國立恆春高級工商職業學校個人資料安全保護作業要點

中華民國 102年10月07日 行政會報通過

1. 依據：

依據「個人資料保護法」、「個人資料保護法施行細則」、「教育體系資通安全管理規範」、「教育機構個人資料保護工作事項」與「國中、國小資通安全管理系統實施原則」等相關規定為基礎引申訂定之。

貳、目的：

為落實本校所屬各單位紙本、電子檔及電腦列印資料等（以下簡稱個人資料）安全管理機制，確保本校個人資料安全，避免被竊取、竄改、毀損、滅失或洩漏等風險，特訂定「國立恆春高級工商職業學校個人資料安全保護作業要點」（以下簡稱本要點）。

參、適用對象：

本校所屬專（兼）任教師、員工、約聘（雇）人員、工讀生、學生及各業務委外服務之廠商人員。

肆、人員安全管理與訓練：

一、新進人員於報到時，需依照規定填寫到職單，並簽署保密切結書。保密切結書涵蓋期間包括從業期間與離職後，均應有保密之責任，任何因未遵守本管理規範導致之資料安全意外事件將依 相關規定處理。

二、資訊業務委外服務之廠商人員，必須簽署專屬切結書切結遵守本要點規定。

三、各單位員工離職時，須依照規定填寫離職單，並辦妥移交作業（含儲存媒體及資料）。

四、新進人員應由業務單位施以適當的系統操作訓練，避免資訊不當之誤用等狀況。

五、處理個人資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置通行碼外，應視需要更換使用者識別帳號。

六、每年度由學校對員工施以個人資料保護法、國家機密保護法及相關法令等之宣導、訓練或講習，以提昇其法治觀念。

伍、檔案資料之安全管理：

一、各單位處理含個人資料時，應依據「個人資料保護法」及相關規定審慎處理，不得私自蒐集或洩漏業務資訊，非公務用途嚴禁調閱使用。

二、各單位個人資料檔案，應指定專人負責，以為防止個人資料被竊取、竄改、毀損、滅失或洩漏。

三、個人資料或儲存資訊設備應置於實體安全區域（如：抽屜上鎖、門禁控管之辦公區域、機房），避免有心人士或非授權人員存取。

四、本校以外其他機關或個人索取資料應有正式公文，主管單位應依據「個人資料保護法」及相關規定予以審查，並簽奉本校首長核准後始可提供資料。

五、依前款所提供之電腦資料，應做成紀錄，並應請該機關確實依照「個人資料保護法」及相關規定，審慎應用處理取得之資料；另提供電腦列印之資料者，應於所提供之資料上須有「本資料

僅供○○參考，請妥慎保管，嚴禁外流」等字樣。

六、網路公告時，應避免公告當事人全名或其敏感資料，引用資料亦同。

陸、電腦媒體之安全管理：

一、應納入管理之電腦媒體包括儲存公務上應保密資料之可攜帶移動的磁帶、磁碟、光碟及其他儲存裝置、電腦列印之各式資料等。

二、電腦媒體應依保存規格要求，存放在安全的環境，非經簽奉核准，不得攜離辦公場所。

三、媒體儲存的資料，不再繼續使用或逾保存年限時，應將儲存的內容消除；報廢時，應由專人以安全的方式處理，例如：燒毀、以碎紙機處理，或將資料從媒體中完全清除至無法解讀之程度， 例如：硬碟敲毀、低階格式化。

