醒吾科大 教職員資安意識宣導

資訊圖書處 製

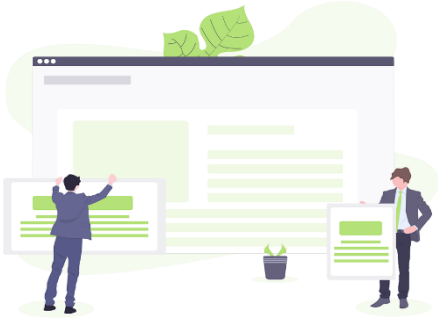
依據高教深耕計畫資安專章評核指標之要求，為強化學校人員資通安全認知，以提升教職員資安意識，特進行以下事項宣導：

- 資訊及系統使用原則
- 電子郵件使用及防範惡意軟體
- 辦公實體環境安全
- 電腦使用安全及行動設備安全
- 儲存媒體防護措施
- 資料安全加密保護措施
- 限制大陸廠牌資通訊產品
- Google表單蒐集個資應注意事項
- 資安事件通報
- 網頁遭置換緊急應變處理

資訊及系統使用原則

- 使用資訊及資通系統前應經其管理人授權，並留意其資通安全要求事項，負對應之責任。
- 資訊處理設施的授權過程應制定安全控管，使用資訊及資通系統時，新增、異動或使用須經過授權程序，資訊存取權限之設定以工作所需之最小權限與最少資訊為原則。
- 非本校同仁使用本校之資訊及資通系統，應確實遵守本校之相關資通安全要求，且未經授權不得任意複製資訊。
- 針對有必要特別保護系統，應嚴格管制並建立申請系統存取特別權限之授權程序，權責主管審查系統存取特別權限名單，宜以執行業務及職務所必要者為限。

電子郵件使用

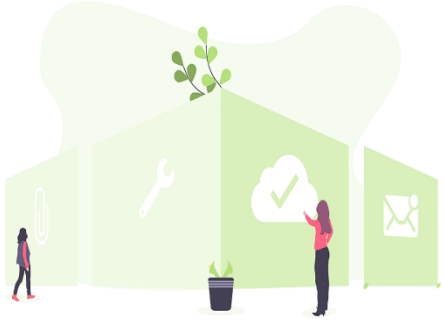


- 機敏公文不得以電子郵件傳送，含有個人資料之信件必須加密傳送。
- 電子郵件加簽以避免發送匿名或偽造。
- 不得利用公務電子郵件進行侵害他人權益、違法之行為。(包括以電子郵件大量傳送廣告信、連鎖信或無用之信息，或以灌爆信箱、掠奪資源等方式。或以電子郵件、線上互動或類似功能之方法散布詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息。)
- 遵循本校「校園網路使用規範」及「電子郵件使用規範」相關規定。

防範惡意軟體

- 學校主機及個人電腦應安裝防毒軟體，並時常進行軟、硬體之必要更新或升級。如需使用外來的可攜式設備或媒體，應確認設備未遭受病毒感染。
- 電子郵件須先經過防毒軟體掃描，並禁止開啟來路不明之檔案或電子郵件及其附加檔案，以避免遭受病毒攻擊。正確配置瀏覽器之安全設定，建議設定在中級風險等級(含)以上。
- 為有效控制「免費軟體」或「共享軟體」的使用，使用人員須事先瞭解其相關版權規定，並且不得任意自行安裝及散佈未經授權之軟體。
- 使用者應避免瀏覽已知或有嫌疑之惡意網站。
- 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

辦公實體環境安全

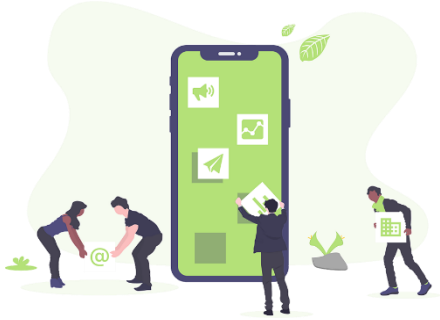


- 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
- 為降低因媒體劣化所造成之無法讀取資料風險，應建立並維持資料備份。
- 針對存有個人資料之紙本文件及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖。
- 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。
- 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

電腦使用安全

- 電腦、業務系統或自然人憑證，若超過十分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證，下班時應關閉電腦及螢幕電源 。
- 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
- 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
- 筆記型電腦及實體隔離電腦定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
- 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

