

新竹縣枋寮國民小學個人資料保護管理要點

(參考教育部提升校園資訊安全服務計畫要點)

中華民國 106 年更新

壹、文件目的：

新竹縣枋寮國民小學（以下簡稱本校）為落實個人資料之保護及管理，特訂定本要點。

貳、本指引用詞定義：

- 一、 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、特徵、家庭、教育、職業、病歷、醫療、健康檢查、聯絡方式、財務情況及其他得以直接或間接方式識別該個人之資料。教育機構中常見之個人資料如教職員人事資料、學生基本資料、家長聯絡方式、家庭狀況、班級成績資料、健康檢查結果、心理輔導檔案等。
- 二、 其餘用詞定義請參見「個人資料保護法」。

參、個人資料保護及安全原則：

- 一、 機關學校應指定單位副首長為機關召集人，統籌決策與執行單位內資訊安全與個資隱私業務之資源整合運用。
- 二、 機關學校應指定專人依相關法令辦理安全維護及保管事項，作為機關內部之個人資料管理代表。機關組織編制較小者，則統一由該機關「個資保護聯絡窗口」兼辦專責人員業務。
- 三、 機關學校應設置並指定「個資保護聯絡窗口」，作為機關學校間個資業務協調聯繫之對口、機關學校本身個資安全事件通報之對口，以及重大個資外洩事件之民眾聯繫單一窗口。另單位應將「個資保護聯絡窗口」之聯繫方式（如：電話、email）置於單位網站，以便利民眾提出申訴與救濟。
- 四、 個人資料檔案應定期備份，並防止個人資料被竊取、竄改、毀損、滅失或洩露。個人資料輸入、輸出、存取、更新、更正或註銷等處理行為，宜釐定使用範圍及調閱或存取權限。個人資料檔案之處理行為應設置使用者代碼及通行碼，不得與他人共用並定期更新。另視需要考量採取權限區隔、資料加密機制，或相關核准程序加以控管，並留存使用者身分、識別帳號與其行為紀錄以供事後稽查。
- 五、 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身份之登入通行碼，並視業務及資料重要性，考量其他輔助安全措施。個人資料檔案使用完畢後，應即退出應用程式，不得留置於電腦終端機。
- 六、 含有個人資料之紙本報表的申請、讀取、列印、使用、存檔、轉交及銷毀等處

理及利用行為，宜建立相關之授權、監督及行為記錄機制。

- 七、內部傳遞或與其他機關交換個人資料時，應選擇可靠且具備保密機制之傳遞方式，如於實體文件封袋加上彌封、或對資料檔案壓縮加密，並對轉交或傳輸行為加以記錄流向備查。
- 八、對於個人資料之調閱宜經申請並核准，並加以記錄其調閱身分及行為。調閱紀錄可視機關實際需求存檔，以利後續人員查詢及追蹤。
- 九、以電腦處理個人資料時，需核對個人資料之輸入、輸出、編輯或更正是否與原件相符。個人資料提供利用時，對資料相符與否如有疑義，應調閱原檔案查核。
- 十、機關學校單位管理之網站或網頁內容，於確有必要公佈個人資料時，需經所屬單位主管核准，且依相關法律及規範處理，始得公佈。

肆、參考注意事項：

一、處理個資之資訊設備使用參考注意事項：

1. 處理個人資料檔案之資訊設備，需設置使用者代碼及通行碼。
2. 通行碼至少每六個月更換一次，通行碼長度應至少 8 碼，且包含文數字。
3. 禁止與他人共用電腦系統帳號。
4. 採取權限區隔，非專責處理特定個人資料者不得具有存取或查閱個人資料之權限。
5. 個人資料檔案應予以加密。
6. 至少每月備份資訊設備內個人資料檔案一次。
7. 個人資料檔案使用完畢後，應立即退出應用程式。
8. 資訊設備應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 15 分鐘以內。
9. 交換個人資料檔案時，應對資料檔案加密，亦或是透過加密通道傳送。
10. 個人資料禁止存放於網路芳鄰分享目錄，並停用 Guest 帳號。
11. 禁止使用 MSN 或其他即時通訊軟體傳輸個人資料檔案。
12. 禁止使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案。
13. 禁止使用點對點(P2P)軟體及 Tunnel 相關工具下載或提供分享檔案。
14. 存放個人資料之資訊設備應與外部網路隔絕（如：防火牆）。
15. 存放個人資料之資訊設備應安裝防毒軟體，除至少每日更新病毒碼外，並應每周執行完整掃描。
16. 存放個人資料之資訊設備應定期檢視、更新作業系統、應用程式漏洞（如：Windows 作業系統、Windows Office、Adobe Acrobat 等）。

二、設備管理參考注意事項：

1. 應指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施等，並檢視、處理其錯誤或異常事件等訊息。
2. 儲存個人資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），避免有心人士或非授權人員存取。
3. 儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境（如：上鎖之防潮箱、書櫃），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。
4. 外部團體或個人更新或維修電腦設備時，應指派專人在場，確保個人資料之安全及防止個人資料外洩。
5. 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用時，應確實刪除該設備所儲存之個人資料檔案。

三、人員管理參考注意事項：

1. 機關學校應對處理個人資料檔案之人員施予資訊安全與個資隱私保護之教育訓練（內、外訓皆可），並定期於單位內宣導個資隱私保護之重要性。
2. 處理個人資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置通行碼外，應視需要更換使用者識別帳號。
3. 處理個人資料檔案之人員，應簽訂保密切結書，並確認於離職時或合約終止時取消或停用其使用者識別帳號，且收繳其通行證及相關證件。

四、系統開發及委外管理參考注意事項：

1. 自行開發或委外處理個人資料檔案之資訊系統，應在系統開發生命週期之初始階段，將個人資料檔案的安全需求納入考量（如：邏輯測試）；系統之維護、更新、上線、及版本異動等作業，應予安全管制，避免危害個人資料安全。
2. 宜避免允許維護人員或系統服務廠商以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，則應透過加密通道進行（如：HTTPS、SSH 等）。
3. 自行開發或委外處理個人資料檔案之資訊系統，應保護及控制測試資料，且宜避免以真實個人資料進行測試；如需使用，應將可辨識之個人資料修改為無法辨識之模糊資訊（如：虛擬或錯置），並於完成測試作業後迅速移除。
4. 個人資料檔案若委外建檔，應於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則。

伍、以上管理要點，經鈞長核可後公佈實施，修正時亦同。

承辦人

教導主任

校長