資安防禦網——事故應變演練與技術檢測解析

國立臺北商業大學 資訊與網路中心 徐國鈞 主任

目錄

01 個資事故

- 個資事故案例
- 個資事故的通報流程
- 個資事故的處理程序
- 個資事故實體演練
- 實作練習：教育體系個資事故模擬演練

02 弱點掃描

- 什麼是弱點掃描？
- 弱點掃描目的
- 弱點掃描怎麼運作？
- 為什麼學校需要做弱點掃描？

03 滲透測試

- 什麼是滲透測試？
- 滲透測試目的
- 滲透測試怎麼運作？
- 為什麼學校需要做滲透測試？

01 個資事故

- 個資事故案例
- 個資事故的通報流程
- 個資事故的處理程序
- 個資事故實體演練
- 實作練習：教育體系個資事故模擬演練

個資事故

個資事故是指保有個資之公務或非公務機關，發生資料被竊取、竄改、毀損、滅失或洩漏（外洩）情形。

個資事故案例 (1)：

- 情境：某專科學校為協助畢業班學生順利通過國家考試，老師們設置「國考輔導LINE群組」，群組內包含全體畢業班學生與多位老師。某位老師（T 師) 急需聯繫幾位特定學生，討論成績評比與補救措施。
- 事件經過：T 師在數百人的學生大群組中發言：「請被 L 老師保薦的學生，盡快跟我聯繫有關於個人成績評比的問題，逾時不候。」並且為了讓學生知道「誰」被保薦，T 師隨手將一份含有學生狀況的私密文件拍照上傳。

個資事故

個資事故案例 (1)：

- 事件經過：T 師雖然用手機內建的畫筆工具試圖塗抹掉學生的姓名與詳細內容，但塗抹的筆觸過細或透明度不足，導致「有遮跟沒遮一樣」，群組內的所有學生放大圖片後仍可清晰辨識出學生姓名與班級座號、身心狀況不佳，以及需照顧生病家人等敏感資訊。
- 核心違規分析

1. **無效的去識別化**：許多人誤以為用螢光筆畫兩下、或用細線劃掉就叫去識別化。若透過調整螢幕亮度、對比度，或單純放大就能辨識出原文，這在法律上「視同未去識別化」。

個資事故

個資事故案例 (1)：

- 核心違規分析

2. **違法揭露「特種個資」**：依據《個人資料保護法》第6條，病歷、醫療、基因、性生活、健康檢查及犯罪前科之資料，原則上不得蒐集、處理或利用。洩漏學生的「身心疾病治療中」屬於第 6 條的保護範圍。
3. **違反比例原則**：老師的目的是「找人 (聯繫學生)」，為了找人只需要公告「學號」或「請相關同學收私訊」即可。完全不需要、也不應該公開該生「為何成績不好」的背後私密原因。

個資事故

個資事故案例 (1)：

- 後續處置及損害

1. 當事人反應：該名學生感到極度受傷與憤怒，認為師生間的信任崩塌，並向主管機關 (教育部) 提起陳情。
2. 學校責任：學校面臨行政調查，且需對該師進行懲處與再教育。若學生提告求償，學校需負連帶賠償責任。
3. 長期影響：師生信任關係破裂、校園氛圍受損，其他學生對隱私保護產生疑慮，影響輔導工作的進行。

個資事故

個資事故案例 (1)：

- 正確的處理流程

1. 只給學號：「請學號110xxxxx、110xxxxx的同學，於今日中午前私訊找老師。」學號重複率低且隱私性較低。
2. 私下聯繫：若知道是哪位學生，直接用LINE私訊或打電話給他，不要在群組公審。
3. 重製名單：不要偷懶直接截圖，請手動打字，只打出必要的資訊 (如：學號、待辦事項)，過濾掉所有不相關的備註。

