新竹市光復高級中學資訊安全管理作業要點

建議文件機密等級：限閱

一、目的

為確保新竹市光復高級中學（以下簡稱「本校）資訊安全管理作業推行，符合資訊安全政策之目標，特訂定本作業要點。

二、適用範圍

本政策適用之管理範圍為本校教職員與學生個人資料處理及其相關資訊服務。

三、權責

(一)資訊安全長：由校長擔任，負責綜理資訊安全管理作業協調與督導工作。

（二）資訊安官：由圖書館主任擔任，負責規劃及管理資訊安全管理作業相關事宜。

(三)執行小組：由資訊媒體組長擔任，負責執行資訊安全管理作業相關事宜。

(四)稽核小組：由人事室擔任，負責規劃及執行資訊安全管理作業稽核工作。

(五)全體人員（含委外廠商)：配合及遵守資訊安全各項要求及規定。

四、相關文件

(一)教育體系資通安全管理規範

(二)資訊安全政策

(三)人員安全守則

(四)保密切結書

(五)外部連絡清單

(六)教育訓練簽到表

(七)內部(含)委外人員移交列表

(八)資訊服務申請表

(九)委外廠商保密切結書

(十)設備進出紀錄表

(十一)異常事件紀錄表

(十二)資訊安全事件報告單

(十三)適用法規清單

(十四)內部稽核計畫

(十五)內部稽核報告

(十六)矯正與預防處理單

(十七)加密 WORD 檔案步驟

五、作業說明

(一)資訊安全組織

1.資訊安全長須每年至少召開一次資訊安全管理審查會議，討論內容包括如下：

(1)資訊安全稽核與審查之結果。

(2)來自利害相關者之回饋。

(3)可用於組織以改進資訊安全績效與有效性之技術、產品或程序。

(4)預防與矯正措施之執行狀況。

(5)資安政策目標達成性衡量結果。

(6)前次相關會議結論之跟催結果。

(7)可能影響資訊安全管理作業之任何變更。

(8)加強或改進資訊安全的其他各項建議。

2.管理審查會議討論結果應包含：

(1)資安政策目標之改進。

(2)因為下列項目之變更，所進行之因應措施。

A、各項營運要求。

B、各項安全要求。

C、影響既有各項營運要求之營運過程。

D、法律或法規各項要求。

E、契約的各項義務。

(3)資源需求。

3.管理審查會議應留存相關會議紀錄備查。

4.資訊處理設備之使用，應具授權程序。

5.本校教職員應簽署「保密切結書」(詳附件一)，課予機密維護責任。

6.為確保資訊安全作業的順利運行，應建立能與相關外部團體(警消單位、主管機關、廠商等）即時連繫之「外部連絡清單」(詳附件二)。

7.任何資訊委外業務，皆應考量與包含資訊安全需求，且明訂廠商之資訊安全責任及保密規定，並列入契約。

(二)資訊資產分類與管制

1.為確實掌控資訊資產現況，各單位須編製資訊資產清冊（詳附件三）並每年更新一次。

2.資訊資產應進行分級，各類資訊資產依據機密等級分為 4 級：一般、限閱、敏感、機密。各級之評估標準如下：

(1)一般：無特殊之機密性要求，可對外公開之資訊。

(2)限閱：僅供組織內部人員或被授權之單位及人員使用。

(3)敏感：僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用。

(4)機密：為組織、主管機關或法律所規範之機密資訊。

(5)資訊資產可依其機密等級進行標示，標示方式如下：

A、實體設備之機密等級標示應以不同顏色標籤區分，一般等級者為藍色標籤;限閱等級者為綠色標籤;敏感等級者為黃色標籤;機密等級者為紅色標籤。

B、文件類別之機密等級應於文件封面做明確的標示。

3.考量重要資訊資產的需求，於必要時制定保護措施及處理流程。

（三）人員安全管理與教育訓練

1.本校應依主管機關要求，辦理資訊安全教育訓練及宣導，強化教職員資訊安全認知，必要時，應請委外廠商人員一同參與資訊安全教育訓練，並留存「教育訓練簽到表」(詳附件四）或其他訓練紀錄備查。

