法規名稱：私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法
修正日期：民國 110 年 12 月 08 日

第 1 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 2 條

本辦法之主管機關為教育部。

第 3 條

1 依私立學校法核准設立之私立專科以上學校（以下簡稱學校）及依學術研究機構設立辦法核准設立之私立學術研究機構（以下簡稱機構）應訂定個人資料檔案安全維護計畫（以下簡稱安全維護計畫），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。

2 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 4 條

1 本辦法用詞，定義如下：

一、個人資料管理人：學校、機構應由校長、機構負責人擔任或指定，負責督導安全維護計畫訂定及執行之人員（以下簡稱管理人）。

二、個人資料稽核人員：學校、機構應由校長、機構負責人指定，負責評核安全維護計畫執行情形及成效之人員（以下簡稱稽核人員）。

三、所屬人員：執行業務之過程必須接觸個人資料之人員，包括學校、機構之定期或不定期契約人員及派遣員工。

2 前項第一款管理人員與第二款稽核人員不得為同一人。

第 5 條

學校、機構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，包括業務終止後個人資料處理方法。

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 6 條

1 學校、機構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。

2 學校、機構經定期檢視，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 7 條

學校、機構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 8 條

1 學校、機構應訂定應變機制，在發生個人資料被竊取、洩露、竄改或其他侵害事故時，迅速處理以保護當事人之權益。

2 前項應變機制，應包括下列事項：

一、採取適當之措施，控制事故對當事人造成之損害。

二、查明事故發生原因及損害狀況，並以適當方式通知當事人。

三、研議改進措施，避免事故再度發生。

3 學校、機構應自第一項事故發現時起七十二小時內，填具個人資料侵害事故通報與紀錄表（如附件），通報主管機關，未依時限內通報者，應附理由說明；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。

4 依規定通報後，主管機關得派員檢查，受檢者不得規避、妨礙或拒絕，主管機關並得依本法第二十二條至第二十五條規定，為適當之監督管理機制。

第 9 條

學校、機構委託他人蒐集、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 10 條

1 學校、機構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，應明確告知當事人其所屬學校、機構立案名稱及個人資料來源。

2 學校、機構於首次利用個人資料為宣傳、推廣或行銷時，應提供當事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 11 條

學校、機構於當事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行使權利之事由，一併附理由通知當事人。

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 12 條

1 學校、機構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。

2 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 12-1 條

1 學校、機構提供電子商務服務系統或本法第六條所定個人資料種類之資通系統時，應採取下列資訊安全措施：

一、使用者身分確認及保護機制。

二、個人資料顯示之隱碼機制。

三、網際網路傳輸之安全加密機制。

四、應用系統於開發、上線、維護等各階段軟體驗證及確認程序。

五、個人資料檔案與資料庫之存取控制及保護監控措施。

六、防止外部網路入侵對策。

七、非法或異常使用行為之監控及因應機制。

2 前項所稱電子商務，指透過網際網路進行有關商品或服務之廣告、行銷、供應或訂購等各項商業交易活動；資通系統，指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

3 第一項第六款及第七款所定措施，應定期演練及檢討改善。

第 12-2 條

學校、機構進行個人資料國際傳輸前，應檢視有無主管機關依本法第二十一條規定為國際傳輸之限制，並且告知學生及教職員其個人資料所欲國際傳輸之區域，同時對資料接收方為下列事項之監督：

一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。

二、當事人行使本法第三條所定權利之相關事項。

第 13 條

學校、機構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，並應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 14 條

學校、機構業務終止後，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、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。

第 15 條

學校、機構對於個人資料蒐集、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 16 條

學校、機構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。

第 17 條

學校、機構執行安全維護計畫各項程序及措施，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 18 條

本辦法自發布日施行。