東方學校財團法人東方設計大學
個人資料安全保護基本措施

105 年 5 月 4 日行政會議審議通過
106 年 7 月 14 日行政會議通過改名修正

壹、人員管理

一、東方設計大學(以下簡稱本校)教職員工職務如有異動，其保管之個人資料（以下簡稱個資）檔案應列入移交，相關資訊系統存取權限應重新設定。

二、凡接觸個資檔案之人員應依照本校個人資料保護管理政策要求，執行相關規定之程序，負擔個資保密及保護之義務，並於離職、職務調動或合約終止時，停用資訊系統使用者識別帳號或終止相關權限或繳回通行證及相關證件。

三、使用 LINE、FB、Skype 或其他即時通訊軟體傳輸業務所知悉之個資時，須與原個資蒐集之特定目的相符及合法，並考量資訊傳輸之安全性後始得交付。

四、在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個資，須與原個資蒐集之特定目的相符。

貳、作業管理

一、個資蒐集應秉持「適當、相當且不過度」，只蒐集必要之個人資料，以降低個資外洩風險。

二、針對所保有之個資，部份甚為敏感的欄位內容，譬如：密碼、身分證號等，於蒐集、處理或利用時，加上適宜之遮蔽措施。

三、與個資檔案有關之資訊系統(程式)使用完畢後，應立即登出應用系統(程式)。

四、個資檔案存放網路共用目錄時，共用目錄需有適當之安全保護。

五、網路傳送個資檔案時，應對資料檔案加密，並再確認傳送對象無誤及請對方收到後回覆確認。

六、使用可攜式儲存媒體時，遵循以下的使用規範：

(一)確定電腦安裝之防毒程式及病毒碼都有定時更新，足以偵測隱藏之病毒後，方可去讀取可攜式電腦儲存媒體內的檔案。

(二)暫存的個資檔案，使用後應確認刪除。

(三)電腦使用應設登入密碼且符合密碼複雜難度要求。

七、影印、列印、傳真使用後須確認設備內並未遺留個資資料及原稿。

八、應定期備份含有個資電腦資料，及確認備份資料的可用性與安全性。

九、個人電腦報廢須對硬碟做低階格式化；移作他用時，應格式化硬碟後再重新安裝系統；故障之硬碟應予以實體破壞。

十、報廢之個資文件須用碎紙機銷毀或依其他核可之方式進行銷毀；電子檔須確實刪除與清空資源回收桶。

十一、委託他人執行上述行為時，需對受委託人依個資法施行細則第八條規定為適當之監督，並明確約定相關事項、方式、義務及責任。

參、物理環境管理

一、校內各單位保有個資之辦公室、檔案室、電腦主機室或儲存空間

(一)無人或下班最後一人離開時，需將辦公室關門上鎖。

(二)下班時記得將敏感之文件與可攜式資訊設備存放於安全地點或裝置。

(三)辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，應主動詢問並儘速通知相關部門進行處理。

(四)重要的辦公室、檔案室或電腦主機室應有適當之安全防護措施。

二、個人資料儲存媒體的保管

(一)應對儲存媒體內重要的個資檔案加強安全管控，例如加密。

(二)應有備份機制，以免重要資料遺失。

(三)隨身碟只適宜儲存暫時性檔案，重要的個資檔案使用後應儘快刪除，以免因隨身碟遺失造成個資檔案外洩。

三、圖書資訊處主機房

(一)為確保相關設施之安全，非權責單位指定之人員不得擅自進入或使用相關資訊設備。

(二)若外部人員或未具進出權限之人員，因執行業務需求進入時，必須指派人員隨行並記錄之，並遵守相關資訊安全管理之規定。

肆、技術管理

一、重要資訊系統主機應做防火牆設定。

二、重要資訊系統應適宜的限制存取 IP。

三、電腦作業系統及相關應用程式之漏洞，應適當修補。資訊系統主機必要時需進行弱點掃描，並應適當進行弱點處理。

四、公務個人電腦應安裝防毒程式並設定自動更新病毒碼及作業系統升級。

五、存有個資的個人電腦及伺服器，應設定登入密碼，且其密碼要符合安全之複雜度至少 6 碼以上，且定期需更換密碼一次。

六、個人電腦應設定螢幕保護密碼，且啟動時間在 10 分鐘以內。

七、應維持個資存取權限的正確性，且原則上不得共用存取權限，並留意個資被存取的情形。

八、禁止人員使用點對點(P2P)軟體提供分享檔案。

九、每年應執行個資盤點，檢查個資之使用狀況及存取情形。

伍、認知宣導及教育訓練

一、應鼓勵教職員工生參與校內外資訊安全與個資保護之教育訓練，並定期宣導個資保護之重要性。

二、本校教職員工每年應至少參加校內舉辦 2 個小時(含)以上的個資保護相關宣導及教育訓練，以養成教職員工個資保護的警覺性。

三、本校各單位個資負責窗口應時常注意個資保護相關知識與訊息，並摘要彙整於本校對外公開之網站或內部網站，以作為教職員工生獲取個資保護資訊的重要管道。

陸、紀錄機制

一、個資交付、傳輸之紀錄

(一)以 Email 方式，交付人應保留相關紀錄。

(二)系統提供授權人連線下載方式，系統應有連線紀錄可供查閱。

二、確認個人資料正確性及更正紀錄

(一)資訊系統設計上應提供個人查核本人的基本資料，並允許做適宜之資料更新，以維持個資正確性。

(二)個人以異於上述的其它方式請求更正時，如電話、Email、信函等，處理人員除做必要的查核身份程序外，尚應設法留存事件紀錄。

三、提供當事人行使權利之紀錄

依據個人資料保護法第三條，當事人得行使之相關權利，例如請求閱覽等，並提供本校各單位個資窗口之詳細連絡資訊，例如連絡電話、Email 及郵寄地址。

四、人員權限新增、變動及刪除紀錄

人員工作異動時，重要資訊系統負責人應即對系統使用權限重新做設定，並保留相關紀錄。

五、個人資料刪除、廢棄紀錄

執行個資盤點與風險評鑑時，個資保管人應對已超過保留期限的部份，列表記錄後依規定銷毀及確認無誤，如碎紙與刪除電子檔或依經核可之方式進行銷毀。

六、教育訓練紀錄

(一)將取得授權之研習課程講義或簡報檔公告「個人資料保護專區」網站。

(二)應保留教育訓練紀錄。

柒、公告實施

本措施經行政會議通過，陳請校長核定後公告實施，修正時亦同。