2.人員離職，須依流程辦理資訊資產移交，並即時移除相關存取權限，且填寫「內部（含）委外人員移交列表」(詳附件五）存查備查。

3.各單位若有資訊服務需求（如：帳號申請、電腦維修、系統開發或程式修改等)，應填寫「資訊服務申請表」(詳附件六)，經權責主管核准後，交由資訊單位依需求處理。

4.本校教職員工之資訊安全管理相關規定，須遵守「人員資訊安全守則」。

5.本校委外廠商所執行之業務，若涉及個人隱私資料，承辦人員應要求其簽訂「委外廠商保密切結書」(詳附件七)。

6.對於委外廠商提供之服務，承辦人員應監視和審查，確認服務內容滿足合約之要求。

7.委外廠商（人員）異動、合約到期或其他因素服務終止時，承辦人員須確認其歸還各項設備、軟體、文件或鑰匙等，並取消或調整存取權限，且填寫「內部（含）委外人員移交列表」(詳附件五）存查備查。

(四)實體與環境安全

1.學校應採取適當防護措施以保障人員辦公處所安全。

2.重要資訊設施應設置於機房，並確保經授權人員方可進出。

3.機房應採取適當的控制措施與指引，確保其安全性。

4.機房內應保持整齊清潔，並嚴禁飲食或堆置易燃物。

5.機房宜設置足量之不斷電系統（UPS)，確保重要資訊設備在非預期斷電情況下能具足夠電源完成緊急處置。

6.冷氣機、不斷電系統（UPS）等機電設備之使用，應依照設備說明書指示操作，並施行檢查作業。

7.資訊設備報廢與再使用時，應將含有個人隱私資料及有版權的軟體移除。

8.禁止資訊設備在未經授權之情況下攜離所屬區域，若需將設備攜出，應填寫「設備進出紀錄表」(詳附件八)。

（五）通訊與作業安全管理

1.資訊單位應建立資訊系統之安全控管機制，保護資料、系統及網路作業，防止未經授權之存取。

2.伺服主機及網路設備應指定負責人，確保設備正常運作。

3.新資訊系統、系統升級，正式上線前應適當的測試，並依驗收規定完成驗收。

4.學校內電腦（伺服主機、個人電腦、筆記型電腦等）應安裝防毒軟體，定期更新病毒碼；伺服主機應定期掃描。

5.各項系統資料（如：設定檔、網頁資料、伺服器日誌、資料庫等）應由系統負責人執行定期備份。

6.系統資料以可攜式儲存媒體保存時，應將該儲存媒體存放於上鎖儲櫃或安全處所。

7.可攜式儲存媒體若存有個人隱私資料，應加密儲存或實施安全控管措施，可參閱「加密 WORD 檔案步驟」。

8.可攜式儲存媒體的遞送，應妥善包裝保護。

9.系統負責人變更系統作業程序時，應適時修改維護相關文件（如：系統文件、操作手冊等）。

10.對外開放之資訊系統，其帳號密碼、個人資料等機密性資料傳輸過程應以加密方式（參閱「加密 WORD 檔案步驟」）處理，並妥善保管該資料，防止遭竊取或擅自挪作他途之用。

