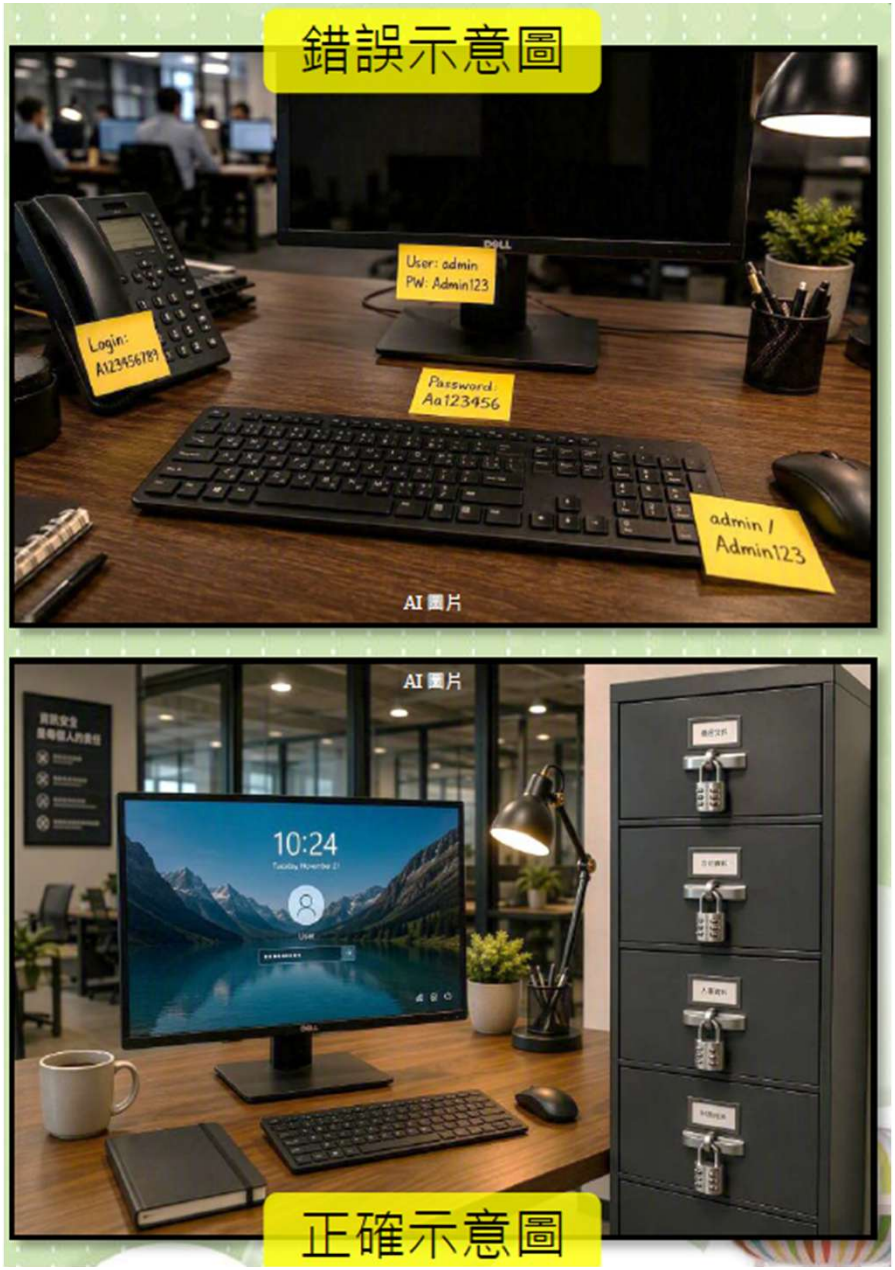
115資訊安全教育訓練

獅湖國小 1007

資料來源:115高雄市資訊組長座談會簡報

善盡個人帳號密碼保管責任。

- **嚴禁使用公務E-mail註冊登錄在非公務相關的外部網站（如：購物平台、社群媒體或遊戲帳號）。**
- **公務網站的登入密碼，不可與私人網站相同（如：購物平台、網路銀行、社群媒體或遊戲帳號、APP）。**
- 不將個人資料、帳號、密碼放置桌面上或張貼在螢幕旁邊等明顯處。
- 啟用電腦登入機制及閒置超過15分鐘螢幕自動登出鎖定。
- 不與他人共用帳號密碼。
- 不使用預設密碼。
- **定期變更密碼，每3個月至少更換一次。**
- 不使用弱密碼、易猜測、公開資訊或與原密碼類似。



