敏惠醫護管理專科學校個人資料檔案安全維護管理要點

電算中心

104.08.19 104學年度第1學期第1次行政會議通過

第 一 條　依據『個人資料保護法』、『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實施辦法』及『教育體系個人資料安全保護基本措施及作法』相關規定辦理，落實個人資料之合理蒐集、處理及利用，符合相關法規之要求，特訂定本校『個人資料檔案安全維護管理要點』(以下簡稱本要點)。

第 二 條　本要點名詞定義如下：

一、個人資料：自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、個人資料檔案：依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

三、當事人：指個人資料之本人。

第 三 條　本校得設置個人資料保護聯絡窗口，辦理下列事項：

一、本校個人資料保護之聯繫、協調及緊急應變通報。

二、重大個人資料外洩事件之當事人聯繫與告知。

三、本校各單位個資保護代表名冊之製作及更新。

第 四 條　各處室得指定個人資料保護聯絡窗口以及相關業務承辦人辦理下列事項：

一、本校個人資料保護政策之執行。

二、個人資料保護事項之協調聯繫。

三、負責個人資料個別作業流程之蒐集、處理及利用。

四、盤點及彙整處室個人資料清冊。

五、建立並定期檢視處室業務流程之個資風險與風險對策。

六、處室個人資料緊急事件之通報。

七、處室個人資料保護之自行查核。

第 五 條　本校各項業務活動所需之個人資料，應以最小化為原則做蒐集、處理及利用，並應以適當方式通知當事人下列事項。經當事人書面同意者，應取得當事人同意書；該同意書作成之方式，依電子簽章法之規定，得以電子文件為之。

一、單位名稱。

二、蒐集之目的。

三、個人資料之類別。

四、個人資料利用之期間、地區、對象及方式。

五、當事人依『個人資料保護法』第三條規定得行使之權利及方式。

六、當事人得自由選擇提供個人資料時，不提供對其權益之影響。

適當方式通知當事人，係指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。。

第 六 條　本校基於校務及業務運作下，尊重當事人之權益，依誠實及信用方法，於特定目的範圍內，蒐集、處理及利用個人資料，如有個人資料保護法第十九條但書所定之特定目的外利用時，應告知並取得當事人之書面同意。

第 七 條　當事人向本校個人資料業管單位請求查詢、閱覽或複製個人資料者，應填具本校「當事人個人資料權利行使申請表」並檢附相關證明文件，由資料業管單位主管於十五日內為准駁決定，必要時得予延長至多十五日。前項申請案件有下列情形之一者，應以書面駁回其申請。

一、申請書件內容有遺漏或欠缺，經通知限期補正而逾期未補正者。

二、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益等情形。

三、妨害本校執行法定職務之情形。

四、妨害本校或第三人個人之重大利益之情形。

查詢或請求閱覽個人資料或製給複製本者，本校得另定收費標準酌收必要成本費用。

第 八 條　當事人向本校個人資料業管單位請求補充、更正、刪除、停止蒐集、處理或利用個人資料者，應填具本校「當事人個人資料權利行使申請表」或業管單位個人資料相關申請單，並檢附相關證明文件，由資料業管單位主管於三十日內為准駁決定，必要時得予延長至多三十日。前項申請案件有下列情形之一者，應以書面駁

回其申請。

一、申請書件內容有遺漏或欠缺，經通知限期補正而逾期未補正者。

二、本校因執行職務或業務所必須並有適當註明者。

第 九 條　人員管理措施。

一、各處室若有個人資料處理需求，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。

二、本校教職員於在校服務期間所經辦、保管或接觸之所有個人資料資訊應具有保密之義務，並應簽訂本校「內部人員保密切結書」。

第 十 條　作業管理措施。

一、各處室若有對個人資料特定目的外之利用者，應填寫本校『個人資料利用申請表』，並檢附相關證明文件，向資料業管單位提出申請。 資料業管單位或會簽單位就申請個案認為有審核困難或疑義者，得提送個人資料保護推行委員會核定。

