資訊安全管理作業要點

104 年 2 月 24 日校務會議通過
113 年 6 月 17 日行政會議修訂
113 年 6 月 28 日校務會議通過

一、目的

為確保私立正德高級中學(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

本作業要點適用之管理範圍為本校教職員工與學生個人資料處理及其相關資訊服務。

三、權責

1. 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。
2. 資訊安全官：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。
3. 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。
4. 稽核小組：由教務主任、學務主任、輔導主任、國中部主任、國小部主任、總務主任、會計主任、人事主任擔任，負責規劃及執行資訊安全管理作業稽核工作。
5. 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

1. 保密切結書(附件一)
2. 外部連絡清單(附件二)
3. 資訊資產清冊(附件三)
4. 資訊服務申請表(附件四)
5. 委外廠商保密切結書(附件五)
6. 設備進出記錄表(附件六)
7. 異常事件記錄表(附件七)
8. 資訊安全事件報告單(附件八)
9. 資訊安全政策(附件九)
10. 學校人員安全守則(附件十)

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. 資訊安全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。

①各項營運要求。

②各項安全要求。

③影響既有各項營運要求之營運過程。

④法律或法規各項要求。

⑤契約的各項義務。

(3)資源需求。

3. 資訊安全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，並列入契約中。

(二)資訊資產分類與管制

1. 為確實掌控資訊資產現況，總務處必須協助各單位編製資訊資產清冊並定期更新「資訊資產清冊」詳(附件三)。

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：

①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。

②文件類別之機密等級應於文件封面做明確的標示。

(6)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。
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。
3. 各單位若有資訊服務需求(如：帳號申請、電腦維修、軟體安裝或其它資訊服務等)，應填寫「資訊服務申請表」詳(附件四)，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「資訊安全政策」詳(附件九)、「學校人員資訊安全守則」詳(附件十)。
5. 本校教職人員、約聘(僱)人員及工讀生於到職時應簽署「保密切結書」詳(附件一)，並克盡保密之責。
6. 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(附件五)。
7. 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。
8. 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。

(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. 學校資訊設備挪做其他用途或報廢時，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(附件六)。

(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。
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，宜以加密機制保護。
12. 學校網頁資訊之公布，應由各處室主任依循申請程序提出，經權責管理人員審查並確認內容未含個人隱私資料及無違反學校規定與法令、法規之要求，校長核可後公布之。
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(附件七)，留存系統異常處理紀錄備查。
15. 系統管理人員應每季執行一次系統校時。

(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(附件四)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. 資訊安全中事件依影響等級區分為 4 個級別，由重至輕分別為「4」級事件、「3」級事件、「2」級事件、「1」級事件。

   (1)「4」級事件，符合下列任一情形者：

   ①法令、法規所規範應保護之資料外洩(例如：個人隱私資料)。

   ②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：

   ①敏感資料外洩(如：財會資料、系統文件)。

   ②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：

①內部行政資料外洩(如：校內行政資料)。

②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(附件八)。

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：著作權法、智慧財產權、個人資料保護法及其他相關法規)、管理規定及合約要求，以確保相關作業符合要求。

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. 系統稽核工具之使用應審慎進行，避免造成系統中斷；系統稽核工具應妥善保管，避免遭誤用。

六、違反規定之處理

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討論，經校務會議通過後陳請校長公布實施，修正時亦同。

（附件一）

保密切結書

本人 _____將嚴守工作保密規定與國家相關法令對業務機密負完全保密之責，保護所接觸到的個人資料，並尊重智慧財產權。絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體，違者願負法律責任。

此致

私立正德高級中學

立同意書人：_____

身分證字號：___－___ ___ ___ ___ ___****

電　　話：_____

住　　址：_____

中　華　民　國　　年　　月　　日

（後續--個人資料提供同意書）

（附件一）

個人資料提供同意書

本同意書說明私立正德高級中學（以下簡稱本校）將如何處理本表單所蒐集到的個人資料，當您勾選「我同意」並簽署本同意書時，表示您已閱讀、瞭解並同意接受本同意書之所有內容及其後修改變更規定。

