第六章
數據保安

6.1 資料分類

6.1.1 在訂立保安措施前，首先應確定需要保護的數據並進行分類。數據的保密級別應按其敏感度劃分。學校可根據其學校保安政策需要把數據分為以下類別：

(a) 機密

(b) 內部限閱

(c) 公開

6.1.2 上述類別的定義：

(a) **機密**：指如被擅自披露會損害學校利益的資訊和材料。

(b) **內部限閱**：指如被擅自披露不合乎學校利益的資訊和材料。

(c) **公開**：指公布或供大眾查閱的資訊和材料。

6.1.3 學校應按照資料的保密類別制訂保密資料標籤及資料處理的程序。

6.1.4 學校應緊記須確保資料的機密性、完整性和可用性，並應在適當時考慮和推行保安措施，以保障資料在處理、傳輸和儲存時的機密性、完整性和可用性。

6.2 加密方法

6.2.1 學校須確保適當和有效使用加密方法，以保護資料的機密性、真確性和完整性。

6.2.2 在傳遞及儲存時，應使用加密技術保護數據並加強機密性。檔案加密的模式很多，例如使用程式自備的加密功能、外置硬件設備、保密匙加密和公開密碼匙加密等。

6.2.3 對於機密類別的資料，對稱密碼匙的長度，建議有 AES 加密法 128 個數元，或相對應的長度；而非對稱密碼匙的長度，則建議至少有 RSA 加密法 2048 個數元。

6.2.4 確保密碼匙得到保護和管理至為重要。用作處理機密資料的密碼匙必須與所處理的資料分開儲存。密碼匙可儲存在智能卡晶片、權標或磁碟等，並用作認證及／或為資料解密。此外，在分發檔案時將解密匙與加密檔案一併分發是十分危險的，因為若有人取得解密匙，便很容易開啓檔案。

6.2.5 由於流動裝置及抽取式媒體體積細小及容易遺失或被竊，如用作儲存資料，將存在風險，故應避免把保密資料儲存在這些裝置內。有關人員應有充分的理據才可使用這類裝置儲存保密資料，並應使用由學校提供的流動裝置及抽取式媒體。有關人員應事先得到正式授權，方可把最少所需的保密資料儲存在流動裝置及抽取式媒體內。為盡量減低資料外泄的風險，應只使用具備適合保護保密資料的加密功能的裝置。當無須使用流動裝置及抽取式媒體儲存保密資料時，所有人員須儘快刪除該等裝置所儲存的保密資料，以盡量減低資料曝光的機會。

6.2.6 數據加密能增強數據的機密性。學校應確認雲端服務所提供的加密功能能夠符合加密控制使用的加密政策。保密數據無論在靜止或傳遞中，都須根據學校保安要求和需要採用嚴謹的加密方式以作保護。

6.2.7 應用系統的密碼保護功能，主要用於保護檔案，防止他人在未獲授權的情況下取閱資料。在保護資料機密性時，用戶應把檔案妥為加密，而非單靠密碼保護。

6.3 備份

6.3.1 學校應定期進行備份工作，並應為其資訊系統制訂及推行備份和復原政策。用戶應定期為儲存在工作站、流動裝置及抽取式儲存媒體內的數據進行備份。備份頻率應視乎失去數據可用性所帶來的影響而定。備份復原測試亦須定期進行。學校在制訂備份及復原政策時，應遵從有關的良好作業模式：

(a) 應為所有操作數據備存備份複本，以便在這些數據無意中受損或遺失時可以重組。

(b) 應定期備份，以便將檔案復原至最新狀態。

(c) 應定期覆檢備份活動。應制訂完善的數據備份及復原程序，並設法徹底測試這些程序在實際操作環境的效用。

(d) 備份複本宜離線存放在安全及穩妥的地方，並遠離系統的所在地。即使發生災難並破壞了系統，仍可在其他地方將系統重組。

(e) 應備存多代備份複本，使復原程序有更大靈活性和彈性。備存備份複本時應考慮實施一套「三代」計劃，以確保兩份備份複本（即上一代及再上一代的備份複本）總是與最新數據及程式操作複本存放在一起。最新操作狀態備份的更新複本，必須與備份複本一併備存及存放。

