件），以降低數據外洩風險的作法。
錯誤資訊	可能在生成式人工智能（GenAI）輸出中看似合理，但必須經過事實查核的虛假或不準確內容。
AI 幻覺	由生成式人工智能產出的虛構或錯誤內容，卻被自信地呈現為事實。
偏見與公平性	源自訓練資料或模型行為、可能影響公平性與準確性的 AI 輸出中不當偏差。
驗證與引用	將 AI 生成的內容與可靠來源進行交叉核對，並適當引用來源的作法。

道德使用	對生成式人工智能（GenAI）的負責任應用，旨在避免造成危害（例如作弊、有害內容），並尊重權利與政策。
智慧財產權 (IP)	與心智創作相關的權利（例如著作權）；在使用或透過生成式人工智能（GenAI）生成內容時需予以考量。
著作權	規範創意作品使用與散佈的法律權利；涉及使用 AI 生成內容或原始內容時。
剽竊	未經適當標示來源，將他人的作品或想法冒充為己有的行為；若未經核實，AI 產出內容可能有此風險。
隱私權政策	供應商所發布的聲明，說明其收集哪些數據、如何使用這些數據，以及與該數據相關的用戶權利。
服務條款 (ToS)	規範服務使用方式的合約條款，包含年齡限制、使用權限及各項限制。
數據隱私條款	由服務提供者制定的合約條款或政策，用以規範個人數據的處理、保護及共用方式。
學校核准的工具	經學校依據風險評估與合規檢查，針對特定使用情境審核並授權的服務。
公開/免費 AI 工具	面向消費者的 AI 服務，可能缺乏企業級隱私保障，且未獲准用於處理敏感任務。
第三方雲端服務	由外部供應商在其基礎設施中主機應用程式或 AI 工具（即「他人的電腦」）。
雲端服務	透過供應商自有基礎設施經由互聯網提供的服務，通常為多租戶架構且由遠端管理。
負責任的人工智能應用	旨在最大化教育效益，同時將風險（隱私、準確性、倫理、合規性）降至最低的實踐方式。
培訓材料	經過嚴選的內容，用於教育員工了解生成式人工智能的優勢、弱點、風險及安全操作規範。
案例研究與實作練習	透過逼真的情境與實作活動，練習資料匿名化、風險辨識及輸出結果的批判性評估。
問題通報	員工向 IT 部門或管理員通報 AI 相關問題（例如：偏見、錯誤、疑似違規）的流程。
年齡管控	設定最低年齡限制，或限制年幼學生使用生成式人工智能服務的政策或技術措施。
聯合國教科文組織指引（2023）	聯合國教科文組織針對教育與研究領域生成式人工智能的建議，其中包含建議最低使用年齡為 13 歲。
全網內容過濾	在學生網路中實施的管控措施（例如 DNS 過濾、防火牆），用以阻擋不當或具風險的內容。
DNS 代理	一種在網域名稱解析層執行過濾與記錄政策，同時轉發查詢的 DNS 服務。
防火牆	一種基於規則允許或封鎖流量的網路安全裝置或服務，用於執行生成式人工智能（GenAI）的存取政策。
網路隔離	將網路進行區隔（例如學生與教職員），以實施不同的管控措施並降低風險。
政策檢討週期	隨著技術與法規的發展，重新檢視並更新 AI 政策與培訓的建議頻率（例如：每年一次）。

核准清單	由學校維護並更新的通用人工智能工具清單，其中工具分為「已核准」或「受限制」兩類。
數據處理準則	針對使用生成式人工智能工具時，對數據進行分類、匿名化及數據保護的機構程序。
內建 AI 功能	整合於作業系統或生產力套件中的 AI 功能（例如 Windows 中的 Copilot、Google Workspace 中的 AI）。
生產力 AI 功能	存在於 Docs 或 Word 等工具中的生成式人工智能功能，可協助起草、摘要，或輔助撰寫與分析。
安全漏洞	在與生成式人工智能（GenAI）或相關服務互動時，可能導致數據外洩或遭濫用的弱點。
即時監控	透過工具（例如 DLP）進行持續監控，以即時偵測並阻擋敏感數據的洩露。
剪貼簿監控	檢查複製/貼上內容，以防止敏感資訊意外外洩。
敏感任務限制	制定政策，禁止在涉及敏感或機密性數據的任何任務中使用公共／免費的 AI 工具。
合規	在使用生成式人工智能工具時，須遵守法律、法規及政策要求（例如：GDPR、COPPA）。

第三部份:

學校常見網絡安全事故應對流程

事件應變工作流程

版本 1.0

本文件僅供參考之用。各校應審閱相關建議，並視需要加以調整，以符合自身環境、資源及需求。作者對基於本指南所採取的任何行動概不負責。

版本歷史

版本 日期	版本號	變更說明	作者

目錄

1. 勒索軟體攻擊 6
1.1 準備工作 6
1.2 偵測 6
1.3 隔離 6
1.4 根除與復原 7
1.5 事件後處理 7
2. 網路釣魚與惡意軟件感染 8
2.1 準備 8
2.2 偵測 8
2.3 隔離 8
2.4 根除與復原 9
2.5 事件後處理 9
3. 遺失／遭竊裝置 10
3.1 準備 10
3.2 偵測 10
3.3 隔離 10
3.4 根除與復原 10
3.5 事件後處理 11
4. 意外數據洩露 12
4.1 準備 12
4.2 偵測 12
4.3 封鎖 12
4.4 根除與復原 12
4.5 事件後處理 13
5. 網站篡改 14
5.1 準備 14
5.2 偵測 14
5.3 隔離 14
5.4 根除與復原 14

5.5 事件後處理 15
6. 拒絕服務 (DoS) 攻擊 16
6.1 準備 16
6.2 偵測 16
6.3 遏制 16
6.4 根除與復原 17
6.5 事件後處理 17
附錄 18
術語表 18

1. 勒索軟體攻擊

勒索軟體攻擊是一種惡意事件，攻擊者會將學校的檔案加密，使其無法存取，並要求支付贖金以換取解鎖。應對措施的優先要務是立即隔離受影響的系統以防止擴散，並依賴從安全的離線備份中還原資料，而非支付贖金。事後處理工作則著重於識別最初的漏洞，並評估敏感資料是否在加密前已被竊取。

1.1 準備工作

1. **建立／維護 CIRT：**組建核心網路事件應變小組（CIRT），並明確界定各成員職責。
2. **備份：**對所有關鍵數據進行定期、自動化的備份。關鍵在於確保至少有一份副本處於離線/物理隔離狀態且不可變更。
3. **測試備份：**定期測試數據還原功能，以確保備份有效。
4. **工具：**部署並維護端點偵測與回應（EDR）或強大的防毒解決方案。使用電子郵件過濾功能來阻擋惡意附件。
5. **培訓：**培訓員工識別釣魚郵件和可疑連結，因為這些是常見的進入點。

1.2 偵測

1. **初步偵測：**收到檔案無法存取、出現新檔案副檔名、贖金通知出現在螢幕上，或防毒軟體針對勒索軟體活動發出警示的通報。
2. **分析：**確認事件屬勒索軟體攻擊。釐清影響範圍（哪些系統/伺服器受到影響？）。若可行，利用 EDR/防毒軟體日誌找出最初的入侵點。**切勿點擊勒索訊息中的任何連結。**

1.3 隔離

1. **立即隔離：**將受影響的裝置從學校網路中斷開（拔除以太網線、停用 Wi-Fi）。切勿關機，以免遺失寶貴的鑑識數據。
2. **網路區段隔離：**若攻擊範圍廣泛，應考慮將整個網路區段（例如學生網路）或全校網路斷開連線，以防止進一步擴散。
3. **停用帳戶：**停用與初始感染相關的用戶帳戶。作為預防措施，請變更所有管理員及服務帳戶的密碼。

1.4 清除與恢復

1. **諮詢專家：**通知您的 IT 服務供應商或網絡安全專家。切勿嘗試支付贖金（根據 NCSC/ACSC 的建議）。
2. **根除：**將所有受影響的系統格式化，並從已知安全的「黃金映像」重新建立系統映像。切勿僅執行防毒掃描。
3. **還原：**從最新、經過測試且乾淨的離線備份中還原數據。確保備份時間早於初始感染時間（「潛伏期」）。
4. **修補：**識別並修補導致攻擊的漏洞（例如：未修補的軟體、弱 RDP 憑證）。

1.5 事件後處理

1. **通報：**向相關主管機關通報事件（例如：警方、英國的 Action Fraud/NCSC、澳洲的 ReportCyber）。
2. **評估數據外洩：**確認個人數據是否遭存取或外洩。若屬實，須向數據保護主管機關（例如英國資訊專員辦公室 ICO、澳洲資訊專員辦公室 OAIC）通報，並依規定通知受影響者（家長／員工）。
3. **經驗教訓：**進行事後檢討，以找出安全控制措施的弱點並改善應變計畫。

2. 網路釣魚與惡意軟件感染

此類事件通常始於一封具欺騙性的釣魚電子郵件，誘使用戶安裝惡意軟件或洩露其憑證。應對措施著重於將威脅限制在單一裝置內，方法包括將該裝置與網路隔離、重設受影響用戶的密碼，以及集中刪除其他郵箱中的惡意電子郵件。復原程序涉及清理或重新映像裝置，而事後工作則著重於用戶溝通及針對性培訓，以防止事件重演。

2.1 準備工作

1. **技術控制措施：**實施強效的電子郵件過濾機制（反垃圾郵件、反釣魚）。使用最新的端點防毒/反惡意軟件。透過 DNS 過濾阻擋已知的惡意網站。
2. **使用者培訓：**針對全體員工定期舉辦強制性的網絡安全意識培訓，重點在於識別釣魚攻擊。
3. **通報流程：**建立簡單明確的流程，供使用者通報可疑的釣魚電子郵件（例如：轉寄至特定的 IT 電子郵件地址）。
4. **最小權限原則：**確保使用者僅擁有其職務所需的存取權限。

2.2 偵測

1. **初步偵測：**使用者通報可疑電子郵件、點擊連結或開啟附件。防毒軟體發出威脅警示。裝置開始出現異常行為（運作緩慢、彈出視窗）。
2. **分析：**IT 團隊在不點擊連結的情況下，檢視通報電子郵件的標頭與內容。他們分析防毒警報中的惡意軟件簽名，以了解其性質（例如：鍵盤側錄程式、資訊竊取程式、木馬）。

2.3 遏制

1. **隔離裝置：**立即將用戶的裝置從網路中斷開。
2. **重設憑證：**強制重設受影響用戶的帳戶密碼，因其憑證可能已遭洩露。
3. **封鎖指標：**在網路防火牆或電子郵件通訊閘處，封鎖寄件者的電子郵件地址，以及在釣魚郵件中發現的任何惡意網域/IP。
4. **掃描郵箱：**搜尋所有學校郵箱中是否還有其他相同的釣魚電子郵件，並集中刪除。

2.4 根除與復原

1. **清除**：使用信譽良好的防毒/反惡意軟件工具執行完整系統掃描。對於高風險感染（如憑證竊取程式），最安全的做法是清除裝置並重新建立映像檔。
2. **驗證完整性**：檢查裝置是否存在惡意軟件可能安裝的持久化機制（例如：排程任務、登錄檔變更）。
3. **恢復**：如有必要，從乾淨的備份中還原任何損毀或遺失的用戶數據。將已清理/重建的裝置重新連接到網路。