個資事故

個資事故案例 (2)：

- 情境：某體育協會發生內部行政人員 B 君離職，以及賽事報名疏漏等行政爭議。為處理相關事宜，該協會採取了兩項可能違反個資法的行動。
- 事件經過：該協會於 B 君離職時，發出正式函文給上級指導機關 (如體育署)，並將該公文副本發送給其他的特定體育團體、體育總會等單位，內容提及 B 君之全名及離職事實，並在公開的社群平台 (如Facebook粉絲專頁) 張貼公告，針對賽事報名疏漏進行說明，內容涉及 B 君的個人資料與處置細節。

個資事故

個資事故案例 (2)：

- 核心違規分析

1. **原始蒐集目的**：該協會當初蒐集 B 君的姓名等資料，目的是為了「人事管理」、「薪資發放」或「勞健保投保」等勞動契約相關事務。
2. **實際利用方式**：將員工姓名在離職後於「公開網頁」公告或「行文轉知」無關之第三方單位。
3. **違規風險**：顯然已經超出了當初約定的「人事管理」目的，除非 B 君曾明確簽署同意書，否則難以主張合法。

個資事故

個資事故案例 (2)：

- 核心違規分析

4. **公共利益**：除非該離職人員是總教練、秘書長等具高度對外代表性的關鍵人物，其異動直接影響國家代表隊運作，才較可能主張涉及公共利益。對於一般職員、行政人員的離職，在公開網頁上公告其姓名，很難被認定是為了「增進公共利益」。
5. **違反比例原則**：該協會用公文副本通知全國各協會，若意在提醒他人注意該員工，則帶有「行業黑名單」的意味，此舉對當事人的隱私權及未來就業權益造成過度侵害，甚至可能構成「意圖損害他人利益」。

個資事故

個資事故案例 (2)：

- 後續處置及損害

1. 行政罰鍰：主管機關可依個資法第 47 條，處新臺幣 5 萬元以上，50 萬元以下罰鍰，並令限期改正。
2. 代表人連帶責任：除處罰機關外，若代表人 (如理事長、會長) 無法證明已盡防止義務，亦可能受同一額度之罰鍰處罰 (個資法第50條)。
3. 民事與刑事責任：當事人可依個資法第 29 條請求民事損害賠償，若認定意圖損害他人利益，甚至可能面臨刑事告訴 (個資法第 41 條)。

個資事故

個資事故案例 (2)：

- 正確的處理流程

1. 對內公告：僅透過內部電子郵件通知協會內部相關職員即可。
2. 個別通知合作夥伴：針對有實際業務往來的廠商或會員，進行點對點的個別通知，而非廣發公文副本。
3. 更新官網資訊：直接將網站上的「聯絡我們」窗口更換為新任承辦人資訊，無須特別提及前任者姓名。

個資事故

個資事故案例 (3)：

- 情境：某國際學校採用國際知名校務資訊系統服務商 P 公司的解決方案，管理全校師生的學籍、成績與行政資料。該資料規模約有 9,000 名學生及 1,000 名教師資料。
- 事件經過：駭客集團鎖定 P 公司 (系統供應商)，成功盜取用於維護客戶系統的高權限維護帳號，並利用合法維護帳號，在 12 月下旬週末持續約 48 小時遠端登入該學校系統，從系統中批量下載師生個人資料。廠商 P 公司發現異狀後通知學校，確認約 10,000 筆個資遭外洩

個資事故

個資事故案例 (3)：

- 核心違規分析

1. **廠商資安防護不足**：委外廠商資安防護不足，導致特權帳號遭竊，進而連累客戶。
2. **委外廠商的監督**：學校對委外廠商未有完善的監督管理機制。

個資事故

個資事故案例 (3)：

- 後續處置及損害

1. 行政罰鍰：學校需依《個人資料保護法》第 12 條通知當事人，並面臨主管機關的行政調查與潛在裁罰。
2. 代表人連帶責任：當組織發生個資外洩並遭主管機關裁罰時，負責人 (校長、理事長、董事長) 將面臨「連坐處罰」，除非能拿出證據證明已盡防止義務 (個資法第50條)。

個資事故

個資事故案例 (3)：

- 正確的處理流程

1. 事前審查：提出與委外廠商簽約前的評估報告，證明曾要求廠商提供 ISO 27001 證書或資安檢測報告。
2. 合約規範：與委外廠商的合約中明確要求廠商需定期進行弱點掃描或滲透測試。
3. 補強證據：提出往來公文或電子郵件，證明在得知廠商有風險時，曾要求廠商限期改善。