(f) 應至少備存三代備份。然而，如每天備份，則在行政上可能較容易保存六至七代備份。舉例來說，星期一的每天備份應保留至下一個星期一，才被蓋寫。如有需要，檔案的月底及年底備份可保留更長時間。

(g) 應定期測試作備份用途的磁帶／光碟／外置硬碟／網絡儲存設備（NAS）／儲存區域網絡（SAN）／雲端備份，以確保在有需要時可復原數據。

6.3.2 在一些不能預計的情況下，如數據在進行備份前被意外刪除，或數據所在的硬磁碟因破損而無法利用系統接達，則可能需要硬磁碟數據復原服務。如需要外聘數據復原服務，學校應遵從有關的良好作業模式，以減低數據外泄的風險：

(a) 盡可能即場進行數據復原服務，並確保承辦商在復原過程中留意保密資料的保護要求。

(b) 陪同承辦商人員，並小心留意，確保保密資料不會外泄。

(c) 淨化用作數據復原的裝備工具及有關媒體內剩餘的用戶數據。

(d) 與承辦商簽訂不可向外披露資料的協議。

6.4 個人資料（私隱）

6.4.1 學校處理個人資料時，必須確保遵行《個人資料（私隱）條例》，特別是保障資料第四原則（有關個人資料的保安），並應採取適當的保安措施，以保護個人資料免在未獲授權或意外的情況下被接達、處理、刪除或作其他用途。有關六個保障資料原則的詳情，請參閱個人資料私隱專員公署網站內的《個人資料（私隱）條例》。
https://www.pcpd.org.hk/tc_chi/data_privacy_law/6_data_protection_principles/principles.html

6.5 刪除資料

6.5.1 當無須要使用數據時，應確保數據被永久銷毀。應實施制衡機制，以核實是否已順利完成安全刪除程序。

6.5.2 在重用、轉移或棄置電腦設備、儲存媒體及辦公室電子設備前，須通過淨化程序或實體銷毀，把媒體內的所有數據徹底清除或銷毀，以確保該等資料無法復原。

(a) 淨化程序：指徹底刪除媒體上的資料，以確保無法讀取原有資料的程序。淨化程序可通過蓋寫或消磁完成。

(b) 實體銷毀：不能淨化的儲存媒體須以切碎、解體或研磨等方法作實體銷毀。

6.5.3 以下表列描述了不同儲存媒體的數據銷毀方式。建議學校根據數據類型、披露風險以及例如意外披露數據的影響，制定合適的風險決策方法。

媒體類型	重用（包括轉移重用）	棄置（包括以舊換新及更換損壞的媒體）
非揮發性磁性媒體，如硬磁碟、軟磁碟、磁帶等	蓋寫	蓋寫 或 消磁 或 實體銷毀
非揮發性固態記憶，如通用串列匯流排閃存盤、記憶卡、固態硬碟等	蓋寫	蓋寫 或 實體銷毀
光學儲存媒體，如不可重寫的光碟、數碼影像光碟、藍光光碟等		實體銷毀
光學儲存媒體，如可重寫的光碟、數碼影像光碟、藍光光碟等	蓋寫	實體銷毀
智能裝置，如個人數碼助理、流動電話、平板電腦等	蓋寫	蓋寫 或 消磁 或 實體銷毀

6.6 提升對資料保安要求的保安意識

6.6.1 要提升學校對資料保安要求的保安意識，一個有效的方法是持續分享資訊，例如分發保安消息或補充資料，尤其在資訊科技保安文件的保安要求有重大修改後，及／或發生對學校／公眾有嚴重影響的重大保安事故之後。以下是派發保安消息及補充資料的指引，供學校參考：

(a) 所有規定都被詳細記錄。應教導受眾可在何處找到有關文件，包括其優先次序。

(b) 應向受眾講解一般原則，使他們能夠容易理解及記住其主要概念。

(c) 應做和不應做的事項及實例可以引起受眾興趣，並從而鞏固他們的理解。

(d) 補充資料應盡量保持精簡，例如預留約五頁予一般事項；一至兩頁有關重大事故後的提醒，或任何很大可能發生的潛在事故通知。

(e) 學校可通過如電子郵件，即時信息群組，教職員會議等的溝通渠道，以發放學校資訊安全訊息的最新消息。