2.5 事件後處理

1. **通報**：向全體員工發送警報，詳述釣魚攻擊活動的細節（例如：主旨、寄件者），並提醒他們切勿與之互動。
2. **檢討**：分析釣魚郵件為何能繞過過濾器，並在可行時調整規則。
3. **針對性培訓**：將此次事件作為未來培訓的實際案例。應對通報此事件的用戶給予正面肯定。若用戶上當受騙，應提供支持性及補救性培訓。

3. 裝置遺失／遭竊

此事件涉及學校所有裝置的實體遺失或遭竊，對裝置上儲存的任何敏感數據造成即時風險。應對措施是一場與時間的競賽，重點在於利用流動裝置管理（MDM）解決方案，遠端鎖定裝置或清除其數據。 控制措施還包括撤銷用戶的帳戶存取權限，以防止憑證遭濫用。事後評估對於判定是否發生須通報的數據外洩事件至關重要，而這在很大程度上取決於該裝置是否經過加密。

3.1 準備工作

1. **資產清查：**建立所有學校所有設備（筆記型電腦、平板電腦）的準確清單。
2. **技術控制：**對所有攜帶式裝置強制實施全磁碟加密（例如 Windows 的 BitLocker、macOS 的 FileVault）。
3. **MDM：**將所有行動裝置註冊至具備遠端鎖定與清除功能的流動裝置管理解決方案中。
4. **政策與培訓：**制定明確的政策，要求教職員與學生必須立即通報裝置遺失或遭竊。並針對此程序對其進行培訓。

3.2 偵測

1. **初步偵測：**教職員或學生通報其校發裝置遺失或遭竊。
2. **分析：**立即透過資產清單確認用戶身分及遺失裝置的詳細資訊。判斷裝置上可能存有何種數據（例如學生紀錄、敏感電子郵件），以及數據是否經過加密。

3.3 控制

1. **遠端鎖定／清除：**立即使用 MDM 解決方案對裝置觸發遠端鎖定，以防止存取。若裝置極可能無法尋回或含有高度敏感數據，則觸發遠端清除。
2. **撤銷存取權限：**暫時停用使用者的學校帳戶，以防止其存取雲端服務（電子郵件、共用資料夾）。
3. **變更密碼：**強制使用者重設密碼。

3.4 清除與恢復

1. **清除：**遠端清除操作可徹底清除遺失裝置上的數據。在資產清單中將該裝置標記為「遺失/遭竊」。

2. **恢復：**為使用者配置一台新的、安全的裝置。將其數據從雲端服務或備份還原至新裝置。重新啟用其學校帳戶。

3.5 事件後處理

1. **向警方報案：**若裝置遭竊，請建議使用者向警方報案並取得案件編號。
2. **評估數據外洩：**此屬實體數據外洩事件。若裝置未加密且含有個人數據，即屬須通報之事件。應依法通知數據保護主管機關（ICO/OAIC）及受影響之個人。
3. **檢視政策：**檢視實體安全與裝置處理政策，評估是否有改進空間。

4. 意外數據洩露

此類事件通常由人為疏失引起，例如將含有敏感資訊的電子郵件寄錯收件人，或錯誤設定檔案共享權限。應對措施不涉及技術層面，重點在於溝通：嘗試召回信息、聯繫非預期收件人要求並確認刪除資料，以及若洩露是透過雲端共享連結發生，則撤銷存取權限。 事後處理步驟包括評估危害風險，以判定是否需要進行正式的數據外洩通知，並為相關人員提供支援性及補救性培訓。

4.1 準備工作

1. **數據分類：**制定簡明的數據分類政策（例如：公開、內部、機密性），並對員工進行相關培訓。
2. **培訓：**針對常見錯誤（例如不當使用「全體回覆」、將電子郵件寄給錯誤的收件人，或錯誤設定檔案共享權限）對員工進行培訓。
3. **DLP 工具：**若可行，請在電子郵件系統中實施基本的數據外洩防護 (DLP) 規則，在用戶將包含敏感關鍵字（例如「學生證號」）的電子郵件發送至校外之前，向其發出警告。

4.2 偵測

1. **初步偵測：**使用者自行通報已將含有敏感數據的電子郵件寄給錯誤對象，或收件者通知學校誤收數據。
2. **分析：**迅速核實事件。精確確認洩露的數據內容、收件人（內部／外部）以及資訊的敏感程度。

4.3 控制

1. **嘗試召回：**立即嘗試召回該電子郵件（需理解此舉未必總是有效，特別是針對外部收件人）。
2. **聯繫收件人：**透過電話或另發電子郵件聯繫非預期收件人，說明錯誤原因，並正式要求對方刪除該資訊，並以書面形式確認已刪除。
3. **撤銷存取權限：**若資料是透過雲端連結（例如 SharePoint、Google Drive）分享，請立即撤銷對該檔案或資料夾的存取權限。

4.4 清除與恢復

1. **徹底清除：**當您收到非預期收件者已刪除數據的確認通知時，即視為已徹底清除。請將此確認記錄在案。

2. **恢復：**無需進行技術性恢復。重點在於程序性恢復：確保原始數據已妥善保管，且使用者已理解此錯誤。

4.5 事件後處理

1. **評估數據外洩：**此屬數據外洩事件。事件負責人必須評估數據遭洩露之個人可能遭受的危害風險。
2. **通報：**根據風險評估結果，若事件符合強制通報門檻，應向數據保護主管機關（ICO/OAIC）通報此數據外洩事件。
3. **通知：**告知受影響的個人（或其父母）有關資料外洩事件、潛在影響，以及為減輕影響所採取的措施。
4. **培訓：**為涉事員工提供補救性培訓，並將匿名化情境應用於更廣泛的員工培訓中。

5. 網站篡改

網站篡改是一種攻擊行為，指未經授權者取得存取權限並竄改學校公開網站的視覺內容，通常意在損害聲譽。即時應對措施是將網站下線，並以靜態維護頁面取代，以控制損害範圍。復原工作並非修復遭篡改的內容，而是應在識別並修補導致存取的漏洞後，從已知無虞的備份中還原整個網站。 事後處置工作則著重於強化網站安全性，以防止攻擊者再次入侵。

5.1 準備工作

1. **安全存取：**為所有網站管理員帳戶強制實施強效且唯一的密碼，並啟用多重認證 (MFA)。限制管理員帳戶的數量。
2. **修補程式：**確保網站的內容管理系統（CMS）、佈景主題及外掛程式隨時保持最新修補狀態並完成更新。
3. **備份：**定期自動備份網站檔案與數據庫，並將備份檔案儲存於與網頁伺服器分開的位置。
4. **監控：**使用檔案完整性監控服務，以偵測網站檔案的未經授權變更並發出警示。

5.2 偵測

1. **初步偵測：**學校透過教職員、學生、家長通報，或透過網站監控系統，發現網站內容遭篡改，出現未經授權的信息或圖片。
2. **分析：**驗證篡改事實。擷取螢幕截圖作為證據。檢查伺服器日誌，以識別篡改發生時段周邊的可疑 IP 位址或活動。

5.3 控制

1. **將網站下線：**立即將網站下線，並替換為預先準備好的靜態維護頁面（例如：「本網站暫時無法使用。我們正在努力盡快恢復服務。」）。此舉可防止聲譽進一步受損。
2. **保存證據：**在進行任何變更前，先對遭篡改的網站進行完整備份/快照，以供日後調查之用。

5.4 根除與復原

1. **識別漏洞：**分析日誌與檔案以找進入點（例如：存在漏洞的外掛程式、遭竊取的密碼）。

2. **清除與恢復：**從伺服器刪除所有網站檔案。從最近的已知乾淨備份中還原網站檔案與數據庫。**切勿**僅嘗試編輯遭篡改的頁面。
3. **強化安全：**變更所有管理、數據庫及 FTP 密碼。針對遭利用的漏洞套用修補程式。掃描還原後的網站，檢查是否仍有後門。
4. **恢復上線：**確認安全無虞後，將還原的網站重新上線。

5.5 事件後處理

1. **檢討：**針對事件進行檢討，以確認根本原因。
2. **強化安全：**根據檢討結果實施額外安全措施，例如部署 Web 應用程式防火牆 (WAF) 或實施更嚴格的存取控制。
3. **溝通：**通知學校社群（如有必要），提供網站問題已解決且安全性已獲得強化的資訊。

6. 拒絕服務（DoS）攻擊

拒絕服務（DoS）攻擊旨在透過惡意流量淹沒關鍵線上服務（例如學校網站或互聯網連線），使其無法正常運作。與其他事件不同，主要應對措施並非技術層面，而是程序層面：應立即聯繫學校的互聯網服務供應商（ISP）或主機代管服務商，因為他們擁有網路層級的工具來過濾並阻擋攻擊流量。 學校的職責在於顯示服務恢復狀況，並在內部通報中斷情況，同時與服務供應商共同進行事後分析，以實施更強有力的預防措施。

6.1 準備工作

在以下情況下應更新《軟體資產清單》：

1. **了解您的服務供應商：**請隨時備妥您的互聯網服務供應商（ISP）及網站主機供應商的 24/7 技術支援聯絡資訊。
2. **使用防護服務：**針對學校網站等關鍵服務，應採用具備 DDoS 緩解功能的雲端 DNS/代理服務（例如 Cloudflare）。
3. **可擴展的主機服務：**將關鍵服務主機於能隨流量小幅激增而自動擴展的平台。
4. **網路監控：**建立基本的網路流量監控機制，以識別異常流量激增。

6.2 偵測

1. **初步偵測：**收到報告指出學校網站、學習平台或整個互聯網連線離線，或速度慢到無法使用。監控工具顯示入站網路流量極高。
2. **分析：**區分一般中斷與 DoS 攻擊。DoS 攻擊的特徵是來自眾多（DDoS）或少數（DoS）來源的大量持續流量，導致伺服器或網路鏈路不堪負荷。

6.3 遏制

1. **聯繫服務供應商：這是最關鍵的一步。**立即聯繫您的網際網路服務供應商（ISP）或網站主機服務商。告知對方您懷疑正遭受 DoS 攻擊。他們具備網路層級的工具來緩解攻擊（例如「黑洞化」流量、流量速率限制）。
2. **啟用緩解措施：**若您使用 Cloudflare 等服務，請啟用其「I'm Under Attack」形式。
3. **內部通報：**告知員工關鍵服務因疑似網路攻擊而中斷，並提供解決問題的資訊，您正與服務供應商合作解決問題。

6.4 根除與復原

1. **與服務供應商合作：**供應商將透過過濾惡意流量來執行根除作業。您的角色是監控服務狀態。
2. **恢復：**隨著服務供應商的緩解措施生效，服務將逐漸恢復可用性。測試關鍵服務（網站、電子郵件）以確認其運作正常。

6.5 事件後處理

1. **攻擊後分析：**與您的服務供應商進行事後檢討，以了解攻擊的性質與規模。
2. **落實建議：**執行服務供應商提出的任何安全建議，以更好地抵禦未來的攻擊。
3. **通報：**提供學校社群資訊，告知服務已恢復正常。通常無需明確指出原因為 DoS 攻擊；僅表示「技術問題」或「網路中斷」往往已足夠。