個資事故

個資事故案例 (3)：

- 正確的處理流程

4. 技術防護落實：委外廠商應定期進行弱點掃描與滲透測試報告、系統存取具有權限控管機制、啟用多因子驗證 (MFA)。
5. 緊急應變通報：學校應於法定時間內（ 72 小時) 完成通報，並通知受害師生；事故後應進行根因分析與提出改善計畫書。

個資事故的通報流程

- 個人資料保護法第 12 條規定：「公務機關或非公務機關知悉所保有之個人資料被竊取、竄改、毀損、滅失或洩漏時，應通知當事人。」

- 個人資料保護法施行細則第 22 條規定：(1)「本法第 12 條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。 」(2)「依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。 」

個資事故的通報流程

- 學校、機構應訂定應變機制，在發生個人資料被竊取、洩露、竄改或其他侵害事故時，迅速處理以保護當事人之權益。其應變機制，應包括下列事項：

1. **採取適當之措施，控制事故對當事人造成之損害。**
2. **查明事故發生原因及損害狀況，並以適當方式通知當事人。**
3. **研議改進措施，避免事故再度發生。**

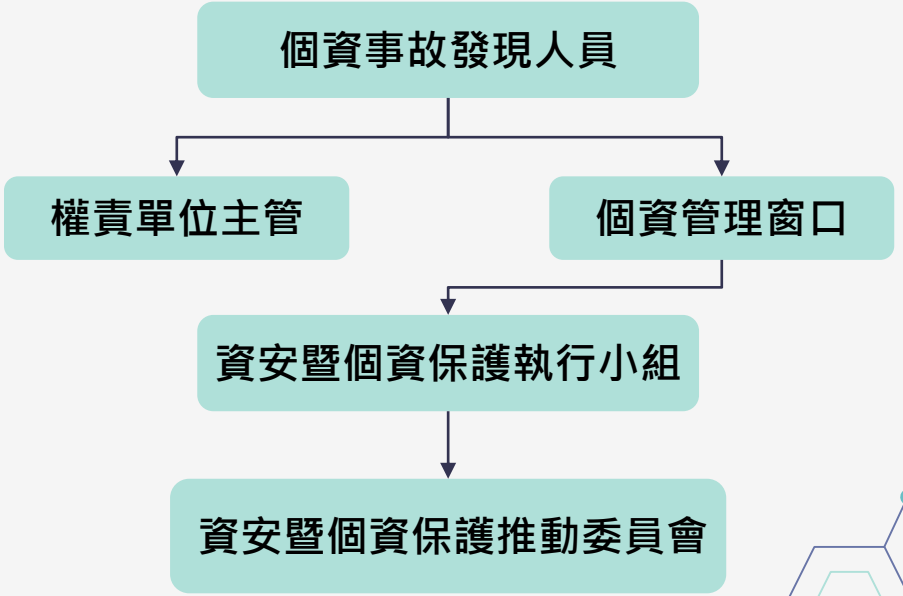
- 學校、機構自第 1 項事故發現時起 **72 小時**內，應填具個人資料侵害事故通報與紀錄表，通報主管機關。