資料來源:115高雄市資訊組長座談會簡報

帳號密碼管理(2/2)

- 依最小權限原則建置帳號及職務分配使用權限。
- 非本市教職員、學生禁止使用OpenID帳號。
- 定期清查使用者帳號及使用權限。
- 定期每學期清除閒置帳號，如有人員職位異動，須**依規定期限內**停用、刪除及收回人員於單位內各項資源（如：資通系統、業務網站、行政網站、班級網站、Google、FB、物聯網、NAS、印表機等）之權限。
- 多人共用電腦應設定不同帳號與密碼登入，以鑑別使用者身分，落實作業安全。

資料來源:115高雄市資訊組長座談會簡報

個資外洩案例(1/8)

- 個資外洩檔案類型**（一）證書證照類：包括環境證書、技能檢定證書、合格證書及語言認證等。**
- （二）行政資料類：如系統操作手冊、活動報名表、授權同意書等，常載有**姓名、身分證字號及聯絡方式等個人資料。**
- **（三）研習資料類：包括教師研習時數、研習名冊及相關紀錄等。**
- （四）人事資料類：如學生幹部資料、愛心服務商家資訊及教師履歷等，內容涉及個人背景與聯絡資訊。
- （五）計畫文件類：包含計畫書、申請表及成果報告書等，經常揭露計畫主持人及相關人員之個人資料。
- （六）**消防管理資料類：**例如防火管理人提報單、消防安全設備檢修申請表等，通常載有聯絡人個資。
- （七）經費文件類：如獎學金申請文件、勞健保計算表等，涉及財務及保險相關資料。

資料來源:115高雄市資訊組長座談會簡報

個資外洩案例(2/8)

- **（一）證書證照類：**
- **包括環境證書、技能檢定證書、合格證書及語言認證等。**
- 部分學校為提供查詢或宣導成果，將學生或教職員之證書影本逕行公開於網站，未對姓名、身分證字號等敏感欄位作適當遮蔽，或僅採無效遮罩方式，致個人資料可被直接讀取。證照類文件格式多屬固定且資訊完整，一旦外洩，即有被冒用或搭配其他資料進行詐騙之風險。



資料來源:115高雄市資訊組長座談會簡報

個資外洩案例(3/8)

- **（二）行政資料類：如系統操作手冊、活動報名表、授權同意書等，常載有姓名、身分證字號及聯絡方式等個人資料。**
- 有學校於編製系統操作手冊或操作說明文件時，將實際操作畫面截圖上傳，而截圖中仍清楚顯示使用者姓名、帳號或其他個資。 此類畫面一旦公開，除造成個人資料暴露外，亦可能被不當利用作為系統入侵或社交工程攻擊之依據。
- **（三）研習資料類：包括教師研習時數、研習名冊及相關紀錄等。**
- 部分教師研習時數或研習名冊等資料，直接公開於教師個人網頁或學校網站，未就姓名、身分證字號及聯絡方式等欄位加以去識別或遮蔽。此等資料原用於校內行政或個人履歷展現，但於網路公開後，恐遭第三人蒐集整理，進而增加教職員遭受詐騙或不當聯繫之風險。
- **（四）人事資料類：**
- **如學生幹部資料、愛心服務商家資訊及教師履歷等，內容涉及個人背景與聯絡資訊。**
- 有系學會或社團網站公開學生幹部名冊，內容包括姓名、系級、職稱及聯絡方式等完整個資。此類資訊一經於網路公開，即超出校內合理使用範圍，增加學生遭受騷擾或詐騙聯繫之可能性。

資料來源:115高雄市資訊組長座談會簡報

個資外洩案例(4/8)