附錄

術語表

術語	定義
意外數據洩露	指敏感資訊因人為疏失（例如將電子郵件寄錯收件者）而無意間暴露給未經授權者的事件。
物理隔離備份	指物理上與網路斷開連接的備份副本，使其免受勒索軟體等線上攻擊的影響。
資產清單	一份詳盡且最新的清單，列出所有學校擁有的技術資產（例如筆記型電腦、平板電腦和伺服器），對於事故管理與應對至關重要。
後門	一種繞過正常驗證或安全控制的隱蔽方法，通常由攻擊者在初次入侵後留存，以便重新取得系統存取權限。
黑洞化	一種 DoS 緩解技術，由網際網路服務供應商（ISP）將所有發送至受攻擊 IP 位址的流量導向「黑洞」，使其在抵達學校網路之前即被有效拋棄。
遏制	事件應變階段中，著重於阻止攻擊擴散並防止進一步損害的階段，例如將受影響的裝置與網路隔離。
內容管理系統 (CMS)	用於建立及管理網站內容的軟體平台（例如 WordPress、Joomla）。若未保持更新，此類系統常成為攻擊者的目標。
網路事件應變小組 (CIRT)	由預先指定且具備明確職責（例如：事件負責人、技術負責人）的成員組成的團隊，負責管理網絡安全事件的應對工作。
數據分類	根據數據的敏感程度（例如：公開、內部、機密性）進行分類，以確定適當的數據保護等級的過程。
數據外洩	未經授權從網路複製或傳輸數據的行為。現代勒索軟體通常會在加密數據前先將其外洩，從而造成數據外洩事件。
數據外洩防護 (DLP)	旨在偵測並防止敏感數據被傳送至組織數據網絡之外的技術或流程。
數據保護主管機關	負責執行數據隱私法規並處理數據外洩通報的政府機關（例如英國的 ICO、澳洲的 OAIC）。
拒絕服務（DoS）／分散式拒絕服務（DDoS）	一種旨在透過單一（DoS）或多個（DDoS）來源發送大量惡意流量，使服務（如網站或互聯網連線）無法正常運作的攻擊。
DNS 過濾	一種安全措施，透過阻止用戶裝置將網站的網域名稱解析為 IP 位址，從而封鎖對已知惡意網站的存取。
駐留時間	從網路最初遭到入侵到攻擊被偵測到的這段時間。了解滯留時間對於勒索軟體復原至關重要，以確保能從攻擊者入侵前的時間點還原備份。
端點偵測與回應 (EDR)	一種進階的防毒軟體，可對端點裝置進行即時監控與分析，以偵測、調查並應對威脅。

根除	事件應變的階段，重點在於從環境中徹底清除威脅的所有痕跡（例如刪除惡意軟件、修補漏洞）。
檔案完整性監控 (FIM)	一種安全流程或工具，用於監控關鍵系統及網站檔案，以偵測並警示任何未經授權的變更。
鑑識映像	儲存裝置的逐二進制數元精確副本，旨在保留受影響系統的狀態以供調查，同時不改變原始證據。
全磁碟加密	一種安全控制措施，會將裝置硬碟上的所有數據進行加密，若裝置遺失或遭竊，未經正確密碼驗證將無法讀取數據。
黃金映像	預先配置、安全且乾淨的作業系統及其應用程式範本，用於快速清除並重建遭入侵的系統。
不可變備份	一種以不可變更或刪除的方式儲存的備份，即使管理員也無法修改，能有效防禦針對備份的勒索軟體攻擊。
入侵指標 (IOCs)	用於識別潛在安全漏洞的鑑識數據片段，例如惡意 IP 位址、檔案雜湊值或網域名稱。
最小權限原則	一項安全概念，旨在確保使用者僅被授予執行其工作職能所需的最低權限。
惡意軟件	旨在破壞運作或未經授權存取電腦系統的惡意軟體，包括病毒、木馬、間諜軟體及鍵盤側錄程式。
流動裝置管理 (MDM)	一種軟體解決方案，可讓 IT 管理員集中控制、保護並在平板電腦和智慧型手機等行動裝置上執行政策。
多重認證 (MFA)	一種安全措施，要求使用者提供兩個或更多驗證因素才能取得存取權限，例如密碼和手機發送的驗證碼。
離線備份	儲存於未連網裝置或媒體上的備份副本，可防止資料在勒索軟體攻擊期間遭加密或刪除。
持久化機制	惡意軟件用以在系統重新啟動後自動重新啟動自身或維持存取權限的技術（例如建立排程工作或登錄檔項目）。
網路釣魚	一種社會工程學攻擊，攻擊者會發送一則偽造信息（通常是電子郵件），旨在誘使受害者透露敏感資訊或安裝惡意軟件。
實體數據外洩	因含有敏感或個人數據的實體裝置（如筆記型電腦）遺失或遭竊所導致的安全事件。
勒索軟體	一種惡意軟件，會將裝置上的檔案加密使其無法存取，並要求支付贖金以恢復存取權限。
流量限制	一種 DoS 緩解技術，用於控制特定時間段內來自單一來源的傳入流量，有助於降低洪水攻擊的影響。
復原	事件應變的階段，重點在於威脅被消除後，將系統與數據恢復至正常運作狀態。
補救性培訓	在發生安全事件後，為使用者提供的針對性輔助培訓，旨在強化最佳實務並防止事件重演。
遠端鎖定／清除	MDM 系統中的功能，允許管理員遠端鎖定遺失的裝置以防止存取，或永久清除裝置上的所有數據。
靜態維護頁面	當網站因維護而離線，或在遭遇篡改等事件時，向訪客顯示的簡單預先準備好的網頁。

網頁應用防火牆 (WAF)	一種安全工具，用於過濾和監控網頁應用程式與互聯網之間的 HTTP 流量，協助防禦常見的網路攻擊。
網站篡改	針對網站發動的攻擊，非法變更其視覺外觀，通常是將原始內容替換為攻擊者自己的信息或圖片。

1. 職責分工

1. 網路事件應變小組 (CIRT)

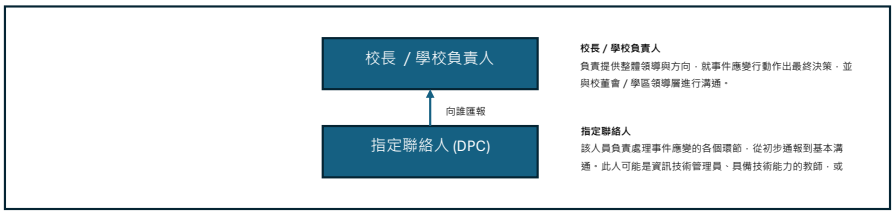
何謂 CIRT？
網路事件應變小組（CIRT）是由負責處理及應對網絡安全事件的成員所組成的團隊。在學校環境中，這類事件包括數據外洩、惡意軟件感染、釣魚攻擊、拒絕服務攻擊及其他網絡威脅。CIRT
的主要目標是將這些事件的影響降至最低，保護學生與教職員的數據，並確保教學活動的持續性。

為何 CIRT 對學校至關重要？
學校對科技的依賴日益增加，使其容易成為網路攻擊的目標。完善的 CIRT
架構能確保對事件做出協調且有效的應對，將中斷與損害降至最低。這同時也展現了對數據保安的承諾，並建立與學校社群之間的信任。

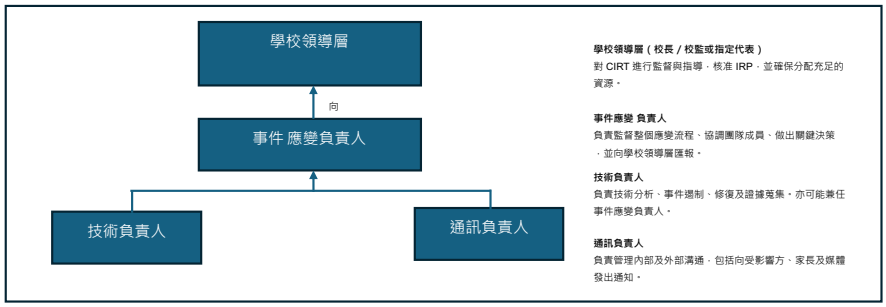
學校分級 CIRT 架構：

以下分級架構為學校提供了一個框架，使其能根據規模、資源及特定需求建立
CIRT。這些層級具備靈活性，讓學校能根據自身情況調整模式。

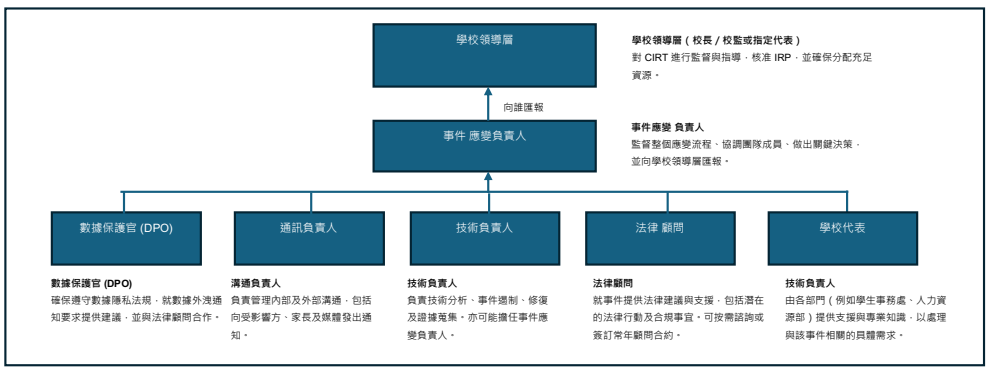
第一層級：簡化版學校 CIRT（小型學校／資源有限）



第 2 級：正規化學校 CIRT（較大規模學校／中等資源）



第三級：全面性學校 CIRT



實施 CIRT 架構：

1. 評估學校的需求與資源： 根據學校規模、預算及技術專業能力，確定最適合的層級。

2. 遴選並培訓 CIRT 成員： 挑選具備必要技能的人員，並針對事件應變程序提供適當的培訓。

3. 制定事件應變計畫 (IRP)： 一份完整的 IRP 應詳述發生網路事件時需採取的步驟，內容應包含角色與職責、通訊規範及技術程序。

4. 定期測試並更新 IRP： 進行演習與模擬，確保 CIRT 具備處理實際事件的準備。至少每年或視需要檢討並更新 IRP。

透過遵循這些步驟，學校可建立穩健的 CIRT
架構，有效保護其數據，並確保能對網路威脅做出迅速且協調的應對。這些資訊應與分層架構一併明確文件編製，並讓所有相關人員都能輕鬆取得。

1. 職責分工

2. CIRT 角色與職責

本表概述了校內電腦事件應變小組（CIRT）的關鍵角色與職責。以下所述的角色可根據各校的具體需求與資源進行適配。部分角色可合併，並可視需要借助外部專業資源。

此架構設計上具有可擴展性與適應性。資源有限的小型學校可整合職責，而較大的學校或學區則可能設有更專業化的職位。在事件發生*之前*明確界定這些職責至關重要，以確保能做出協調且有效的應對。