個資事故的通報流程

1. 發現個資疑似遭侵害時，應通報權責單位主管及個資管理窗口；

2. 由個資管理窗口與資安暨個資保護執行小組判斷是否發生個資事故；

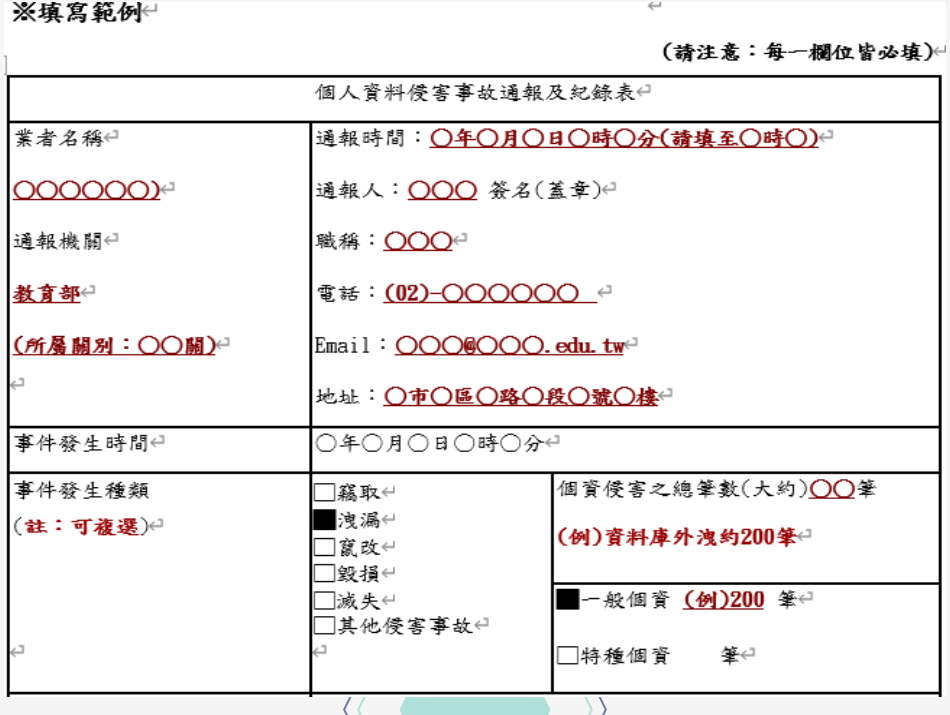
3. 判斷確實發生個資事故，應依照下列流程進行通報，以便即時處理與解決。



個資事故的通報流程

個人資料侵害事故通報及紀錄表範例（節錄）：

https://docs.google.com/spreadsheets/d/1kGcpm6tqf3F6WPYvbRiTG2MOIeTTSTkt4Mgb8ifdBzI/edit?usp=sharing



※填寫範例

（請注意：每一欄位皆必填）

個人資料侵害事故通報及紀錄表		
業者名稱 ○○○○○○) 通報機關 教育部 (所屬關別：○○關)	通報時間：○年○月○日○時○分(請填至○時○) 通報人：○○○ 簽名(蓋章) 職稱：○○○ 電話：(02)-○○○○○○ Email：○○○@○○○.edu.tw 地址：○市○區○路○段○號○樓	
事件發生時間	○年○月○日○時○分	
事件發生種類 (註：可複選)	☐竊取 ■洩漏 ☐竄改 ☐毀損 ☐滅失 ☐其他侵害事故	個資侵害之總筆數(大約)○○筆 (例)資料庫外洩約200筆 ■一般個資 (例)200 筆 ☐特種個資 筆