行動設備安全



- 使用可攜式設備與媒體時，應謹慎防範資訊洩漏或妨害組織利益等情節發生，資料攜入或攜出，主管應盡控管之責，提醒使用人員自我要求。
- 私人可攜式設備與媒體，應評估風險後方可存取公務資料。
- 處理內部使用等級以上資料工作區域，未經許可禁止使用相關設備進行拍攝或是螢幕畫面捕捉之行為，使用時需有工作區域管理人員在場陪同。

儲存媒體防護措施

- 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。
- 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。
- 為降低媒體劣化所造成之無法讀取資料風險，宜定期將所儲存資訊傳送至其他媒體 。
- 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

資料安全加密保護措施

- 學校之機密資訊於儲存或傳輸時應進行加密。
- 將「機敏」或「限閱」等級之資訊資產存放於可攜式設備與媒體時，應採取適當加密處理或保護措施，避免遺失時洩漏資訊。
- 採用加密保護措施應遵守下列規定：
  - 採用尚未被破解或尚無被破解疑慮之公開演算法。
  - 保護私密金鑰或解密資訊之機密性。
  - 建立私密金鑰或解密資訊之備份。
  - 對私密金鑰或解密資訊及期備份實施邏輯與實體之存取控制。
  - 一旦加密資訊具遭破解跡象，應立即更改私密金鑰或解密資訊。

限制大陸廠牌資通訊產品

- 除因業務需求且無其他替代方案外，不得採購及使用主管機關核定屬危害國家資通安全之生產、研發、製造或提供之廠商及產品。
  - 於請購資通訊產品時，可要求廠商在簽約時提供非大陸廠牌之切結書或是於合約條款明訂禁止陸製廠牌資通訊設備產品(含硬體、軟體、服務)。
- 既有使用的危害國家資通安全產品，應列冊管理，並指定特定區域及特定人員使用，且不得傳播影像或聲音供不特定人士直接收視或收聽，購置理由消失或使用年限屆滿應立即銷毀。
- 各單位自行或委外營運，提供公眾活動或使用之場地，應將限制聲明納入委外契約或場地使用規定中，並督導辦理。

Google 表單蒐集個資應注意事項

- 個資蒐集聲明
  - 使用Google表單蒐集個人資料，需一開始明確告知個人資料蒐集、處理及利用方式。
- 最少蒐集原則
  - 只蒐集必要且需要的資訊，不過度蒐集個人資訊，以減少資料保管之負擔。
- 保護作答內容
  - 避免不小心公開作答內容，請勿勾選【顯示摘要圖表和其他作答內容】，避免使用者能瀏覽其他使用者資料，造成個人資料外洩。
- 不發布到網路
  - Google表單連動試算表，請勿設定【發布到網路】，避免任何知道網址的人，都可以瀏覽所有填答者的資料。

Google 表單蒐集個資應注意事項

- 不共用資料夾及限制存取權限
  - Google表單連動資料表共用設定一要設定為【限制】，只有取得授權的使用者才可以開啟。
- 資料保存期限
  - 蒐集之個資應訂定保存期限，並於期限或業務終止後，將蒐集之個資予以銷毀(包括表單及其連動資料表)，以降低個資外洩的風險。

資安事件通報

- 什麼狀況下要進行資安通報？
  - 當公務電子郵件遭遇到侵害權益、假冒來源、信件內容有惡意連結時。
  - 公務電腦遭遇到無法解決的病毒、木馬，或有人使用可疑的免費共享軟體時。
  - 各單位自行建置之系統發生重大異常事件，以致於機敏性資料外洩時。
- 如發生以上狀況，請儘速聯絡本校資安通報窗口【資訊圖書處】
  - 依據「臺灣學術網路各級學校資通安全通報應變作業程序」之要求，如經確認為資安事件，需於1小時內至教育機構資安通報平台登錄通報，並依事件等級於時限內完成應變處理。

網頁遭置換緊急應變處理

- 目前各系、所、單位網站多已統整至單一平台並由資訊圖書處進行管理，如各單位發現所屬網站內容遭竄改、頁面遭置換等狀況，請聯絡【資訊圖書處】網頁管理窗口。
- 本校網頁遭置換緊急應變處理原則
  1. 原網站下架：LOG完整保存
  2. 切換維護公告網頁：靜態頁面放置備援主機，以十分鐘完成為目標
  3. 靜態資訊網頁呈現：確定網站安全後，恢復部分優先服務
  4. 逐步功能恢復：系統進行弱點掃瞄，確認更新後無重大安全性弱點
  5. 網站全面恢復：持續觀察一段時間，確認無異常狀況後，即恢復原網站。