CIRT 職責	適用層級	職責	要求
學校領導層（校長／校務主任或指定代表）	1,2,3	為 CIRT 提供整體領導與方向。核准 IRP、分配資源，並與校董會／學區領導層溝通。	需具備學校營運、風險管理及數據保安；數據安全最佳實務之相關知識。
指定聯絡人 (DPC) / 事件應變負責人	1,2,3	負責監督整個事件應變流程、協調團隊成員、做出關鍵決策，並向學校領導層匯報。擔任對外機構的主要聯絡窗口。	具備強大的領導力、溝通能力及組織能力。熟悉網絡安全最佳實踐與事件應變框架。
技術負責人	2,3	負責技術層面：分析、遏制、根除、復原。管理技術人員／供應商。	具備網路安全、系統管理及資料復原的深厚技術專長。熟悉安全工具與技術。
溝通協調主管	2,3	制定並執行針對內部及外部利害關係人的溝通策略。負責媒體關係及公眾溝通。	具備出色的溝通與寫作能力。具備危機溝通與公共關係經驗。
數據保護官 (DPO)	3	確保符合數據隱私法規（如《個人資料保護條例》等）。就數據外洩通知提供建議。與法律顧問合作。	對數據隱私法律與法規有深入了解。具備數據治理與合規經驗。具法律背景者尤佳。
學校部門代表（例如：學生服務、人力資源、教學）	3	提供各部門的支援與專業知識，以應對事件相關的具體需求（例如：學生輔導、員工培訓、課程調整）。	熟悉所屬部門的職能及其與網絡安全事件的關聯性。具備與CIRT有效協作的能力。
法律顧問（視需要）	3	就事件提供法律建議／支援，包括潛在的法律行動／合規事宜。	具備數據隱私法、契約法、過失與責任等領域的專業知識。

2. 網路事件嚴重性等級分類

2.1. 事件嚴重性分類

CIR 經理應審查通報的安全事件並評估其嚴重性。以下為事件嚴重性等級分類與定義。

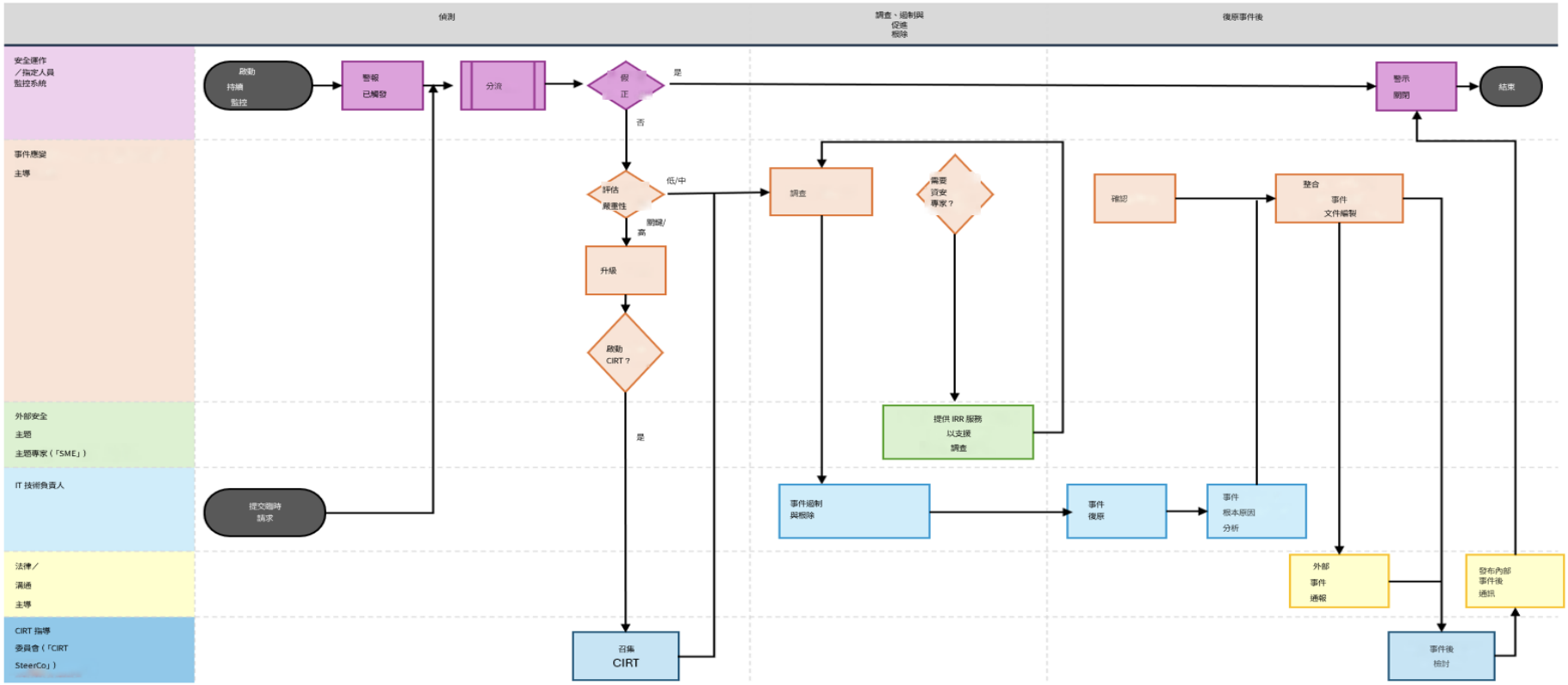
此分類係依據安全事件的 MITRE
類別，以及對本校關鍵資產的潛在風險和／或影響而定。同時亦會考量對運作造成的干擾，以及對本校資產機密性、完整性與可用性的影響。

嚴重性	**事件描述（範例）**	**潛在風險及／或影響**
關鍵	勒索軟體攻擊：關鍵系統遭加密且無法存取，影響學校基本運作。數據遭扣為人質。	- 教學、學習及行政功能遭受重大中斷。 因支付贖金及復原作業所導致的財務損失。 - 聲譽受損及信任流失。 - 法律與監管後果。
	重大數據外洩：大規模竊取敏感的學生或教職員數據，造成重大的法律與聲譽風險。	- 受影響個體面臨身分盜用與金融詐欺風險。 - 面臨法律及監管處罰。 - 聲譽受損及公眾信任流失。 - 需負擔信用監控及身分盜用修復服務相關費用。
	系統中斷（關鍵級）：核心系統完全無法使用，嚴重干擾學校運作。此情況可能源於針對性攻擊或災難性故障。	- 無法存取關鍵資訊系統（學生資訊、成績管理、通訊系統）。 - 課程取消或學校停課。 - 若緊急通知系統受影響，將產生安全與保安風險。 - 因生產力損失及復原成本所導致的財務損失。
高	惡意軟件感染（擴散中）：惡意軟件正在校內網路中積極擴散，可能危及多個系統。	- 數據遭失或損毀。 - 系統運行緩慢或當機。 - 感染擴散至其他連線網路。 - 干擾學校運作及學習活動。
	針對性入侵：有證據顯示黑客正積極鎖定學校系統，企圖取得敏感數據或干擾運作。	- 數據外洩及敏感資訊遭竊。 - 系統損壞或中斷。 - 聲譽受損及信任流失。 - 法律與法規層面的後果。
	系統中斷（重大）：重要系統無法使用，導致學校關鍵功能中斷。	- 特定學校功能中斷（例如：互聯網連線、電子郵件、圖書館系統）。 - 學生資訊或成績查詢受限。 - 通訊及行政任務延誤。 - 學生、教職員及家長感到沮喪與不便。
中度	**網路釣魚攻擊（成功）：** 憑證或敏感資訊已因網路釣魚攻擊而外洩。	- 學校系統與數據遭未經授權存取。 - 可能引發進一步攻擊（例如：惡意軟件安裝、數據外洩）。 - 遭入侵的帳戶被用於發送垃圾郵件或釣魚郵件。 - 若遭入侵的帳戶被用於惡意目的，將造成聲譽損害。
	未經授權存取（有限）：有證據顯示特定系統或帳戶遭未經授權存取，但無跡象顯示存在廣泛的系統遭入侵。	- 可能導致數據外洩或系統損壞。 - 需調查未經授權存取的範圍。 - 需加強安全措施以防止未來發生類似事件。
	安全性設定錯誤：因系統設定錯誤而發現安全漏洞。	- 網路攻擊與數據外洩的風險增加。 - 系統不穩定或出現異常行為。 - 需重新配置系統以解決該漏洞。
低	可疑活動：已觀察到異常活動，但尚不確定是否構成真實威脅。	潛在安全漏洞 - 可能顯示為攻擊或惡意活動的初期階段。 - 資源濫用：未經授權將學校電腦或電腦網絡用於非教育目的。 違反《合理使用政策》：學生或教職員從事禁止的線上活動。
	安全警報（誤報）：安全系統觸發警報，經調查後證實為無害事件。	- 掉以輕心：反覆出現的誤報可能導致未來忽略警報，進而錯失真正的威脅。 - 調查過程耗費時間與資源。 - 可能造成不必要的壓力與干擾。 - 可能表示需要微調安全系統以減少誤報。