11.以電子郵件傳送含有個人隱私之資料時，宜以加密機制（參閱「加密 WORD 檔案步驟」）保護。

12.學校網頁資訊之公布，應經權責管理人員審查，確認內容未含個人隱私之資料及無違反學校規定與法令、法規之要求。

13.重要系統應留存電腦稽核紀錄，並妥善保護與保存，以作為日後調查及監督之用。

14.系統管理人員發現資訊系統異常、駭客入侵等異狀時，應進行緊急應變處置並通報權責主管，並填寫「異常事件紀錄表」(詳附件九)，留存系統異常處理紀錄備查。

15 系統管理人員應每月執行一次系統校時。

（六）存取控制安全

1.資訊系統使用權限之申請、異動應依「資訊服務申請表」(詳附件六)流程辦理；使用權限之終止，應依離職程序辦理。

2.使用者職務異動或離職時，使用單位應通知資訊單位，調整或終止使用者之存取權限。

3.各項設備與系統相關之使用權限（例如使用者帳戶與作業權限）宜有授

權紀錄，以備查核。

4.系統管理人員結束系統操作應登出系統，並鎖定主控台螢幕。

5.宜依業務性質之不同，區分不同內部網路網段，例如：教學、行政、宿網等，以降低未經授權存取之風險。

6.網路管理人員應定期監控網路使用狀況，例如：網路流量、封包等，以及早發現異常狀況。

7.對於開放提供外部使用者或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。

8.避免委外廠商使用系統管理者帳號（例如：Root、Adminstrator）或共用帳號，以釐清責任。

(七)系統開發與維護之安全

1.系統開發應包含安全性功能之規劃。

2.應用系統之資料輸入，應檢核、過濾主要欄位之資料輸入或資料內容，以確保資料的有效性及真確性。

3.輸出之資料，應確認其正確性；對於系統內之資料處理，則須保護其完整性。

4.作業系統變更，應審查與測試，以確保現行資訊系統與服務正常運作。

5.系統軟體應由系統負責人進行安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

(八)資訊安全事件之反應及處理

1.資訊安全事件依影響等級區分為4個級別，由重至輕分別為「4級」、「3級」、「2級」及「1級」。

(1)「4」級事件，符合下列任一情形者：

A、法令、法規所規範應保護之資料外洩（例如：個人隱私資料）。

B、重要系統或資料遭竄改、破壞或嚴重毀損。

(2)「3」級事件，符合下列任一情形者：

A、敏感資料外洩（如：財會資料、系統文件）。

B 重要系統運作停頓，影響業務正常運作。

(3)「2」級事件，符合下列任一情形者：

A、內部行政資料外洩（如：校內行政資料）。

B、非重要系統運作遭影響或系統停頓，已影響業務正常運作。

(4)「1」級事件，符合下列情形者：

系統運作遭影響或系統停頓，不致影響業務正常運作。

2.人員發現資訊安全事件，應即時通報，並記錄於「資訊安全事件報告單」（詳附件十），或教育機構資安通報平台(TACERT)。

3.資訊安全事件確認處理完成後，相關單位應檢討現行管理措施之完整性，

必要時進行檢討會議，討論改善之事宜。

（九）相關法規與施行單位政策之符合性

1. 學校應蒐集相關法律條文（如：智慧財產權、資料隱私保護及其他相關法規)、管理規定及合約要求，以確保相關作業符合要求，並填寫適用法令法規項目至「適用法規清單」(詳附件十一）存查備查。
2. 學校應定期進行弱點掃描或滲透測試，確保資訊系統之運行符合既定之安全實施標準，執行結果應留存紀錄。
3. 應於內部稽核前，規劃「內部稽核計畫」(詳附件十二)，內容包含詳細時程、範圍、參與人員、工作分派、稽核地點等稽核活動細節，以作為施行稽核作業之依據。
4. 內部稽核作業施行結果應產出「內部稽核報告」(詳附件十三)，並依稽核結果所發現之缺失項目分析發生原因，並提出改善或預防未來再發生之改善措施或計畫。為便利追蹤改善之情形，填寫「矯正與預防處理單」（詳附件十四）以作為追蹤之依據。

六、違反規定之處理

（一)人員未遵循上述規定者，視情節重大，提報校務會議議處。

七、本作業要點提行政會議決議， 校長核准後公告實施，修訂時亦同。