# 私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法

第一條　本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。

第二條　本辦法所稱主管機關：在中央為教育部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

第三條　本辦法用詞，定義如下：

一、個人資料管理人（以下簡稱管理人）：指由校長、園長擔任或指定，負責督導個人資料檔案安全維護計畫(以下簡稱安全維護計畫)訂定及執行之人員。

二、個人資料稽核人員（以下簡稱稽核人員）：指由校長、園長指定，負責評核安全維護計畫執行情形及成效之人員。

三、所屬人員：指私立高級中等以下學校(以下簡稱學校)及幼兒園執行業務之過程，必須接觸個人資料之人員，包括定期或不定期契約人員及派遣員工。

前項第三款所定幼兒園，包括依幼兒教育及照顧法對幼兒提供教育及照顧服務之幼兒園、社區互助教保服務中心及部落互助教保服務中心。

第一項第一款管理人與第二款稽核人員不得為同一人。

第四條　學校及幼兒園應依本辦法規定訂定安全維護計畫，落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

學校及幼兒園訂定安全維護計畫時，應視其經營型態、規模、保有個人資料之性質及數量等事項，訂定適當之安全維護措施。

前項計畫，應包括業務終止後，個人資料處理方法等相關個人資料管理事項。

第五條　學校及幼兒園得指定或設管理單位，或指定專人，負責個人資料檔案安全維護；其任務如下：

一、訂定及執行安全維護計畫。

二、定期就個人資料檔案安全維護管理情形，向管理人提出書面報告。

三、依據稽核人員就安全維護計畫執行之評核，於進行檢討改進後，向管理人及稽核人員提出書面報告。

第六條　學校及幼兒園應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。

學校及幼兒園經定期檢視，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置。

第七條　學校及幼兒園於蒐集個人資料時，應檢視是否符合前條第一項所定之類別及範圍。

**學校及幼兒園於傳輸個人資料時，應採取必要保護措施，避免洩漏。**

第八條　學校及幼兒園應依已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能產生之風險，訂定適當之管控措施。

第九條　學校及幼兒園於蒐集個人資料時，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。

第十條　**學校及幼兒園依本法第二十條第一項規定利用個人資料為宣傳、推廣或行銷時，應明確告知當事人學校及幼兒園立案名稱及個人資料來源。**

學校及幼兒園於首次利用個人資料為宣傳、推廣或行銷時，應提供當事人或其法定代理人表示拒絕接受宣傳、推廣或行銷之方式，並支付所需費用；當事人或其法定代理人表示拒絕宣傳、推廣或行銷後，應立即停止利用其個人資料宣傳、推廣或行銷，並周知所屬人員。

第十一條　學校及幼兒園委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定對受託者為適當之監督，並明確約定相關監督事項及方式。

第十二條　學校及幼兒園於當事人或其法定代理人行使本法第三條規定之權利時，得採取下列方式辦理：

一、提供聯絡窗口及聯絡方式。

二、確認是否為資料當事人之本人或其法定代理人，或經其委託。

三、有本法第十條但書、第十一條第二項但書或第三項但書得拒絕當事人或其法定代理人行使權利之事由，一併附理由通知當事人或其法定代理人。

四、告知是否酌收必要成本費用及其收費基準，並遵守本法第十三條處理期限規定。

第十三條　學校及幼兒園應訂定應變機制，在發生個人資料被竊取、洩漏、竄改或其他侵害事件時，迅速處理，以保護當事人之權益。

前項應變機制，應包括下列事項：

一、採取適當之措施，控制事件對當事人造成之損害。

二、查明事件發生原因及損害狀況，並以適當方式通知當事人或其法定代理人。

三、研議改進措施，避免事故再度發生。

學校及幼兒園應自第一項事件發生之日起三日內，通報主管機關；並自處理結束之日起一個月內，將處理方式及結果，報主管機關備查。

第十四條　學校及幼兒園對所保有之個人資料檔案，應設置必要之安全設備及採取必要之防護措施。

前項安全設備或防護措施，應包括下列事項：

一、紙本資料檔案之安全保護設施及管理程序。

二、電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。

三、訂定紙本資料之銷毀程序；電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。

第十五條　學校及幼兒園為確實保護個人資料之安全，應對其所屬人員採取下列措施：

一、依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之適當性及必要性。

二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。

三、要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。

四、所屬人員離職時取消其識別碼，並要求將執行業務所持有之個人資料（包括紙本及儲存媒介物）辦理交接，不得攜離使用，並應簽訂保密切結書。

第十六條　學校及幼兒園應訂定個人資料檔案安全稽核機制，定期或不定期檢查安全維護計畫所定相關事項是否落實執行，並將檢查結果向管理人提出報告。

執行前項稽核之人員與第五條指定之專責人員，不得為同一人。

學校應將第一項稽核機制，納入其內部控制制度訂定作業程序、內部控制點及稽核作業規範（內部管理及稽核作業規章）規定辦理。

第十七條　學校及幼兒園執行安全維護計畫各項程序及措施，至少應保存下列紀錄：

一、個人資料之交付及傳輸。

二、個人資料之維護、修正、刪除、銷毀及轉移。

三、提供當事人或其法定代理人行使之權利。

四、存取個人資料系統之紀錄。

五、備份及還原之測試。

六、所屬人員權限之異動。

七、所屬人員違反權限之行為。

八、因應事故發生所採取之措施。

九、定期檢查處理個人資料之資訊系統。

十、教育訓練。

十一、安全維護計畫稽核及改善措施之執行。

十二、業務終止後處理紀錄。

第十八條　學校及幼兒園對於個人資料之蒐集、處理及利用，應符合本法第十九條及第二十條規定，並應定期或不定期對其所屬人員，施以教育訓練或認知宣導，使其明瞭個人資料保護相關法令規定、責任範圍、作業程序及應遵守之相關措施。

第十九條　學校及幼兒園業務終止後，其保有之個人資料之處理方式及留存紀錄如下：

一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

前項紀錄應至少留存五年。

第二十條　學校及幼兒園應參酌安全維護計畫執行狀況、技術發展、法令依據修正等因素，檢視所定安全維護計畫是否合宜，必要時應予以修正。

第二十一條　本辦法自發布日施行。