一、本校因執行業務蒐集您的個人資料包括姓名、身分證字號、電話、地址等。

二、若您的個人資料有任何異動，請主動向本校人事室申請更正，使其保持正確、最新及完整。

三、若您提供錯誤、不實、過時或不完整或具誤導性的資料，您將損失相關權益。

四、您可依中華民國「個人資料保護法第3條」，就您的個人資料行使以下權利：

1. 查詢或請求閱覽。
2. 請求製給複製本。
3. 請求補充或更正。
4. 請求停止蒐集、處理或利用。
5. 請求刪除。

五、本校利用您的個人資料期間為即日起至離職生效日止，利用地區為台灣地區。

六、除非取得您的同意或其他法令之特別規定，本校絕不會將您的個人資料揭露予第三人使用。

七、僅有經過授權的人員才能接觸您的個人資料，相關處理人員皆簽有保密合約，如有違反保密義務者，將會受到相關的法律處分。

八、本同意書可能會因應個人資料保護法或其他相關法規，以及實際需求進行修正。

□ 我瞭解與同意以上文字＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿簽章

中　　華　　民　　國　　年　　月　　日

（附件二）

外部連絡清單

單　位	聯　絡　人					備　註
	職　稱	姓　名	電　話	手　機	電子郵件/地址	

（附件三）

資訊資產清單

文件編號：　　機密等級：□一般 ■限閱 □敏感 □機密

紀錄編號：　　填表日期：＿＿＿＿年＿＿＿＿月＿＿＿＿日

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
資產類別：通訊(CM)、資料(DA)、文件(DC)、環境(EV)、硬體(HW)、人員(PE)、軟體(SW)										

（附件四）

資訊服務申請表

紀錄編號：＿＿＿＿＿＿＿＿　　填表日期：　　年　　月　　日

問題分類	☐ 教務處 ☐ 學務處 ☐ 輔導室 ☐ 實習處 ☐ 總務處 ☐ 會計室 ☐ 人事室 ☐ 國中部 ☐ 國小部 ☐ 其他
申請項目	☐ 帳號申請 ☐ 電腦維修 ☐ 軟體安裝 ☐ 其他＿＿＿＿＿＿＿＿＿＿＿＿
用途說明 問題描述	
附　　件	

申請單位	
申請人	單位主管

資訊媒體組					
評估結果	☐ 配合辦理，可於時限內完成　☐ 配合辦理，無法於時限內完成 ☐ 尋求委外廠商　☐ 尋求＿＿＿＿＿＿協助 ☐ 不建議執行　☐ 其他＿＿＿＿＿＿＿＿				
處理情形					
接案日期		預定完成日期		完成日期	
承辦人		單位主管			

（附件五）

委外廠商保密切結書

具保密切結廠商（人員）＿＿＿＿＿＿＿＿＿＿於民國　　年　　月　　日起於私立正德高級中學執行「＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿」業務(或專案)，因而知悉貴校機密或任何不公開之文書、電子資料、圖畫、消息、物品或其他資訊，將恪遵保密規定，未經貴校書面授權，不得以任何形式利用或洩漏、告知、交付、移轉予任何第三人，如有違誤願負法律上之責任。

此致

私立正德高級中學

具切結書委外廠商（人員）：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

身分證字號／護照號碼（人員）：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

代 表 人（委外廠商）：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

統一編號：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

地　　址：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

中　　華　　民　　國　　年　　月　　日

（附件六）

設備進出紀錄表

填表日期：　　年　　月　　日

□攜入 □攜出	日　期 時　間	年　月　日 時　　分	攜入／出人員 單　　位	
設備名稱			設備序號	
設備品牌/規格				
攜入/出方式	□自行攜入／出 □貨運代送(貨運編號：＿＿＿＿＿＿＿＿＿＿＿＿) 公司名稱／電話：＿＿＿＿＿＿＿＿＿＿＿＿) □其他(請說明：＿＿＿＿＿＿＿＿＿＿＿＿＿＿)			
攜入/出原因	□備份媒體異地儲存 □異地儲存之備份媒體送回 □新增設備 □設備送修(預計修復完成日期：　　／　　／　　) □調／□借／□還 其他單位：＿＿＿＿＿＿＿＿＿＿＿＿ 聯 絡 人：＿＿＿＿＿＿＿＿＿＿＿＿ 聯絡電話：＿＿＿＿＿＿＿＿＿＿＿＿ (預計歸還日期：　　／　　／　　) □其他(原因說明：＿＿＿＿＿＿＿＿＿＿＿＿＿＿)			