個資事故的通報流程

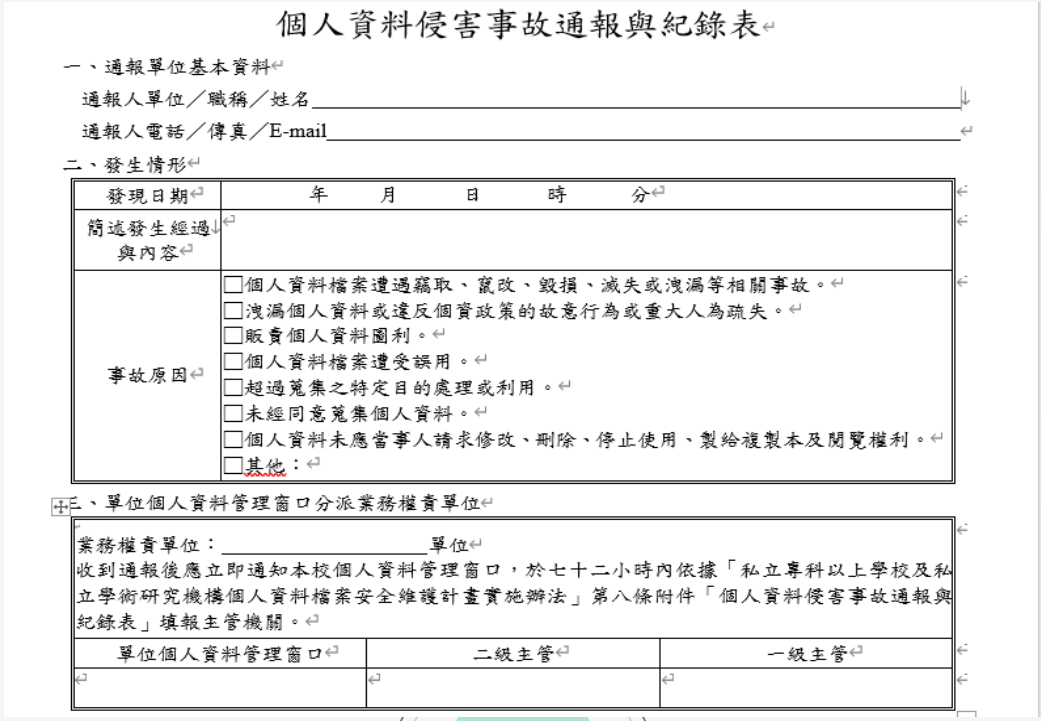
個人資料侵害事故通報及紀錄表範例（節錄）：

發生原因及事件摘要	(例) 時間：〇年〇月〇日/ 原因：公司資料庫遭駭客入侵或作業疏失…/ 外洩資料範圍為員工或學生姓名、電話、身分證統一編號、電子郵件地址、地址……
損害狀況	(例)外洩資料〇筆/受影響人數〇人/財物損失金額〇元/公司帳務損失約〇元/公司名譽形象受損嚴重
個資侵害可能結果	(例)受影響人員可能收到網路釣魚信件、受騙蒙受損失
擬採取之因應措施	(例)重新設定使用權限/立即檢測電腦系統/停止交易/強化管理作業……
擬採通知當事人之時間及方式	(1)通知時間：〇〇 (2)通知方式：以電話、簡訊、電子郵件通知… (3)通知內容：含個資被侵害事實、已採取因應措施、後續處置方式(非僅提醒防詐騙訊息)… (4)其他
是否於發現個資外洩後七十二小時內通報	■是 □否，理由

個資事故的通報流程

個人資料侵害事故通報及紀錄表範例（節錄）：

https://docs.google.com/spreadsheets/d/1x8cX8dyBQSzkhjc_h5F7y8jkkT7GGXYj3Rg5gBh17B4/edit?usp=sharing



個人資料侵害事故通報與紀錄表

一、通報單位基本資料

通報人單位／職稱／姓名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

通報人電話／傳真／E-mail＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

二、發生情形

發現日期	年　月　日　時　分
簡述發生經過與內容	
事故原因	☐個人資料檔案遭遇竊取、竄改、毀損、滅失或洩漏等相關事故。 ☐洩漏個人資料或違反個資政策的故意行為或重大人為疏失。 ☐販賣個人資料圖利。 ☐個人資料檔案遭受誤用。 ☐超過蒐集之特定目的處理或利用。 ☐未經同意蒐集個人資料。 ☐個人資料未應當事人請求修改、刪除、停止使用、製給複製本及閱覽權利。 ☐其他：

