實踐大學個人資料安全維護計畫

113 年 6 月 19 日 112 學年度第 2 學期資通安全暨個人資料保護委員會通過

一、依據

實踐大學（以下簡稱本校）依個人資料保護法（以下簡稱個資法）第二十七條第三項規定、「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」及本校「個人資料保護政策」，訂定實踐大學個人資料安全維護計畫（以下簡稱本計畫）。

二、目的

本校為符合政府法令相關規範，落實個人資料檔案之安全維護及管理，並防止個人資料被竊取、竄改、毀損或洩漏，本校所屬人員應依本計畫及方法辦理個人資料檔案維護及業務終止後個人資料處理事項。

三、適用範圍

本校之個人資料管理維護範圍應涵蓋全校，且基於特定目的內所有教職員工、學生及外部互動關係人之個人資料蒐集、處理、利用，以及國際傳輸等相關作業程序。

四、推動組織與管理單位

（一）本校為確實執行個人資料保護及管理相關事務，設置「資通安全暨個人資料保護委員會」（以下簡稱本委員會），資通安全暨個人資料保護委員會設置辦法另訂之。

（二）本校設置個人資料保護聯絡窗口，辦理下列事項：

1. 個人資料保護業務協調、聯繫及緊急應變通報。
2. 發生重大個人資料外洩事件，通報主管機關、當事人。
3. 以非自動化方式檢索、整理個人資料安全事件之通報。
4. 本校個資管理專人名冊製作及更新。
5. 本校個資管理專人與教職員生教育訓練名單及紀錄彙整。

（三）各單位應指定個資管理專人，協助單位內同仁辦理下列事項：

1. 當事人依個資法第十條及第十一條第一項至第四項所定之請求作業程序及法令規章。
2. 個資法第十一條第五項及第十二條所定通知之作業程序及法令規章。
3. 個資法第二十七條第一項所定個人資料檔案安全維護。
4. 依本委員會擬議工作執行。
5. 個人資料保護法令諮詢。
6. 個人資料保護事項協調、聯繫。

7. 單位內個人資料遭竊取、竄改、毀損、滅失、洩漏之預防、危機處理、應變及通報。
8. 配合本校個人資料保護相關規定及安全措施執行與稽核。
9. 單位內其他個人資料保護管理規劃及執行。

五、界定個人資料及風險管理

（一）本校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。本校經定期檢視，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。

（二）本校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。

六、個人資料與設備管理安全

（一）本校於當事人行使個資法第三條規定之權利時，得採取相關方式辦理。

（二）個人資料檔案之存取，應釐定使用範圍及使用權限，並設置帳號、密碼且不與他人共用。

（三）存有個人資料之相關資通系統與資通訊設備，業務單位應採取必要之防護措施。紙本個人資料檔案應妥善保存，放置於安全地點。

（四）個人資料檔案儲存在個人電腦或資通系統者，應依本校規定於個人電腦及系統設置開機密碼、螢幕保護程式及相關安全措施。

（五）個人電腦或資通系統應定期更換密碼，且密碼設定之長度、複雜度與變更頻率應符合本校之要求。

（六）個人資料檔案使用完畢，應即退出應用系統，不得留置在電腦顯示畫面上。

（七）個人資料檔案蒐集之特定目的消失或期限屆滿，或個人資料檔案若已超過保存期限時，應依本校程序提出申請，經核准後進行銷毀作業。

（八）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。

（九）以網際網路蒐集、處理、利用及國際傳遞個人資料時，應採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

（十）本校所屬人員離職或職務異動時，應取消或變更其相關資通訊系統與設備之通行碼（密碼），且應將其執行業務所保管之儲存媒體及持有之個人資料（包括紙本及儲存媒介物）列冊移交，不得攜離使用，並應簽訂保密切結書。

（十一）本校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本校單位名稱及個人資料來源。

（十二）本校委託他人蒐集、處理或利用個人資料之全部或一部份時，應依個資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。

（十三）本校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。

（十四）本校涉及個人資料檔案相關作業，應遵守本校個人資料保護管理制度之要求與規定辦理。

七、國際傳輸

本校進行個人資料國際傳輸前，應檢視有無主管機關依個資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，同時對資料接收方之告知事項及當事人權利行使權利進行監督。

八、個資事件通報應變

（一）本校應訂定應變機制，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。

（二）本校應於個資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」，通報主管機關（教育部），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，必要時應配合主管機關進行本計畫之之行政檢查作業。

九、業務終止後之個人資料處理作業

本校業務終止後，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。

十、 教育訓練

本校對於個人資料蒐集、處理及利用應符合個資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。

十一、個人資料稽核

為強化個人資料檔案資訊系統存取安全，防止非法授權存取，維護個人資料之隱私性，應建立個人資料保護稽核制度，由本委員會成立「個資料保護稽核小組」定期查考本計畫所定相關事項是否落實執行，並保存稽核資料。

十二、紀錄留存

本校執行本計畫之各項程序及措施，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。

十三、實施本計畫各項作業及管理措施細節，另訂本校個人資料管理制度規範之。

十四、本計畫每年應依法令政策持續規劃、修訂及執行，落實個人資料安全維護作業，以強化本校個人資料安全。

十五、本計畫經資通安全暨個人資料保護委員會通過，陳請校長核定後公布實施，修正時亦同。