3. 事件應變程序

3.1. 事件應變流程圖

僅供說明之用



#	事件類型 負責方	A. 準備階段	B. 偵測與分析階段	C. 隔離	D. 根除與復原	E. 事件後處理
		事故管理負責人（例如：校長／業務經理）、技術負責人（例如：IT 協調員）、通訊負責人（例如：辦公室經理）	IT 人員／全體教職員與學生（作為通報者）	技術負責人、事件應變負責人	技術負責人	事件應變負責人、技術負責人、通訊負責人
1	勒索軟體攻擊	1. 建立/維護 CIRT：組建核心網路事件應變小組 (CIRT)，並明確界定各成員職責。 2. 備份：對所有關鍵數據進行定期自動備份。至關重要的是，確保至少有一份備份處於離線/物理隔離狀態且不可變更。 3. 測試備份：定期測試數據還原功能，以確保備份有效。 4. 工具：部署並維護端點偵測與回應（EDR）或強大的防毒解決方案。使用電子郵件過濾功能阻擋惡意附件。 5. 培訓：培訓員工識別釣魚郵件和可疑連結，因為這	1. 初步偵測：收到檔案無法存取、出現新檔案副檔名、贖金通知出現在螢幕上，或防毒軟體針對勒索軟體活動發出警示的通報。 2. 分析：確認事件屬勒索軟體攻擊。釐清影響範圍（哪些系統/伺服器受到影響？）。若可行，利用 EDR/防毒軟體日誌找出最初的入侵點。切勿點擊贖金通知中的任何連結。	1. 立即隔離：將受影響的裝置從學校網路中斷開（拔除以太網線、停用 Wi-Fi）。請勿關閉裝置電源，以免遺失寶貴的鑑識數據。 2. 分割網路：若攻擊範圍廣泛，應考慮將整個網路區段（例如學生網路）或整個學校網路下線，以防止進一步擴散。 3. 停用帳戶：停用與初始感染相關的用戶帳戶。作為預防措施，請變更所有管理員及服務帳戶的密碼。	1. 諮詢專家：通知您的 IT 服務供應商或網絡安全專家。切勿嘗試支付贖金（此為 NCSC/ACSC 的建議）。 2. 徹底清除：將所有受影響的系統格式化，並從已知安全的「黃金映像」重新建立系統映像。切勿僅執行防毒掃描。 3. 還原：從最新、經過測試且乾淨的離線備份中還原數據。確保備份時間早於初始感染時間（「潛伏期」）。 4. 修補：識別並修補導致攻擊的漏洞（例如：未修補的軟體、弱 RDP 憑證）。	1. 通報：向相關主管機關通報事件（例如：警方、英國的 Action Fraud/NCSC、澳洲的 ReportCyber）。 2. 評估資料外洩：確認個人資料是否遭存取或外洩。若屬實，須向數據保護主管機關（例如英國資訊專員辦公室（ICO）、澳洲資訊專員辦公室（OAIC））通報，並依規定通知受影響者（家長／教職員）。 3. 經驗教訓：進行事後檢討，以找出安全控制措施的弱點並改善應變計畫。
2	網路釣魚與惡意軟件感染	1. 技術控制措施：實施強效的電子郵件過濾（反垃圾郵件、反釣魚）。使用最新的端點防毒/反惡意軟件。透過 DNS 過濾阻擋已知的惡意網站。 2. 使用者培訓：針對全體員工定期舉辦強制性的網絡安全意識培訓，重點在於識別的魚攻擊。 3. 通報流程：建立簡單明確的流程，供使用者通報可疑的釣魚電子郵件（例如轉寄至特定的 IT 電子郵件地址）。 4. 最小權限原則：確保使用者僅擁有其職務所需的存	1. 初步偵測：使用者通報收到可疑電子郵件、點擊連結或開啟附件。防毒軟體發出威脅警示。裝置開始出現異常行為（運作緩慢、彈出視窗）。 2. 分析：IT 團隊在不點擊連結的情況下，檢視通報電子郵件的標頭與內容。他們分析防毒警示中的惡意軟件簽名，以了解其性質（例如：鍵盤側錄程式、資訊竊取程式、木馬）。	1. 隔離裝置：立即將用戶裝置從網路中斷開。 2. 重設憑證：強制重設受影響用戶帳戶的密碼，因其憑證可能已遭洩露。 3. 封鎖指標：在網路防火牆或電子郵件通訊閘處，封鎖發件人的電子郵件地址，以及釣魚郵件中發現的任何惡意網域/IP。 4. 掃描郵箱：搜尋所有學校郵箱中是否存在其他相同的釣魚郵件，並集中刪除。	1. 根除：使用信譽良好的防毒/反惡意軟件工具執行完整系統掃描。對於高風險感染（如憑證竊取程式），最安全的做法是清除裝置並重新建立映像。 2. 驗證完整性：檢查裝置是否存在惡意軟件可能安裝的持久化機制（例如：排程任務、登錄檔變更）。 3. 恢復：如有必要，從乾淨的備份中還原任何損毀或遺失的用戶資料。將已清理/重建的裝置重新連線至網路。	1. 溝通：向全體員工發送警示，說明釣魚攻擊的詳細資訊（例如：主旨、寄件者），並提醒他們切勿與之互動。 2. 檢討：分析釣魚郵件為何能繞過過濾機制，並在可能的情況下調整規則。 3. 針對性培訓：將此事件作為未來培訓的實際案例。應對通報此事件的使用者給予正面肯定。若使用者上當受騙，應提供支持性及補救性培訓。
3	裝置遺失或遭竊	1. 資產清查：維持所有學校所有設備（筆記型電腦、平板電腦）的準確清單。 2. 技術控制：強制所有攜帶式裝置實施全磁碟加密（例如 Windows 的 BitLocker、macOS 的 FileVault）。 3. 流動裝置管理：將所有行動裝置註冊至具備遠端鎖定與資料清除功能的流動裝置管理解決方案中。 4. 政策與培訓：制定明確政策，要求教職員與學生立即通報裝置遺失或遭竊。並針對此程序進行培訓。	1. 初步偵測：教職員或學生通報其校發設備遺失或遭竊。 2. 分析：立即透過資產清單確認使用者身分及遺失設備的詳細資訊。判定設備上可能存有何種數據（例如：學生紀錄、敏感電子郵件），以及數據是否經過加密。	1. 遠端鎖定/清除：立即使用 MDM 解決方案對裝置觸發遠端鎖定，以防止存取。若裝置難以尋回或含有高度敏感數據，則觸發遠端清除。 2. 撤銷存取權限：暫時停用使用者的學校帳戶，以防止其存取雲端服務（電子郵件、共用磁碟）。 3. 變更密碼：強制使用者重設密碼。	1. 清除：執行遠端清除操作，以刪除遺失裝置上的數據。在資產清單中將該裝置標記為「遺失/遭竊」。 2. 恢復：為使用者配置一台新的、安全的裝置。將其數據從雲端服務或備份還原至新裝置。重新啟用其學校帳戶。	1. 向警方報案：若裝置遭竊，應建議使用者向警方報案並取得案件編號。 2. 評估資料外洩：此屬實體資料外洩事件。若裝置未加密且含有個人資料，則屬須通報之事件。應依法通知數據保護主管機關（ICO/OAIC）及受影響之個人。 3. 檢視政策：檢視實體安全與裝置處理政策，評估是否有改進空間。
4	意外數據外洩	1. 數據分類：建立簡單的數據分類政策（例如：公開、內部、機密性），並對教職員進行相關培訓。 2. 培訓：針對常見錯誤對教職員進行培訓，例如不當使用「回覆所有人」、將電子郵件寄送給錯誤的收件者，或錯誤設定檔案共享權限。 3. DLP 工具：若條件許可，請在電子郵件系統中實施基礎的資料外洩防護 (DLP) 規則，在使用者將含有敏感關鍵字（例如「學生證號」）的電子郵件發送至校外之前發出警告。	1. 初步偵測：使用者主動通報誤將含敏感數據的電子郵件寄給錯誤對象，或收件者通知學校誤收數據。 2. 分析：迅速核實事件。精確辨識外洩的數據內容、收件對象（內部／外部），以及數據的敏感程度。	1. 嘗試撤回：立即嘗試撤回該電子郵件（需知此舉未必總是有效，特別是針對外部收件人）。 2. 聯繫收件者：透過電話或另發電子郵件聯繫非預期收件者，說明錯誤原因，並正式要求對方刪除相關資訊，並以書面形式確認已刪除。 3. 撤銷存取權限：若資料是透過雲端連結（例如 SharePoint、Google Drive）分享的，請立即撤銷該檔案或資料夾的存取權限。	1. 清除：當您收到非預期收件者已刪除數據的確認通知時，即視為已完成清除。請將此確認記錄在案。 2. 恢復：無需進行技術性恢復。重點在於程序性恢復：確保原始數據的安全，並讓使用者了解此錯誤。	1. 評估數據外洩：此屬數據外洩事件。事件負責人必須評估數據遭洩露之個人所面臨的危害風險。 2. 通報：根據風險評估結果，若事件符合強制通報門檻，應向數據保護主管機關（ICO/OAIC）通報此數據外洩事件。 3. 通知：向受影響的個人（或其家長）說明數據外洩事件、潛在影響，以及為減輕影響所採取的措施。 4. 培訓：針對涉事員工提供補救性培訓，並將匿名化情境納入更廣泛的員工培訓中。
5	網站篡改	1. 安全存取：強制要求所有網站管理員帳戶使用強效且唯一的密碼，並啟用多重認證（MFA）。限制管理員帳戶的數量。 2. 修補程式：確保網站的內容管理系統（CMS）、佈景主題及外掛程式隨時保持最新修補狀態並完成更新。 3. 備份：定期自動備份網站檔案與數據庫，並將備份儲存於與網頁伺服器分開的位置。 4. 監控：使用檔案完整性監控服務，以偵測網站檔案的未經授權變更並發出警示。	1. 初步偵測：學校透過教職員、學生、家長通報，或透過網站監控系統發現網站內容遭篡改，出現未經授權的信息或圖片。 2. 分析：確認網站遭篡改。擷取螢幕截圖作為證據。檢查伺服器日誌，以識別篡改發生時段周邊的可疑 IP 位址或活動。	1. 將網站下線：立即將網站下線，並替換為預先準備好的靜態維護頁面（例如：「本網站暫時無法使用。我們正在努力盡快恢復服務。」）。此舉可防止聲譽進一步受損。 2. 保存證據：在進行任何變更之前，對遭篡改的網站進行完整備份/快照，以供日後調查之用。	1. 識別漏洞：分析日誌與檔案，找進入點（例如：存在漏洞的外掛程式、遭竊的密碼）。 2. 根除與恢復：從伺服器刪除所有網站檔案。從最近一次已知無惡的備份中還原網站檔案與數據庫。切勿僅嘗試編輯遭篡改的頁面。 3. 強化安全：變更所有管理、數據庫及 FTP 密碼。針對遭利用的漏洞套用修補程式。掃描已還原的網站，檢查是否殘留後門。 4. 恢復上線：確認安全無虞後，將還原的網站重新上線。	1. 檢討：針對該事件進行檢討，以確認根本原因。 2. 強化安全：根據檢討結果實施額外安全措施，例如部署網路應用程式防火牆（WAF）或實施更嚴格的存取控制。 3. 溝通：告知學校社群（如有必要），說明網站問題已解決且安全性已獲得強化。
6	拒絕服務 (DoS) 攻擊	1. 了解您的服務供應商：隨時備妥您的互聯網服務供應商（ISP）及網站主機供應商的 24/7 技術支援聯絡資訊。 2. 使用防護服務：針對學校網站等關鍵服務，應採用具備 DDoS 緩解功能的雲端 DNS/代理服務（例如 Cloudflare）。 3. 可擴展的託管服務：將關鍵服務主機於能隨流量小幅激增而自動擴展的平台。 4. 網路監控：建立基本的網路流量監控機制，以識別異常流量激增。	1. 初步偵測：接獲通報指學校網站、學習平台或整個互聯網連線離線，或速度慢到無法使用。監控工具顯示入站網路流量極高。 2. 分析：區分一般性中斷與 DoS 攻擊。DoS 攻擊的特徵是來自眾多（DDoS）或少量（DoS）來源的大量持續流量，導致伺服器或網路鏈路不堪負荷。	1. 聯絡服務供應商：這是最關鍵的一步。立即聯絡您的網際網路服務供應商（ISP）或網站主機服務商。告知對方您懷疑正遭受 DoS 攻擊。他們擁有網路層級的工具來緩解攻擊（例如「黑洞化」流量、流量限制）。 2. 啟用緩解措施：若您使用 Cloudflare 等服務，請啟用其「I'm Under Attack」形式。 3. 內部通報：告知員工關鍵服務因疑似網路攻擊而中斷，並說明您正與服務供應商合作解決問題。	1. 與服務供應商合作：供應商將透過過濾惡意流量來執行清除作業。您的角色是監控服務狀態。 2. 恢復：隨著供應商的緩解措施生效，服務將逐漸恢復可用性。測試關鍵服務（網站、電子郵件）以確認其運作正常。	1. 攻擊後分析：與服務供應商進行事後檢討，以了解攻擊的性質與規模。 2. 落實建議：實施服務供應商提出的任何安全建議，以更好地抵禦未來的攻擊。 . 通報：通知學校社群服務已恢復。通常無需明確指出原因為 DoS 攻擊；僅表示「技術問題」或「網路中斷」往往已足夠。