- **（五）計畫文件類：**
- **包含計畫書、申請表及成果報告書等，經常揭露計畫主持人及相關人員之個人資料。**
- 有學校將計畫申請書或相關計畫文件全文上傳，文件中載明計畫主持人及成員之姓名、身分證字號、聯絡電話等個資，未事先刪除或匿名化。該等作法雖基於資訊公開考量，然未兼顧個資保護要求，恐有違反相關法規之虞。
- **（六）消防管理資料類：例如防火管理人提報單、消防安全設備檢修申請表等，通常載有聯絡人個資。**
- 有學校將計畫申請書或相關計畫文件全文上傳，文件中載明計畫主持人及成員之姓名、身分證字號、聯絡電話等個資，未事先刪除或匿名化。該等作法雖基於資訊公開考量，然未兼顧個資保護要求，恐有違反相關法規之虞。
- **（七）經費文件類：如獎學金申請文件、勞健保計算表等，涉及財務及保險相關資料。**
- 部分學校將勞健保經費計算表公開上網，雖將相關工作表設定為隱藏，但檔案內仍存有可被程式或使用者還原之個人資料欄位。該等表格往往載有姓名、身分證字號及投保薪資等敏感資訊，若僅以「隱藏」方式處理，並不足以達成保護個資之目的。

資料來源:115高雄市資訊組長座談會簡報

常見資料不當處理方式()

- **未經適當處理即公開**
- 有部分檔案載有機敏個人資料，未經遮罩、去識別化或權限控管，即逕行上傳至學校網站供自由下載或瀏覽。此種作法等同將個資公諸於世，使任何人均得取得並使用該等資料，風險甚鉅。
- 建議各單位應建立文件上架前之審查流程，明確區分可公開與不得公開之資料，並加強人員個資防護教育訓練，使承辦人員能於製作及公布文件時，確實落實檢視及處理機敏個資之作業。



資料遮罩的處理方式_ 遮罩截圖後再上傳

資料來源:115高雄市資訊組長座談會簡報

清查學校網站個資與機敏資料

班級、行政網站洩露的個資數量更驚人

清查校網內容：
有關「Google搜尋中出現不當文字及連結處理方式」可參酌114年8月14日高市教資字第11436129500號函辦理。
建議會簽各處室，請各處室清查校網個資與機敏資料，**學校網站不要放個資與機敏資料，不公開不代表找不到！只要放在網路上就有機會找到。**
常見個資或機敏資料：**研習紀錄、證照、證書、老師及學生資料、學生名單、密碼**等。

步驟一：
在Google搜尋，輸入**site:校網網址 “關鍵字”** ，如site:example.abc.edu.tw “研習紀錄”
步驟二：
檔案處理方式：
方法一：**盡速移除下架含有個資與機敏資料與檔案**後，至 Google 申請更新過舊的內容。
方法二：仍要使用資料，請**去識別化或遮罩確實**後，至 Google 申請更新過舊的內容。
淺談個資遮罩(https://www.cc.ntu.edu.tw/chinese/epaper/0040/20170320_4008.html)
步驟三
Google Search Console搜尋處理方式：
Google移除過舊的內容網頁（**需先申請管理者帳號**，再登入Google帳號）
https://support.google.com/websearch/answer/6349986?sjid=14094625064062651353-AP
https://support.google.com/websearch/troubleshooter/3111061

資料來源:115高雄市資訊組長座談會簡報

115年資安巡檢及校安檢查（配合政風室）

- 本年度資安到校巡檢期程從115年3月12日起至115年6月4日，共計查核38所學校（佔全市學校10%）。
- 查檢項目為**資通安全維護計畫實施情形、機關應辦事項**，共計有四校項目全數符合。
- 其餘巡檢有**不符合**項目類型多以「**作業系統未更新**」、「**為符合密碼複雜度設定**」、「**大陸廠牌與公務網路介接**」、「**未設定螢幕保護程式**」、「**未落實物聯網盤點**」。
- 尚有檢查項目不符合且未補件之學校共4校（**左營區新莊高中、左營區新民國小、仁武區仁武高中、仁武區烏林國小**），擬持續追蹤並優先列為明年巡檢學校。

資料來源:115高雄市資訊組長座談會簡報

資安素養與時俱進

活網人生，平安順遂^_^

資訊教育組 與您同在！