

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十三條、第十四條之一、第十四條之二修正條文

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、竄改或其他侵害事故時，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；通報之主管機關為直轄市、縣（市）政府者，並應副知教育部，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。

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，為適當之監督管理措施。

第十四條之一 學校及幼兒園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。

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；資訊系統，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。

第一項第六款及第七款所定措施，應定期演練及檢討改善。

第十四條之二 學校及幼兒園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，並告知學校學生、幼兒園幼兒、學生及幼兒之法定代理人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。