附錄 - 啟動 CIRT 的標準／考量因素

本表提供一般性準則，用以評估何時應啟動學校的事件應變計畫，並可能尋求外部支援。各校必須根據其具體情況、資源及風險承受能力，調整這些準則。建議諮詢法律顧問及資訊科技專業人員。

關鍵因素	
影響範圍	**學校是否為唯一受影響方？** 除非攻擊目標是共享服務供應商，否則可能性極高。需進行調查以確認。 **有多少系統或使用者受到影響？** 單一遭入侵的帳戶與廣泛感染，所需採取的應對措施不同。 **涉及何種數據類型？** 敏感學生數據外洩需採取更高層級的應對措施。
潛在後果	**財務影響：** 復原成本、數據外洩的潛在罰款（視當地法規而定），以及教育服務中斷。 **營運影響：** 教學、學習、行政任務及通訊中斷。 **聲譽影響：** 損害學校形象及公眾信任。
對利害關係人的影響	**教職員與教師：** 課程規劃、評分、溝通受阻，以及工作量增加。 **學生：** 學習進度、資源存取及評分作業受阻。 **合作機構：** 對依賴共享系統的其他學校、圖書館或組織造成影響。 **家長：** 擔憂情緒及溝通需求。
法律與法規義務	**數據外洩通報法規：** 確認事件是否觸發強制通報要求。 **合約與協議：** 檢視相關合約中的事件應變義務。 **學校政策：** 確保符合內部政策與程序。

附錄 – 網路事件應變小組聯絡名單

請在此聯絡名單中填寫事件應變小組所有成員的姓名、職務及聯絡資訊。此名單應在發生事件時能立即取得，並定期更新。

職務	姓名	主要電話	備用電話	電子郵件
指定聯絡人（第 1 級）／事件應變負責人（第 2/3 級）				
技術負責人（第 2/3 級）				
通訊負責人（第 2/3 級）				
IT 管理員／支援人員				
校長／督學				
外部 IT 服務供應商				
執法單位（非緊急情況）				
法律顧問（如適用）				
[其他 - 自訂]				

附錄 - 監管及執法聯絡資訊

	何時應通報	**聯絡方式**
香港電腦緊急事故應變小組（HKCERT）	- 若事件屬針對學校的潛在多點攻擊	電話：8105 6060，傳真：8105 9760 電郵地址：hkcert@hkcert.org 網上表格：https://www.hkcert.org/form/incident-report-end-user-sme/entry
學校是否是受此問題或事件影響的唯一一方？	可能性極高，除非該攻擊是針對多家學校共同使用的服務供應商。這需要進一步調查。	電話：2860 5012 電子舉報中心：https://www.police.gov.hk/ppp_en/contact_us.html
個人資料私隱專員公署 (PCPD)	- 若學生、教職員或家長的個人數據外洩 - 特別是若該外洩事件可能對受影響人士造成傷害或困擾	若個人資料涉及安全事件，各局／部門應盡快透過個人資料私隱專員公署網站（https://www.pcpd.org.hk/english/resources_centre/publications/forms/files/DBN_e.pdf）提供的資料外洩通報表格，向公署通報該個案。 該數據外洩通報表格亦可透過個人資料私隱專員公署網站（https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn_form.html）以線上方式提交。

附錄 - 事件處理表格

I. 一般資訊			
事件處理人員資訊			
學校是否是受此問題或事件影響的		地點：	
職稱：		部門：	
辦公室／手機號碼：		事件日期/時間：	
對教職員的影響			
姓名：		日期／時間：	
職稱：		辦公室／手機號碼：	
II. 事件詳情			
事件類型：	☐ 數據外洩 ☐ 網站篡改 ☐ 釣魚攻擊 ☐ 勒索軟體攻擊 ☐ 分散 / 分布式阻斷服務攻擊 (DDOS) ☐ 系統遭入侵／運作受損 ☐ 其他：_____		
事件描述／發現事項／已採取行動：			
涉及數據：	☐ 個人數據（教職員／學生） ☐ 營運數據 ☐ 其他 ☐ 無		
估計受影響的遭洩露紀錄數：	☐ >1,000 行 ☐ <1,000 至 >500 行 ☐ <500 至 >100 行 ☐ <100 行 ☐ 若已知確切數值：_____ ☐ 無		
受影響使用者數／數據量（GB）估計值：	☐ >5,000 ☐ <5,000 至 >500 ☐ <500 ☐ 若已知確切數值：_____ ☐ 無		

受影響教職員／學生名單：

#	姓名	部門／地點	聯絡人	備註

觀察到的影響：	☐ 財務影響 ☐ 聲譽影響 ☐ 法律／法規遵循影響 ☐ 營運影響 ☐ 其他：_____
影響詳情及潛在風險：	
III. 後續行動	
已採取的後續行動（如有）：	
是否需要外部專業協助？	☐ 是 ☐ 否
首選外部專家（如有）	

附錄 A – 行動紀錄

#	行動／事項	負責方	日期/時間	狀態

附錄 – 事件後評估

事後評估表			
事件參考編號：		評估日期/時間： (時:分 DD/MMM/YYYY)	
事件聲明： (時:分 DD/MMM/YYYY)		事件結束時間： (時:分 DD/MMM/YYYY)	
對教職員的影響	該事件可能干擾教師的課程規劃、評分及溝通。行政人員可能因復原工作而面臨工作量大幅增加。薪資發放亦可能受到影響。 學生可能面臨學習、資源存取及成績評分中斷。依賴共享系統的合作機構（例如：其他學校、圖書館）亦可能受到影響。家長可能會感到擔憂並需要相關溝通。 ☐ 業務系統遭入侵／運作受損 ☐ 其他：_____		
事件描述：			
I. 一般資訊			
通報單位資訊			
姓名：		地點：	
職稱：		部門：	
辦公室／手機號碼：		電子郵件：	
II. 評估詳情			
a. 事件應變 (IR) 程序			
遵循的 IR 程序：	☐ 是 ☐ 否 若為否，偏離原因：		
已採取之額外措施：	☐ 是 若為是，請列出已採取的措施： ☐ 否		
b. 偵測、遏制、根除效率			
所需資訊能否及時可用：	☐ 是 ☐ 否 若為「否」，請說明缺漏內容及延遲原因：		
所需資源的可用性：	☐ 是 ☐ 否 若為否，請說明缺失項目及無法及時提供之原因：		
所需任務是否如期完成：	☐ 是 ☐ 否 若為否，請說明哪些任務及延遲原因：		
是否聘請外部專家：	☐ 是 若為是，請說明專業領域及供應商名稱： ☐ 否		
c. 營運恢復			
營運能力是否已如期恢復：	☐ 是 ☐ 否 若為否，延遲原因：		
d. 事件分析			
是否已進行根本原因分析：	☐ 是 若為是，請列出根本原因： ☐ 否		
已識別必要的矯正措施：	☐ 是 若為是，請列出將採取的矯正措施、負責人及時程： ☐ 否		
已識別監控控制改善措施：	☐ 是 若為是，請說明針對類似事件應如何改進： ☐ 否		
建議採購之額外工具：	☐ 是 若為是，請列出相關工具： ☐ 否		
e. 政策與程序			
需更新應變手冊：	☐ 是 若為是，請列出需更新的範疇及原因： ☐ 否		
其他政策與程序需更新：	☐ 是 若為是，請列出相關政策／程序及原因： ☐ 否		
f. 其他意見			
III. 改善路線圖			
立竿見影的改善措施（立即實施）			
短期（3 個月）			
長期（6 個月）			

附錄 - 依據事件嚴重性等級的升級處理程序（參考）

本表格僅供一般參考，必須根據各校的具體情況、資源及組織架構進行調整。使用本表格前，請先審閱並加以客製化，以反映貴校的具體情境。
請確保所有佔位角色（[角色/職稱]）均已明確界定，並已指派相關人員承擔責任。

嚴重性	事件描述	升級程序
關鍵	**勒索軟體攻擊：** 關鍵系統遭加密且無法存取，影響學校基本運作。數據遭扣為人質。 **重大資料外洩：** 大規模竊取學生或教職員的敏感數據，造成重大的法律與聲譽風險。 **系統中斷（嚴重）：** 關鍵系統完全無法使用，嚴重干擾學校運作。此情況可能源於針對性攻擊或災難性故障。	**立即向 [校董會/管理機構/教育總監] 及法律顧問升級通報。** - 啟動學校的事件應變計畫。 - 聘請外部網絡安全專家並聯繫執法機關。 - 與受影響方（學生、家長、教職員）保持透明溝通。
高	**惡意軟件感染（擴散中）：** 惡意軟件正在校內網路中積極擴散，可能危及多個系統。 **針對性入侵：** 有證據顯示黑客正積極鎖定學校系統，企圖取得敏感資料或干擾運作。 **系統中斷（重大）：** 重要系統無法使用，導致學校關鍵功能受阻。	- 向 [指定高級管理員/校長] 升級通報。 - 啟動學校的事件應變計畫。 - 調查事件的範圍與影響。 - 考慮聘請外部網絡安全專家。
中度	**釣魚攻擊（成功）：** 憑證或敏感資訊已因釣魚攻擊而外洩。 **未經授權存取（有限）：** 有證據顯示特定系統或帳戶遭未經授權存取，但無跡象顯示已造成廣泛損害。 **安全性設定錯誤：** 因系統設定錯誤而發現安全性漏洞。	- 向指定的事件應變負責人（[職稱/職位]）通報。 - 調查事件並控制潛在影響。 - 實施矯正措施並進行文件編製。
低	**可疑活動：** 觀察到異常活動，但尚無法確定是否構成真實威脅。 **安全警報（誤報）：** 安全系統觸發警報，經調查後證實為無害。	**記錄事件並通知事件應變負責人。** - 評估風險並決定是否需要採取進一步行動。