三、單位個人資料管理窗口分派業務權責單位

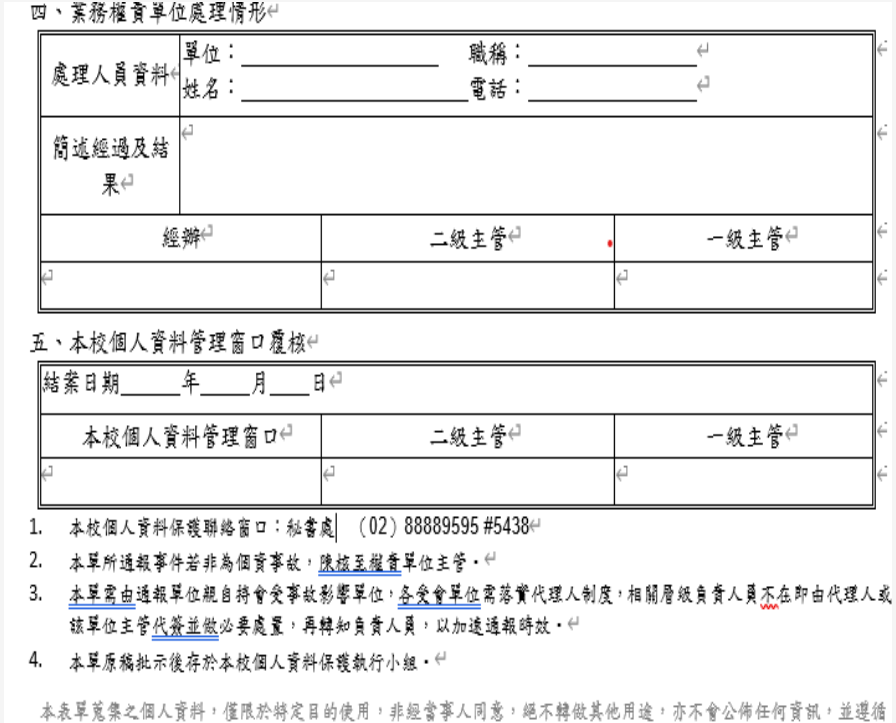
業務權責單位：＿＿＿＿＿＿＿＿單位

收到通報後應立即通知本校個人資料管理窗口，於七十二小時內依據「私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法」第八條附件「個人資料侵害事故通報與紀錄表」填報主管機關。

單位個人資料管理窗口	二級主管	一級主管

個資事故的通報流程

個人資料侵害事故通報及紀錄表範例（節錄）：



四、業務權責單位處理情形

處理人員資料	單位：＿＿＿＿＿＿ 職稱：＿＿＿＿＿＿ 姓名：＿＿＿＿＿＿ 電話：＿＿＿＿＿＿	
簡述經過及結果		
經辦	二級主管	一級主管

五、本校個人資料管理窗口覆核

結案日期＿＿＿年＿＿＿月＿＿＿日		
本校個人資料管理窗口	二級主管	一級主管

1. 本校個人資料保護聯絡窗口：秘書處 （02）88889595 #5438
2. 本單所通報事件若非為個資事故，陳核至權責單位主管。
3. 本單需由通報單位親自持會受事故影響單位，各受會單位需落實代理人制度，相關層級負責人員不在即由代理人或該單位主管代簽並做必要處置，再轉知負責人員，以加速通報時效。
4. 本單原稿批示後存於本校個人資料保護執行小組。

本表單蒐集之個人資料，僅限於特定目的使用，非經當事人同意，絕不轉做其他用途，亦不會公佈任何資訊，並遵循

個資事故的處理程序

1. 準備階段

- 建立各項個資安全防護準備工作，如建立個資團隊、規劃及部署個資防護設備、辦理相關人員個資安全認知教育訓練訓練等。
- 建立各項預防作業，以監控並分析可疑事件。如啟動必要之系統日誌、記錄個人資料存取時之活動等。

個資事故的處理程序

2. 偵測與分析階段

- 透過個資與資訊防護設備的部署及建立相應之防護機制後，開始偵測潛在性的個資與資訊安全事件。
- 當個資事故發生時，即依照組織之應變管理辦法，由**組織內部相關人員**或**外部專家**組成**事故應變處理小組**，以研判事故之發生原因及其可能影響範圍。
- 留存與保管個資事故相關之必要證據。

個資事故的處理程序

3. 控制、清除及復原階段

- 如屬**非資訊面**之個資事故，應立即採取緊急因應措施，並迅速通報個資工作小組，由其依程序進行後續通報作業。
- 如屬**資訊面**之個資事故，應依組織之資通安全緊急應變計畫及處置作業程序辦理，並迅速通報資訊安全或個資事故處理小組之資安聯絡人員。
- 如屬**委外廠商**發生之個資事故，委外廠商之事故應變處理小組應依其資通安全緊急應變計畫及處置程序執行處置，並依契約所約定之 SLA（服務水準協議）通報委託機關之資安聯絡人員。

