崇仁醫護管理專科學校個人資料檔案安全維護計畫

104年4月8日資訊安全暨個資保護推動委員會通過

壹、目的

崇仁醫護管理專科學校（以下簡稱本校）為確保個人資料檔案管理之安全，並強化對所保有之個人資料之保護能力，防止個資外洩事件發生，特制訂本計畫。

貳、依據

(一)個人資料保護法。

(二)個人資料保護法施行細則。

(三)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。

(四)教育體系個人資料安全保護基本措施及作法。

參、權責

(一)「資訊安全暨個資保護推動委員會」為本校推動個資保護之管理組織，督導個資保護相關業務。

(二) 校長為「資訊安全暨個資保護推動委員會」主任委員，主任秘書為資安長兼個資保護業務執行長。

(三) 秘書室為個資保護各項業務聯繫窗口。

(四) 各個資保有單位主管及承辦人為個資相關業務負責人。

肆、計畫內容

一、個人資料管理安全

(一)個人資料範圍包含自然人姓名、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)本校「資訊安全暨個資保護推動委員會」為管理組織 ， 督導各單位個資安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

(三)本校應建立風險管理機制 ，以鑑別組織處理相關個資作業於個資生命週期過程中可能產生之風險 ， 釐清並配合適當控制措施，降低風險於可接受範圍內。

(四)本校對個人資料之蒐集、處理、利用、傳輸與銷毀應訂定相關作業程序或作業標準，且符合適當、相關且不過度之使用原則，記錄個人資料之紙本文件或電子檔案，應妥善保管並建立存取管控機制。

(五)執行重點：

1.直接或間接蒐集個人資料時應依法令規定為之，必要時應向當事人盡到告知義務，並取得同意。

2.個人資料之蒐集、處理與利用須評估目的及範圍為適當、相關且不過度，不處理無關或超過原來所陳述使用目的之個人資料。

3.處理個人資料之系統或業務，應每年定期檢視，確保個人資料處理之適當性及不過度使用。

4.個人資料存取權限之授權管理，必須依人員執掌角色所需，且以執行業務及職務所必要的最低資源存取授權為限。

5.含有個人資料之電子檔案或紙本文件，非日常作業之讀取、列印、存檔、交換、分享及銷毀等處理及利用行為，應提出申請，經核准後方可執行，以建立授權、監督及行為記錄機制。

二、事故預防、應變與通報機制

(一)本校應制訂個人資料事故通報及處理之作業程序。

(二)本校秘書室為當事人行使個資法賦予各項權力之請求或申訴事件 之單一受理窗口。

(三)建立完整之內部個人資料事故通報流程，於發生個資外洩事故時，必須告知當事人並留下通報與處理紀錄。

(四)權責單位於處理完成時，應確認應變措施之有效性，隨時回報權責主管及相關單位，並視情況調整應變措施。

三、個人資料保護

本校應確保個人資料受到妥善保護，避免非經授權之閱覽、存取。

執行重點：

(一) 個人資料之存取應與本身業務範圍相關，任何人未經授權不得存取與個人業務無關之個人資料。

(二)各單位公務文書及紙本郵件應有專人負責收發。

(三)針對存有個人資料之紙本文件及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖。

(四)伺服器、電腦應設定螢幕保護程式，並設定密碼或採取登出鎖定方式保護。

(五)個人資料檔案應建立保存期限，並制訂管理保存與銷毀之作業程序。

四、內部稽核管理

本校應將個人資料保護業務納入內部控制制度，並透過定期內部稽核管理，確認個人資訊管理制度與矯正預防措施之實施情形。

五、實體環境與設備安全管理

本校應確保個人資料存放環境與設備之安全，避免未經授權之人員進出辦公環境，處理或儲存大量個人資料之資訊設備，應規劃安全防護作業標準，採取適當隔離控管措施，執行重點：

(一)本校同仁應保持警覺，留意陌生人員進出辦公環境，若發現身 份不明或可疑的人員，應主動詢問其身份，並視需要通報校安中心或警衛室處理。

(二)委外廠商及訪客應於本校各單位指定之區域內活動。

(三)網路環境應建立安全防護機制，網路路由之規劃必須確保任何網路連線或資訊傳輸符合網路存取之安全需求。

(四) 存放個人資料之伺服器、應用系統及資料庫等必須留存存取軌跡相關資訊。

(五) 敏感性系統或處理大量個人資料之資訊設備，應採取適當控管程序或隔離措施。

六、人員管理及認知宣導教育訓練

本校應定期對組織內部人員規劃訓練課程，以提升人員個人資料保護之安全認知及警覺意識，並要求委外廠商人員遵循本校個人資料保護相關規定。

(一)本校同仁、接觸個人資料之外部人員、委外服務廠商人員於在職及離、退職後，均不得洩漏所知悉之機敏資訊，或為不當之使用，否則得視其情節輕重予以處分或追究其民、刑事責任。

(二)權責單位每年應對組織內部人員規劃訓練課程，或派員參加外單位辦理之專業課程，以提升人員個人資料保護之安全認知及警覺意識。

(三)委外廠商人員於專案服務期間所知悉之業務資訊，應遵守「個 人資料保護法」及本校個人資訊管理制度相關規定，且不得對 外透露。

七、個人資料安全持續改善

本校應建立個人資料管理持續改善機制，透過適當的矯正或預防措施，矯正因內部或外來威脅所產生之風險，以達成持續改善之目標，提升整體個資保護安全的強度。