第四部份：

網絡安全配置建議清單

類別	檢查清單項目	優先級	說明	指引 / 範例	參考	實施狀況
架構與基礎設施	DMZ	高	Web 伺服器是否位於 DMZ 內，並與內部網路隔離？	**DMZ 實施：** 將學校的網頁伺服器置於 DMZ 內，使其與儲存學生資訊及其他敏感資訊的內部數據網絡隔離。此舉可限制網頁伺服器遭入侵時可能造成的影響。 **防火牆規則：** 配置防火牆規則以限制 DMZ、內部網路與互聯網之間的流量。僅允許必要的流量（例如 HTTP/HTTPS）從互聯網傳輸至網頁伺服器。 **範例：** 若學校使用簡易型防火牆設備，請配置其為 DMZ 建立獨立的網路區域，並套用適當的存取控制規則。	8.1.1 (a)	
架構與基礎設施	防火牆多樣性	中等	內部網路與外部網路是否使用不同廠商或類型的防火牆？	**防火牆多樣性：** 若可行（且在預算範圍內），應針對內部與外部網路邊界分別採用不同廠商或不同技術的防火牆。此舉可降低單一漏洞同時影響兩套防火牆的風險。 **範例：** 外部邊界採用硬件防火牆設備，內部網路則採用軟體防火牆。	8.1.1 (a)	
架構與基礎設施	NIDS/NIPS	高	是否已部署並定期更新網路入侵偵測/防禦系統？	**NIDS/NIPS 部署：** 部署網路入侵偵測系統 (NIDS) 或網路入侵防禦系統 (NIPS)，以監控網路流量中的惡意活動。 **簽名檔更新：** 保持 NIDS/NIPS 簽名檔最新，以偵測最新威脅。 **範例：** 若預算有限，可考慮 Snort 或 Suricata 等開源 NIDS/NIPS 解決方案。針對可疑活動配置警示。	8.1.1 (b)	
架構與基礎設施	WAF	高	是否已部署 Web 應用程式防火牆 (WAF)？	**WAF 部署：** 部署 WAF 以保護 Web 伺服器免受常見的 Web 應用程式攻擊，例如 SQL 注入、跨站腳本 (XSS) 及跨站請求偽造 (CSRF)。 **雲端型 WAF：** 雲端型 WAF 解決方案對中小企業及學校而言，可作為一種具成本效益的選擇。 **範例：** 可考慮使用雲端型 WAF 服務，例如 Cloudflare 或 AWS WAF。	8.1.1 (b)	
架構與基礎設施	防 DDoS	高	是否已實施防 DDoS 措施？	**DDoS 防護服務：** 建議訂閱 DDoS 防護服務，以緩解流量型 DDoS 攻擊。 **速率限制：** 在網頁伺服器上實施速率限制，以限制單一 IP 位址的請求數量。 **範例：** Cloudflare 將 DDoS 防護納入其服務範疇。若需基本速率限制，請配置網頁伺服器（例如，在 Apache 中使用 *mod_evasive*）。	8.1.1 (b)、8.7	
架構與基礎設施	防火牆配置	高	防火牆配置是否定期檢視與更新？	**預設拒絕：** 在防火牆規則集的最末端實施「預設拒絕」（或「隱含拒絕」）政策。這意味著除非防火牆規則明確允許，否則所有流量均被阻擋。此舉可顯著縮小攻擊面。 **最小權限原則：** 僅允許必要最低限度流量通過防火牆。依據來源 IP、目的地 IP、埠號及通訊協定來限制存取。**防火牆規則審查：** 定期（例如每季）審查並更新防火牆規則，以確保其仍具適切性與有效性。移除任何不必要的規則（例如：當僅需 HTTP 和 HTTPS 時，卻允許所有埠的流量傳輸至伺服器的規則；或是因所針對的系統或服務已不再使用，而變得不再需要的規則）。 **文件編製防火牆規則：** 針對所有防火牆規則建立清晰的文件編製，包含其目的與依據。 **範例：** 針對位於 DMZ 中的學校網頁伺服器，僅允許來自互聯網的 HTTP/HTTPS（80/443 埠）流量。封鎖所有其他進入 DMZ 的流量。同樣地，限制從 DMZ 傳往內部網路的流量，僅允許必要的連線。	-	
Web 伺服器安全性	安全配置	高	網頁伺服器是否已安全配置？	**停用目錄列出功能：** 防止瀏覽網站檔案。範例：在 Apache 中，於 .htaccess 檔案中設定 *Options -Indexes*。 **自訂錯誤頁面：** 提供通用誤差信息，而非揭露伺服器詳細資訊。 **保護配置檔（Apache/Nginx）：** 透過檔案系統權限（例如 chmod 640）限制對 httpd.conf、nginx.conf 等檔案的存取。	8.2.3 (b)	
Web 伺服器安全性	最小權限原則	高	程序是否以最低權限運行？	**網頁伺服器使用者：** 以專用使用者帳戶（例如 www-data、apache 等）執行 Apache/Nginx，並限制其系統權限。 **數據庫存取：** 為網頁應用程式建立專屬的數據庫使用者，並僅授予必要的權限（例如針對特定資料表的 SELECT、INSERT、UPDATE 權限）。**避免使用 root 數據庫帳戶。**	8.2.3 (c)	
Web 伺服器安全性	修補程式	高	是否及時套用安全性修補程式？	**作業系統與網頁伺服器修補：** 定期修補作業系統（Windows Server、Linux 發行版）及網頁伺服器軟體（Apache、Nginx）。 **修補程式部署優先級範例：** - 關鍵級（CVSS 9.0-10.0）：立即修補（24-48 小時內）。 - 高危 (CVSS 7.0-8.9)：1-2 週內修補。 - 中等 (CVSS 4.0-6.9)：1-3 個月內修補。 - 低危 (CVSS 0.0-3.9)：作為例行維護週期的一部分進行修補。 **在預備伺服器上測試修補程式：** 在將修補程式套用至正式伺服器之前，請先在預備或開發伺服器上進行測試，以確保相容性。 **訂閱安全郵件列表以接收漏洞通知。**	8.2.3 (d)	
Web 伺服器安全性	存取控制	中等	存取權限是否已嚴格配置？	**學生入口網站：** 使用強認證機制（例如：使用者名稱與密碼，若可行則採用多因素驗證）以保護學生數據。 **管理界面：** 將管理界面（例如：網頁伺服器控制台、內容管理系統）的存取權限限制為僅限授權人員。使用強密碼並考慮採用多因素驗證。	8.2.3 (e)	
Web 伺服器安全性	帳戶管理	中等	未使用帳戶是否已停用/刪除？	**學生帳戶：** 當學生離校時，應停用或刪除其帳戶。 **職員帳戶：** 當職員離職時，應停用或刪除其帳戶。	8.2.3 (f)	
Web 伺服器安全性	密碼保護	高	密碼是否已安全儲存（經雜湊處理 / 加密）？	**採用強密碼政策：** 針對學生與教職員： – 最小長度：8 個字符 – 複雜度：須包含大寫字母、小寫字母、數字及符號。 – 密碼重複使用：禁止重複使用最近 5 組密碼。 – 密碼到期：考慮每 90 至 180 天讓密碼到期。 針對管理員： – 最小長度：15 個字符 – 複雜度：必須包含大寫字母、小寫字母、數字及符號，並考慮使用密語。 – 密碼重複使用：禁止重複使用最近 10 組密碼。 – 密碼到期：每 60 至 90 天讓密碼失效。 **多重認證 (MFA)：** 在可行情況下，強制要求所有管理員帳戶啟用 MFA。 **禁止使用常見密碼及字典單字** （例如：「password」、「123456」、「qwerty」、「schoolname」、「mascot」、學生姓名、教師姓名、與學校相關的詞彙）。**使用**包含字典詞彙檢測功能的**黑名單或密碼強度檢查工具**。 **密碼雜湊：** 若進行自訂應用系統發展，請確保使用 bcrypt 或 Argon2 等強效算法，並搭配唯一鹽值對密碼進行雜湊處理。 **密碼管理工具：** 鼓勵學生、教職員及管理員使用信譽良好的密碼管理工具。	8.2.3 (g)	

