113 年國教署資安宣導

一、依個人資料保護法第 50 條規定：「非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。」，爰請私立學校之校長、個資長應善盡個資管理義務。

二、依國家發展委員會 103 年 12 月 31 日發資字第 1031501471 號函，各機關行文及網站資料涉及國民身分證統一編號者之登載者，統一隱碼欄位為身分證號後 4 碼(即第 7 碼至第 10 碼)，並以「*」取代(特殊性用途除外)。

三、依教育部 110 年 9 月 8 日臺教資(四)字第 1100122001 號函，學校使用雲端資通服務(如 Google 表單等)蒐集個人資料時，可能因設定不當而增加個資外洩及資安風險，請學校使用資通系統或雲端資通服務蒐集教職員、學生及家長個人資料者，應注意「學校使用資通系統或服務蒐集及使用個人資料注意事項」、Google 表單蒐集個人資料使用原則（https://sites.google.com/email.nchu.edu.tw/g-form)，以「最小化」為原則，並請學校建置公告、資料收集審查機制，避免因系統設定錯誤或人為因素，誤將機敏個資、機密檔案公布於網路上。

四、重申教育部 109 年 9 月 25 日臺教資（五）字第 1090135390 號函轉行政院資通安全處 109 年 9 月 14 日院臺護字第 1090188336 號書函，即時通訊軟體(如 Line 等)使用應注意不得傳送公務敏感資料為原則。

五、依行政院 112 年 6 月 20 日院授數資安字第 1121000202 號函，重申各公務機關使用資通訊產品原則：公務用資通訊產品(含軟體、硬體及服務)不得使用大陸廠牌，機關若因業務需求且無其他替代方案，仍需使用危害國家資通安全產品時，應具體敘明理由，並經機關資通安全長及其上級機關資通安全長逐級核可，函報資通安全管理法主管機關(數位發展部)核定，產品未汰換前，應加強下列資安強化措施：

(一)強化資安管理措施，例如：設定高強度密碼、禁止遠端維護等。

(二)產品遇資安攻擊導致顯示畫面遭置換，應立即置換靜態畫面，或立即關機。

(三)產品若為硬體，應確認其不具 WiFi 等持續連網功能(非僅以軟體關閉)。若需以外接裝置方式進行更新，須有專人在旁全程監督，於傳輸完成後立即移除外接裝置。

(四)產品使用屆期後不得再購買危害國家資通安全產品。

六、依「資通安全事件通報及應變辦法」，知悉資通安全事件後，學校應於一小時內進行資通安全事件之通報；另資通安全事件有一般公務機密、敏感資訊（個人資料等）遭輕微洩漏或竄改，為第三級資通安全事件，提供「國立高級中等以下學校資安情資傳遞及應變處理作業流程」1 份(如附件)。

七、重申帳號權限與密碼管理原則，落實管理資通系統，以避免資安事件發生：

(一)最高管理者權限帳號數量，原則不得超過 3 個。

(二)使用者於第一次登錄系統時，應立即更改預設密碼，並妥善保管帳號與維持密碼之機密性。

(三)使用者禁止共用自己或他人的帳號及密碼。

(四)使用者每次存取系統時應輸入密碼登入系統，避免使用記錄密碼功能，導致開機時自動登入系統。

(五)密碼長度設定至少 8 碼，且應符合帳號及密碼內容設置原則。

(六)密碼內容之設定，應參雜數字、英文字母大小寫及特殊符號，至少符合下列 4 項要求中之 3 項。

1、內含至少 1 個大寫英文字母。

2、內含至少 1 個小寫英文字母。

3、內含至少 1 個阿拉伯數字。

4、內含至少 1 個特殊符號。

(七)密碼內容之設定，應盡量避免使用易猜測或公開資訊如下說明：

1、個人姓名、出生年月日、身分證字號。

2、機關、單位名稱或是其他相關事項。

3、使用者 ID、其他系統 ID。

4、電腦主機名稱、作業系統名稱。

5、電話號碼、空白、字典字(具有意義的英文單字，例如：password 等)。

6、禁止使用鍵盤順序鍵(如：qwer)。

7、密碼不得與帳號相同。

(八)密碼最短使用期限為 1 天，並應定期更換，90 天(含)以內必須更換密碼一次，逾期未變更者，應暫停其系統登入之權限，以避免盜用情形;密碼變更時不得使用與前 3 次相同的密碼。