覆核單位	
承辦人	權責主管

（附件七）

異常事件紀錄表

編號：_____ 填表日期：_____年____月____日

異常原因 資產名稱：_____ 異常項目(說明)：
處理說明 異常排除時間：　　年　　月　　日　　時　　分

承辦人	權責主管

（附件八）

資訊安全事件報告單

通報單位聯絡資料			
單位名稱		通 報 人	
電　　話		電子郵件	

資訊安全事件通報事項	
發生時間	_____年____月____日____時____分
設備資料	IP位址（無；可免填）： Web位址（無；可免填）： 設備廠牌、機型： 作業系統名稱、版本： 已裝置之安全機制：

資訊安全事件資料				
事件影響等　　級	☐ 4級	☐ 3級	☐ 2級	☐ 1級
事件分類	☐ 非法入侵	☐ 感染病毒	☐ 阻斷服務	☐ 其他
破壞程度	☐ 系統當機	☐ 資料庫毀損	☐ 網頁遭篡改	☐ 其他
事件說明				
可能影響範圍及損失評估				
應變措施				
期望支援項　　目				
解決辦法				
解決時間	_____年____月____日____時____分			

權責單位	會辦單位	資訊安全官

（附件九）

資訊安全政策

一、目的

為確保私立正德高級中學(以下簡稱本校)資訊安全管理作業，維護資訊及其處理設備之機密性、完整性及可用性，並符合相關法令、法規之要求，特訂定本政策。

二、適用範圍

本政策適用之管理範圍為本校各單位所提供的各項資訊相關服務與個人資料為實施範圍。

三、資訊安全管理範疇

資訊安全分為下列11項領域，進行管理:

1. 資訊安全政策訂定與評估。
2. 資訊安全組織。
3. 資訊資產分類與管制。
4. 人員安全管理與教育訓練。
5. 實體與環境安全。
6. 通訊與作業安全管理。
7. 存取控制安全。
8. 系統開發與維護之安全。
9. 資訊安全事件之反應及處理。
10. 業務永續運作管理。
11. 相關法規與施行單位政策之符合性。

四、目標

本校資訊安全管理目標分定性化指標及定量化指標。

(一)定性化指標

1. 確保本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全。
2. 保護本校個人隱私資訊之安全，確保資訊需經授權人員才可存取資訊。
3. 保護本校個人隱私資訊之安全，避免未經授權的修改。
4. 確保本校各項業務服務之執行符合相關法令或法規之要求。

(二)定量化指標

1. 網路服務品質，需達全年上班時間網路正常服務時間可用性 98%。

   註：計算公式；

   可用性＝1－（中斷時數÷（9小時×5天×52週）
2. 資料遭未經授權之異動、毀損、誤植或其他非預期性事件影響資料正確性，已衝擊業務正常運作之資安事件，全年不得超過三件。
3. 校譽傷害、經濟損失、個人權益嚴重受損或犯罪觸法之資安事件，全年不得超過三件。

五、責任

1. 由校長統籌資訊安全事項推動。

2. 本校各單位主管應積極參與及支持資訊安全管理作業,並透過適當的作業管理程序達成本政策目標。

3. 本校全體人員、委外服務廠商與訪客等皆應遵守本校資訊安全相關規定。

六、審查

本政策應每年至少審查一次，以因應政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

七、實施

本政策提行政會議討論，經校務會議通過後陳請校長公布實施，修正時亦同。

（附件十）

學校人員資訊安全守則

一、禁止共用帳號及密碼，當發現帳號密碼可能遭破解時，應立即更改密碼。

二、六個月至少更換密碼 1 次。

三、密碼設置長度應至少 8 碼，且避免使用下列方式設定密碼：

1. 純數字。
2. 自己的英文名字、生日、電話等個人資料。
3. 與帳號相同。
4. 簡單的連續英文字元，例如 aaaa。
5. 簡單的英文字元加數字，例如 abc123。
6. 電腦鍵盤上的連續字元，例如 asdf、qwerty。
7. 單字或簡單詞語。

四、未經核可，禁止私自使用或下載未經授權及與業務無關之軟體（如：P2P 軟體）。

五、提防來路不明之電子郵件及其附件，勿隨意開啟。

六、電子郵件發送應避免洩露他人個資。

七、如發現疑似電腦中毒、駭客入侵，應通知電算中心處理。

八、電腦應設定閒置 15 分鐘自動啟動螢幕保護程式，並設定鎖定密碼。

九、電腦作業系統弱點應即時更新修補。

十、電腦應安裝防毒軟體且即時更新病毒碼。

十一、使用行動裝置(包括行動硬碟、隨身碟等)，必須先以防毒軟體進行掃瞄。

十二、本守則提行政會議討論，經校務會議通過後陳請校長公布實施，修正時亦同。