Web 伺服器安全性	HIDS/HIPS	中等	網頁伺服器上是否已安裝 HIDS/HIPS？	**若預算有限，可考慮開源選項：** OSSEC、Fail2ban 能提供基本的入侵偵測與防禦功能。 **與現有安全工具整合：** 若學校或中小企業已配備防火牆或安全資訊與事件管理（SIEM）系統，應將網頁伺服器的日誌與警示進行整合。	8.2.3 (h)	
Web 伺服器安全性	日誌檢視	中等	是否定期檢視安全日誌？	**定期檢查日誌：** 指定一名工作人員，至少每週檢視一次網頁伺服器日誌（存取日誌、錯誤日誌）。留意異常活動，例如登入失敗、來自陌生 IP 位址的存取，或大量檔案下載。 **自動化日誌分析：**若可行，請使用日誌分析工具（例如：GoAccess 進行簡單的網頁日誌分析，或使用 SIEM 進行更全面的記錄管理），以協助識別可疑模式。	8.2.3 (i)、8.3.1	
Web 伺服器安全性	資訊洩露	高	敏感的配置資訊是否受到保護？	**伺服器版本：** 停用 HTTP 回應中的網頁伺服器版本標示。範例：在 Apache 中，設定 *ServerTokens Prod* 及 *ServerSignature Off*。 **誤差信息：** 配置網頁伺服器向使用者顯示通用誤差信息，避免揭露詳細的內部錯誤資訊。	8.2.3 (j)	
Web 伺服器安全性	模組管理	中等	是否已停用/移除不必要的模組？	**範例（Apache）：** 停用未使用之模組，例如 *mod_dav*、*mod_cgi* ，或其他對學校網站功能非必要之模組。此舉可降低潛在漏洞。 **定期檢視模組：** 定期檢視已啟用之模組，並停用任何不再需要之模組。	8.2.3 (k)	
Web 伺服器安全性	服務最小化	中等	是否已停用未使用之服務 / 連接埠？	**範例：** 若網頁伺服器僅用於主機學校網站，請停用不必要的服務，例如 FTP、SSH（若非用於遠端管理）或其他未使用之網路服務。此操作可透過作業系統的服務管理工具執行（例如 Windows 上的 services.msc、Linux 上的 systemd）。	8.2.3 (l)	
Web 伺服器安全性	預設檔案	中等	是否已移除預設/範例檔案？	**範例：** 安裝網頁伺服器或內容管理系統 (CMS) 後，請移除學校網站不需要的預設安裝檔案、測試腳本及範例頁面。這些檔案通常含有已知的漏洞。	8.2.3 (m)	
Web 伺服器安全性	網頁爬蟲限制	中等	是否對敏感內容的網頁爬取進行了限制？	**學生目錄 / 入口網站：** 使用 *robots.txt* 檔案，防止搜尋引擎索引包含學生資料或校內內部資源的頁面。 **教職員內部資源：** 透過存取控制（例如：密碼保護、IP 位址限制）限制網站中僅限教職員瀏覽的區塊，並使用 *robots.txt* 檔案防止其被索引。	8.2.3 (n)	
Web 伺服器安全性	檔案保護	高	重要檔案是否受到保護？	**配置檔：** 透過適當的檔案系統權限（例如在 Linux/Unix 系統上設定 chmod 640）來保護網頁伺服器配置檔（例如 *httpd.conf*、*nginx.conf*）及 *.htaccess* *檔案*，以防止未經授權的修改。 **數據庫備份：** 將數據庫備份儲存於安全位置，最好是離線儲存，若備份內容包含敏感數據，則應進行加密。	8.2.3 (o)	
Web 伺服器安全性	SSL/TLS 憑證管理	高	私密金鑰是否已安全備份並受到保護？	**SSL 憑證與金鑰儲存：** 應安全儲存 SSL 憑證與私密金鑰，最好離線儲存，或若具備條件則存放於硬件安全模組 (HSM) 中。 **備份：** 應維持 SSL 憑證與金鑰的安全備份。這些備份對於在伺服器故障或遭入侵時恢復 HTTPS 功能至關重要。	8.2.3 (p)	
Web 伺服器安全性	網站備份	高	是否定期執行備份？	**網站定期備份：** 應定期（至少每週一次）備份整個網站（檔案與數據庫）。 **異地備份：** 將備份儲存於安全的異地位置，以防因當地災難（例如火災、洪水）導致數據遺失。雲端儲存服務可作為異地備份的經濟實惠選項。	8.2.3 (q)	
Web 應用程式安全	數據處理	高	傳輸中的敏感數據是否受到妥善處理？	**強制使用 HTTPS：** 將所有 HTTP 流量重定向至 HTTPS。確保所有網站頁面（尤其是處理登入、表單或任何敏感數據的頁面）皆透過 HTTPS 提供服務。 **使用強效的 SSL/TLS 加密套件與協定：** 停用過時且不安全的 SSL/TLS 版本（如 SSLv2、SSLv3、TLS 1.0 及 TLS 1.1）與加密套件。優先採用具備 AES-256 加密的強效加密套件與協定，例如 TLS 1.3 和 TLS 1.2。 根據業界最佳實踐定期檢視並更新加密套件。使用 Qualys SSL Labs Server Test 等工具來評估您的 SSL/TLS 配置。 **向信譽良好的核證機關取得 SSL 憑證：** 向受信任且信譽良好的核證機關 (CA) 取得 SSL 憑證。考慮使用擴展驗證 (EV) 憑證以增強信任度與使用者信心，特別是針對登入頁面。 **HSTS（HTTP 嚴格傳輸安全性）：** 實施 HSTS 以強制瀏覽器始終透過 HTTPS 連線至您的網站，即使使用者手動輸入「http://」亦然。這有助於防止中間人攻擊。 **避免在查詢參數中傳輸敏感資料：** 請勿在 URL 查詢參數中傳輸敏感資訊（例如：密碼、學生證號）。 – 不良實務範例：*https://school.edu/grades?studentId=12345&grade=A*（在 URL 中暴露學生證號與成績） – 良好實務範例：使用 POST 請求將敏感數據提交至請求主體中，此數據不會顯示在 URL 中。	8.4.1 (c)、8.6.1(a-e, g)	
Web 應用程式安全	數據處理	高	靜態儲存的敏感數據是否受到妥善處理？	**數據庫加密：** 若使用數據庫，請啟用數據庫加密以保護靜態數據。 **檔案系統加密：** 應考慮對檔案系統或包含敏感數據的特定目錄進行加密。建議對筆記型電腦及其他可攜式裝置採用全磁碟加密。	8.4.1 (c)、8.6.1 (f)	
Web 應用程式安全	會話管理	中等	是否已安全管理連線，以防止連線劫持並維護使用者隱私？	**安全的會話 ID：** 產生隨機且無法預測的會話 ID。避免在會話 ID 中使用可預測的模式或特定於使用者的資訊。 **會話使用 HTTPS：** 僅透過 HTTPS 傳輸會話 ID。 **會話超時：** 實施會話超時機制，以自動登出閒置使用者。範例：為學校入口網站會話設定合理的超時時間（例如 15 至 30 分鐘）。 **重新產生會話 ID：** 在執行登入或變更密碼等重要操作後，重新產生會話 ID。	-	
Web 應用程式安全	密碼管理	高	是否強制執行並定期更新強密碼？	**採用強密碼政策：** 針對學生與教職員： – 最小長度：8 個字符 – 複雜度：須包含大寫字母、小寫字母、數字及符號。 – 密碼重複使用：禁止重複使用最近 5 組密碼。 – 密碼到期：考慮每 90 至 180 天讓密碼到期。 針對管理員： – 最小長度：15 個字符 – 複雜度：必須包含大寫字母、小寫字母、數字及符號，並考慮使用密語。 – 密碼重複使用：禁止重複使用最近 10 組密碼。 – 密碼到期：每 60 至 90 天讓密碼失效。 **多重認證 (MFA)：** 在可行情況下，強制要求所有管理員帳戶啟用 MFA。 **禁止使用常見密碼及字典單字** （例如：「password」、「123456」、「qwerty」、「schoolname」、「mascot」、學生姓名、教師姓名、與學校相關的詞彙）。**使用** 包含字典詞彙檢測功能的**黑名單或密碼強度檢查工具**。 **密碼雜湊：** 若進行自訂應用系統發展，請確保使用 bcrypt 或 Argon2 等強效算法，並搭配唯一鹽值對密碼進行雜湊處理。 **密碼管理工具：** 鼓勵學生、教職員及管理員使用信譽良好的密碼管理工具。	8.5.1(d)	

Web 應用程式安全	防注入攻擊	高	是否對輸入進行驗證以防止注入攻擊？	**輸入驗證：** 驗證所有使用者輸入（表單字段、URL 參數等），以防止注入攻擊。範例：針對學生註冊表單，驗證「姓名」字段僅接受英文字元及空格。 **參數化查詢（用於數據庫互動）：** 使用參數化查詢或預備陳述式以防止 SQL 注入。切勿透過直接串接使用者輸入來建構 SQL 查詢。 **輸出編碼：** 對網頁上顯示的所有輸出進行編碼，以防止跨站腳本（XSS）攻擊。範例：將 <、>、& 及 " 字符編碼為其 HTML 實體等價物（<、>、&、"）。		
Web 應用程式安全	存取控制	中等	是否已實施基於角色的存取控制？	**學生/教師/管理員角色：** 實施基於角色的存取控制，以限制對學校網站不同區塊的存取權限。範例：學生可存取自己的成績與作業，教師可管理所屬班級，而管理員則擁有完整存取權限。	-	
Web 應用程式安全	數據安全	高	是否使用 HTTPS 且數據經過加密？	**全面採用 HTTPS：** 強制所有網站流量使用 HTTPS。向信譽良好的憑證授權機構 (CA) 取得 SSL 憑證（Let's Encrypt 是一個免費且不錯的選擇）。 **數據庫加密：** 對儲存於數據庫中的敏感數據進行加密。大多數數據庫系統都提供加密功能。 **檔案系統加密（針對敏感檔案）：** 對儲存於網頁伺服器檔案系統中的敏感檔案進行加密。	8.5.1(b)、8.6.1(a)	
Web 應用程式安全	輸入安全	中等	上傳的檔案類型是否經過驗證/檢查？	**檔案類型限制：** 限制上傳的允許檔案類型（例如，僅允許 .pdf、.docx、.jpg）。 **檔案大小限制：** 限制上傳檔案的最大大小，以防止拒絕服務攻擊。 **惡意軟件掃描：** 若可行，請使用病毒掃描程式掃描上傳的檔案以檢查惡意軟件。	-	
Web 應用程式安全	誤差處理	中等	錯誤訊息是否避免洩露敏感資訊？	**通用誤差信息：**向使用者顯示通用誤差信息，避免揭露詳細的內部錯誤資訊或堆疊追蹤。範例：與其顯示數據庫誤差信息，應顯示通用信息「發生錯誤。請稍後重試。」 **記錄詳細錯誤：** 將詳細錯誤信息記錄至伺服器日誌以供除錯，但勿向使用者顯示。	-	
Web 應用程式安全	記錄與監控	中等	是否已啟用並審查存取日誌？	**啟用網頁伺服器記錄功能：** 確保網頁伺服器存取記錄已啟用，並記錄重要資訊，例如 IP 位址、時間戳記、請求的 URL 以及使用者代理程式。 **定期檢視日誌：** 指派一名工作人員（或使用自動化工具）定期（例如每週）檢視日誌，以偵測可疑活動，例如重複的登入失敗嘗試、來自異常位置的存取，或對敏感檔案的請求。 範例：使用 GoAccess 或 Webalizer 等日誌分析工具來產生網站流量報告，並識別潛在問題。若需更進階的監控，請考慮採用安全資訊與事件管理（SIEM）系統。	8.3.1, 8.5.1(e)	
Web 應用程式安全	組態管理	中等	是否採用安全的預設配置？	**強化網頁伺服器設定：** 安裝網頁伺服器（Apache、Nginx、IIS）後，應停用不必要的模組與功能，並遵循該網頁伺服器軟體專屬的安全強化準則。 **範例（Apache）：** 停用目錄列出功能、設定自訂錯誤頁面，並限制對配置檔案的存取權限。 **範例（Nginx）：** 限制請求大小、停用伺服器憑證，並設定適當的存取控制。	8.2.3 (k, l)	
一般網站安全	軟體更新	高	是否定期套用軟體更新？	**修補程式排程：** 針對作業系統、網頁伺服器軟體、內容管理系統（CMS）以及任何其他網頁應用程式，建立定期的修補程式排程。 **測試更新：** 在將更新套用至正式伺服器之前，應先在預備或發展系統上進行測試，以確保相容性。 範例：訂閱安全郵件列表或漏洞數據庫，以便及時收到有關新漏洞與修補程式的通知。	8.5.1 (a)	
一般網站安全	安全遠端管理	中等	是否採用安全的遠端存取方式？	**強密碼/多重認證 (MFA)：** 對網頁伺服器的遠端存取，應使用強密碼及多重認證 (MFA)。 **VPN：** 使用虛擬私人網路（VPN）進行安全的遠端管理。 **依 IP 限制存取：** 若可行，請將管理界面（例如：網頁伺服器控制台、SSH）的存取權限限制在特定 IP 位址或範圍內。 範例：請將標準 SSH 埠 22 變更為非標準埠。	8.5.1 (c)	
一般網站安全	搜尋索引控制	中等	是否已採取措施防止透過搜尋引擎發生數據外洩？	**robots.txt：** 使用 robots.txt 檔案，阻止搜尋引擎爬蟲存取敏感目錄或頁面。 **元標籤：** 使用元標籤（例如：*<META name="robots" content="noindex">*）防止特定頁面被索引。 **範例：** 使用 robots.txt 阻擋對學生目錄、教職員專用區或內部管理界面的存取。	8.5.1 (f)	
一般網站安全	安全掃描	低	是否進行了漏洞掃描？	**定期漏洞掃描：** 使用漏洞掃描工具（例如 Nessus Essentials、OpenVAS）定期掃描網站，以檢查已知漏洞。 頻率： --- 外部掃描（對外連網系統）：至少每半年一次；若貴校處理高度敏感資料或近期曾發生安全事件，則應更頻繁執行。 --- 內部掃描（內聯網系統）：至少每年一次。 **滲透測試（若預算許可）：** 考慮聘請合格且經驗豐富的安全評估人員或滲透測試公司進行滲透測試，以模擬真實世界的攻擊並識別漏洞。 頻率：至少每年一次，或在系統進行重大變更後。重點針對關鍵系統與應用系統。	8.5.1 (g)	
一般網站安全	安全外包	中等	網頁主機服務是否符合安全要求？	**服務水準協議 (SLA)：** 審閱網頁託管服務供應商的 SLA，以確保其符合學校的安全要求（例如：資料中心安全、正常運作時間保證、事件應變程序）。 **安全稽核：** 若可行，請索取網頁託管服務供應商的安全稽核與認證相關資訊（例如：ISO 27001、SOC 2）。	8.5.1 (h)	

實施摘要	數量	% 實施
高 應優先實施並納入為基礎安全層級，被視為維護安全環境不可或缺的措施 (總計：18)	0	0%
中等 有助於維持安全的重要防護措施，但可延後實施	0	0%
低 用於加強保護的額外防護措施	0	0%