(九)管理者及使用者帳號應避免共用，並負帳號及密碼保管之責，不得對任何人透露或以任何形式公開自己帳號及密碼，亦避免將帳號、密碼記錄在書面上，或張貼在個人電腦、螢幕或其他未保護且容易洩漏秘密之處所，以避免密碼外洩。

(十)懷疑密碼被他人知悉或發現密碼可能遭破解時，應立即更改密碼。

(十一) 帳號登入進行身分驗證失敗達 5 次後，系統將自動鎖定帳號時間至少 15 分鐘不許該帳號繼續嘗試登入。

(十二) 使用者職異動或離職時，部門主管應即時通知相關單位調整或終止使用者之存取權限。

(十三) 系統之帳戶，若超過 6 個未曾登錄，則視需要清除閒置帳號。

八、國教署 113 年度國立高級中等以下學校資通安全輔導計畫之實地稽核訪視預計於 5 月至 9 月辦理，請各校事先備妥相關之佐證資料，俾利稽核訪視行程順利進行，相關資訊將於後續發函通知。

九、重申教育部 110 年 6 月 29 日臺教資(四)字第 1100085899A 號函，請學校加強檢核自身資通安全防護及相關措施：

(一)學校因管理不當導致發生資通安全事件，本署將以不遮蔽學校方式作為教育體系內部案例宣導。

(二)針對發生重大資通安全事件之學校，本署將辦理或配合教育部資安專案實地稽核，未落實稽核缺失改善者，將循相關機制予以懲處。

學校使用資通系統或服務蒐集及使用個人資料注意事項

一、教育部為保護教職員、學生、家長之權益，特訂定學校使用資通系統或服務蒐集及使用個人資料注意事項（以下簡稱本注意事項）。

二、各級學校為行政目的使用資通系統或服務蒐集教職員、學生、家長之個人資料者，應遵循個人資料保護法相關規定並參酌本注意事項辦理。但各直轄市、縣（市）政府另有規定者，其所轄學校從其規定。

三、學校為行政目的使用資通系統或雲端資通服務（如 Google 表單、Microsoft Forms 等問卷調查服務）涉及蒐集個人資料者，應注意下列事項：

（一）資料蒐集最小化：僅蒐集適當、相關且限於處理目的所必要之個人資料，處理及利用時，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

（二）存取控制：應注意檔案存取權限設定，應採最小權限原則，僅允許使用者依目的，指派任務所需之最小授權存取。

（三）使用雲端資通服務者，應詳閱設定內容，不宜使用者共同編輯個人資料檔案清冊，並應注意避免設定允許顯示其他使用者作答內容（如 Google 表單不應勾選「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。公佈前應確實做好相關設定檢查，並實際操作測試，確認無誤後再行發布。

（四）傳輸之機密性：網路傳輸應採用網站安全傳輸通訊協定（HTTPS）加密傳輸，並使用 TLS 1.2 以上版本傳輸。

（五）資料儲存安全：如涉及蒐集個人資料保護法第 6 條之個人資料或其他敏感個人資料，應以加密方式儲存。

（六）應訂定個人資料保存期限，並於期限或業務終止後將蒐集之個人資料予以刪除或銷毀，避免個人資料外洩。

四、各校或其主管機關得依本注意事項，訂定各校相關作業流程規定。

國立高級中等以下學校資安情資傳遞及應變處理作業流程

教育部 | **國教署政風室** | **國教署資訊中心** | **國立高級中等以下學校**

知悉外部情資

開始

接獲檢調單位(法務部、調查局、調查站等)及教育部政風處外部資安情資(國立高級中等以下學校)

電子郵件/電話通知

公文通知

收文

內部簽陳

結案

公文會辦

接獲國立高級中等以下學校之資安外部情資

電子郵件/電話通知

接獲資安情資

判斷是否屬資安事件

否

通知

接獲資安情資非屬資安事件

通知

是

通報

至教育機構資安通報平台通報

教育機構資安通報平台副知

接獲學校通報資安事件

損害控制或復原作業

完成損害控制或復原作業，至教育部機構通報平台填報緊急應變措施(1、2級事件72小時內，3、4級事件36小時內)

3級以上
(含個資外洩)

TACERT覆核資安事件

等級是否調升為3級

否

是

由資安長召開緊急應變會議

結報作業

進行事件調查及資安鑑識

撰寫改善報告並函送國教署

14日內函送

審核改善報告

內部簽陳

退請修正

改善報告函送教育部

收到改善報告

後續追蹤

辦理專案稽核(3級以上)

接受稽核

結案