四、電腦資料需經加密作業處理後才得以電子郵件的方式傳送。

五、電腦媒體運送過程，應有妥善的安全措施，以防止資料遭竄改破壞、誤用或未經授權的取用。

六、電腦媒體運送，應慎選安全及可信賴的運送機構或人員，對於機密及敏感性的資料，應採取特

別相關安全保護措施，必要時加派人員運送。

柒、委外作業之安全管理：

一、資訊業務委外時，應於事前審慎評估可能的潛在安全風險（如資料被竊取等），需與廠商簽定

適當的資訊安全協定（如 OWASP 開放 Web 軟體安全計畫），及規範相關的安全管理責任，並納 入契約條款中。

二、委外作業承包之工作人員，如需進入相關系統作業，由委外業務之主管單位依規定申請使用者代碼，並於委外業務完成後立刻依規定撤銷。

三、委外作業鍵入之資料由主管單位指派專人核對以確保資料之正確性，委外資訊除安全管理責任外，尚應落實保密作為。

四、資訊支援或維護服務人員需由資訊人員或電腦管理員陪同或經授權並登記，始得進出管制區域。

捌、資訊作業安全守則：

一、電腦應設定密碼確實保密。

二、電腦應設定螢幕保護程式（啟動時間設定為 15 分鐘內）並設定密碼保護。

三、電腦之作業系統漏洞應即時更新修補。

四、電腦應安裝防毒軟體並即時更新病毒碼。

五、應定期將重要資料備份存放。除管理需求及經授權外，禁止使用密碼破解、網路監聽工具軟體， 並不得突破他人帳號，中斷系統服務。

六、不得在任何公開的新聞群組、論壇、或公佈欄中透露任何有關本校資訊細節。

七、開啟來路不明之電子郵件及其附件時應謹慎小心，以防電腦中毒。

八、當有跡象顯示系統可能中毒時，應儘速通知相關人員。

九、禁止濫用系統及網路資源，複製與下載非法軟體。

十、嚴禁開啟網路芳鄰分享目錄與檔案。

十一、嚴禁使用即時通訊軟體傳輸個人資料檔案。

十二、嚴禁使用作業系統 Guest 帳號，無使用帳號應立即停用。

十三、嚴禁使用非公務網頁式電子郵件傳輸個人資料檔案。

玖、密碼設置安全守則：

一、應保護密碼，維持密碼的機密性，使用者應至少每 6 個月更換密碼一次，並禁止重複使用相同 的密碼。

二、應避免將密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。

三、當有跡象顯示系統及密碼可能遭破解時，應立即更改密碼。

四、密碼的長度最少應有 8 位長度，且應符合密碼設置原則。

五、密碼設置原則，應儘量避免使用易猜測或公開資訊為密碼設定基礎，建議須包含英文字母及數字混合而成。

拾、通報處理機制：

一、設置校長為個資隱私業務之機關召集人。

二、設置個人資料保護窗口負責人為秘書，並應將「個資保護聯絡窗口」之聯繫方式（如：電話、email）置於單位網站，以便利民眾提出申訴與救濟。

三、各處室需指派乙名主管擔任「個資管理代表」，辦理安全維護及保管事項，個資之調閱需由調閱人員向該處室提出申請，經該單位之個資管理代表核可後方能調閱。

四、各單位人員發現有資料洩漏或違反本要點及「個人資料保護法」等事件時，應迅速通報單位個資管理代表、人事主任及窗口聯絡人處理。

五、資料洩漏者之行為若觸犯法律規定，並構成犯罪事實時，由人事室、本校個人資料管理代表成員進行查處。

拾壹、安全稽核：

一、每年得辦理電腦系統資料安全管制稽核作業，查核是否按本要點之規定辦理。

二、前款稽核作業事宜，由人事主任(會同設備組)執行，並得併同年度資訊安全稽核工作辦理。

三、為因應突發性、專案性或特殊性之需要，得不定期針對特定目的之項目、單位或人員進行專案稽核工作。

四、稽核作業至少每年稽核乙次，稽核完之個人資料保護檢核表需交予人事室留存以備政風單位查

驗。

拾貳、各單位教職員工、約聘（雇）人員、工讀生、學生及委外服務人員違反本要點規定者，視其情 節輕重，依相關規定予以處分，或依法追究其民、刑事責任。

拾參、學校應於法律允許之範圍內提供資料當事人下列權利：

一、查詢或請求閱覽。

二、請求製給複製本。

三、請求補充或更正。

四、請求停止蒐集、處理或利用。

五、請求刪除。

拾肆、本要點如有未盡事宜，悉依相關法令之規定辦理。 拾伍、本要點經行政會報通過後，陳請校長核定後實施。