二、若需以可攜式儲存媒體傳遞個人資料時，應將檔案壓縮加密，方可進行資料之傳遞，並於交付時填寫「個人資料交付紀錄」，於個人資料使用完畢後留存資料刪除、廢棄之紀錄。

三、 以電子郵件傳遞含個人資料之檔案時，應將檔案加密，不得以明碼方式傳遞。

四、 針對重要之個人資料，應定期備份，備份檔案應經過壓縮加密。

第十一條　環境安全管理措施。

各單位應依辦公作業環境規劃出個資保護區域，將個人資料放置於上鎖檔案櫃中或實施門禁管理。

第十二條　技術管理措施。

一、 各單位應參照本校「網路及系統安全管理說明書」，定期管理公務電腦，以確保資訊及個人資料之安全。

二、 需定期檢查個人資料系統之狀況與個人資料存取情形。

第十三條　認知宣導與教育訓練。

本校應針對教職員，定期施以認知及教育訓練，以確保教職員熟悉相關法令及提高個人資料保護意識。

第十四條　紀錄維護措施。

為確保所訂定之相關程序確實執行，以及釐清個人資料於蒐集、處理及利用過程之相關權責，各單位應保存以下相關紀錄以供查驗。

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。

第十五條　個人資料安全持續改善措施。

一、個資風險評估作業應每年進行。

1. 各單位應針對個人資料檔案清冊內容，建立風險評量之標準，包括影響及衝擊之程度與風險發生之機率。
2. 個資檔案之風險評估應依實際狀況，對照「影響及衝擊等級表」(表 1)及「風險發生可能性等級表」(表 2)內容，進行風險分析。

表 1 影響及衝擊等級表

	個資數量	敏感程度	影響程度
輕微(1)	50 筆以下	僅有一般識別資料，如姓名、服務單位、職稱、電子郵件地址等。	◎對本校形象無任何影響，資料外洩或遭竄改不致影響當事人權益，資料無須重新取得。 ◎該事件不會造成任何關於法令法規之影響。
嚴重(2)	◎一般個資 51~1,000筆	含有政府資料中之辨識者及財務資料等，如身分證統一編號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。	◎對本校形象造成輕微影響，造成的衝擊可接受；資料外洩或遭竄改對個人權益影響輕微，資料重新取得容易可立即回復。 ◎該事件造成承辦人遭受內部懲處或外部廠商違

			反訂定之契約 。
非常嚴重(3)	◎一般個資 1,001筆以上 ◎特種個資 1筆以上	含有特種個人資料。	◎對本校形象造成嚴重影響(媒體的負面報導)；資料外洩或遭竄改造成大規模個人權益損害，資料重新取得不易無法立即回復。 ◎該事件造成承辦人及其主管遭受懲處或嚴重違反法令規章。

表 2 風險發生可能性等級表

等級	評估標準
可能性低(1)	◎很少發生或無發生可能性 ◎5年期間沒有發生過
可能性中(2)	◎可能發生或偶爾發生 ◎1年內發生次數小於2次(或5年內發生次數小於10次)
可能性高(3)	◎經常發生 ◎1年內發生3次以上

3. 風險值計算

識別風險發生之可能性及影響衝擊程度，將此兩項評分相乘，即計算出該個資檔案之風險值(表 3)。

表 3 風險值

影響及衝擊等級表	風險發生可能性		
	可能性低(1)	可能性中(2)	可能性高(3)
非常嚴重(3)	中(3)	高(6)	高(9)
嚴重(2)	低(2)	中(4)	高(6)
輕微(1)	低(1)	低(2)	中(3)

二、內部稽核管理落實

1. 本校應建立內部稽核管理機制，以確保相關管理措施之有效性。

2. 本校應定期執行稽核作業，並針對缺失與潛在風險，規劃矯正及預防措施。

第十六條　本要點經行政會議通過後，陳請校長核定後實施，修正時亦同。