教育體系個人資料安全保護基本措施及作法

人員管理措施	說明及作法
一、指定蒐集、處理及利用個人資料個別作業（以下簡稱「作業」）流程之負責人員。 二、就個別作業設定所屬人員不同之權限並控管之，以一定機制管理其權限，且定期確認權限內容設定之適當與必要性。 三、要求所屬人員負擔相關之保密義務。	一、針對人員管理之部分，首先應先確認實際進行個人資料之蒐集、處理及利用之負責人員為何，方可確認相關管理程序之權責歸屬。 二、各機關所屬人員與個人資料相關之各項作業，若有設定權限控管之必要，則應以一定機制管理之，並確認其權限設定是否適當或必要。避免人員取得不適當之權限，得以接觸非於作業必要範圍內之個人資料。 三、各機關應要求其所屬人員負擔相關之保密義務，使所屬人員能明瞭其責任，必要時亦可以訂定契約條款之方式為之，以作為相關權責之紀錄。
作業管理措施	**說明及作法**
一、運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，訂定使用可攜式設備或儲存媒介物之規範。 二、針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制。 三、作業過程有備份個人資料之需要時，比照原件，依本法規定予以保護之。 四、個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，嗣該媒介物於報廢或轉作其他用途時，採適當防範措施，以免由該媒介物洩漏個人資料。 五、委託他人執行前款行為時，對受託人依本法施行細則第八條規定為適當之監督，並明確約定相關監督事項與方式。	一、使用可攜式儲存媒體，可能提高處理個人資料之電腦及相關設備遭受惡意程式攻擊及個人資料外洩之風險，因此若有使用可攜式儲存媒體之情況，應訂定相關使用規範。 二、針對個人資料處理之不同態樣，包括儲存、傳輸及備份之狀況，如資料有加密之必要，即應採取適當之加密機制。 三、針對有備份必要之個人資料，除有必要時採取加密機制，儲存備份資料之媒體亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。 四、儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之，以避免資料不當外洩。 五、說明委託他人執行前款行為時，對受託人依本法施行細則第八條規定為適當之監督，並明確約定相關監督事項、方式、義務及責任。

物理環境管理措施	說明及作法
一、依作業內容之不同，實施必要之門禁管理。 二、妥善保管個人資料之儲存媒體。	在實體之物理環境管理方面，各機關亦應針對不同之作業內容、作業環境及個人資料之種類與數量，實施必要之門禁管理，以適當方式或場所保管個人資料之儲存媒體。
技術管理措施	**說明及作法**
一、於電腦、相關設備或系統上設定認證機制，帳號及密碼使其具備一定安全之複雜度並定期更換密碼。 二、於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。 三、對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。 四、具備存取權限之終端機不得安裝檔案分享軟體。 五、定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。	一、認證機制使用密碼之方式時，並應有適當之管理方式，並定期測試權限機制之有效性。 二、電腦系統中安裝防毒軟體，並定期更新病毒碼。 三、避免惡意程式與系統漏洞對作業系統之威脅。 四、檔案分享軟體之控制。 五、檢查系統之使用狀況與個人資料存取之情形。
認知宣導及教育訓練	**說明**
各機關應對所屬人員施以認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序。	為落實執行相關管理程序，各機關應透過認知宣導及教育訓練使所屬人員均能明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序。
紀錄機制	**說明**
一、個人資料交付、傳輸之紀錄。 二、確認個人資料正確性及更正之紀錄。 三、提供當事人行使權利之紀錄。 四、所屬人員權限新增、變動及刪除之紀錄。 五、個人資料刪除、廢棄之紀錄。 六、教育訓練之紀錄。	為確認所訂定之相關程序是否落實執行，以及釐清個人資料於蒐集、處理及利用過程之相關權責，各機關應保存相關紀錄以供查驗。