個資事故的處理程序

4. 事後處置階段

- 由**事故應變處理小組**會同**外部專家**及**委外廠商**，對事故發生的來源及影響範圍進行辨識與分析，並利用資料記錄及存證設備執行鑑識分析及必要之證據保存。
- 在清查個資事故的影響範圍後，由個資聯絡窗口人員依程序對受影響之當事人進行通報（具體處置程序應依主管機關施行細則規定辦理）。
- 法務人員應針對相關法律議題提出應變對策，以配合後續法律處理事宜。

個資事故實體演練

私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法第 14 條之一規定：

學校及幼兒園提供**電子商務服務系統**或**本法第 6 條所定個人資料種類之資通系統**時，應採取下列資訊安全措施：

一、 使用者身分確認及保護機制。
二、 個人資料顯示之隱碼機制。
三、 網際網路傳輸之安全加密機制。
四、 應用系統於開發、上線、維護等各階段軟體驗證及確認程序。
五、 個人資料檔案與資料庫之存取控制及保護監控措施。
六、 防止外部網路入侵對策。
七、 非法或異常使用行為之監控及因應機制。

前項所稱電子商務，指透過網際網路進行有關商品或服務之廣告、行銷、供應或訂購等各項商業交易活動；資通系統，指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

第一項第六款及第七款所定措施，應定期演練及檢討改善。

個資事故實體演練

複雜程度	演練模式	執行重點與程序	建議執行頻率
低	書面審查	針對計畫書內容進行合宜性審視與校對	至少每年度一次
中	局部計畫演練	針對特定任務或計畫細節進行壓力測試與挑戰	至少每年度一次
中	模擬演練	設定特定情境，驗證應變流程之邏輯與可行性	至少每年度或每半年一次
中	關鍵活動演練	啟動可控制之模擬情境進行實作，且以不影響日常營運為原則	每年度一次或依需求辦理
高	完整演練	進行跨部門、大規模之實地演練，全面檢視體系聯防能力	每年度一次或依需求辦理

個資事故實體演練

演練計畫內容項目：

- 演練目的與範圍
- 演練情境說明
- 演練時程規劃
- 演練順序及步驟
- 演練所需資源清單
- 參與單位及負責人員清單
- 協力廠商聯絡清單
- 模擬通報機制

個資事故實體演練

演練計畫執行過程中應留存之紀錄：

- 模擬通報機制、啟動備援機制之過程與時間點
- 演練步驟（含操作指令）
- 演練步驟執行時間
- 演練各步驟執行之人員
- 演練各步驟執行結果
- 演練過程及各步驟發生之問題記錄

個資事故實體演練

演練測試預備會議：

- 導入單位應於演練實施前召開相關協調會議，向參與人員說明演練內容、流程及執行方式，以確保各項演練作業順利進行。

個資事故實體演練

演練測試檢討會議：

- 演練結束後，導入單位應於一個月內召開檢討會議，針對演練過程中所發現之問題與改善事項進行檢視與討論，並將會議紀錄送請單位主管核定後留存備查，以供後續追蹤；
- 於演練檢討會議中，如有決議需修正持續營運計畫之內容，導入單位應儘速完成更新並通知相關人員；
- 此外，導入單位並應於「資訊安全暨個人資料保護推動委員會」中報告本次演練測試之執行結果與相關情形。

實作練習：教育體系個資事故模擬演練

情境 1：教師誤寄學生個資名冊

導師寄送成績名冊給行政人員時，不慎將含有全班學生姓名、學號、聯絡方式的 Excel 名冊寄給錯誤的外部收件者。

演練重點：

- 認定是否構成個資外洩
- 啟動通報流程（校內 + 教育主管機關）
- 評估外洩資料內容與風險等級
- 模擬通知受影響學生與家長
- 檢視是否需採取封鎖或回收郵件措施
- 研擬後續改善措施（如：加密寄送、再次確認收件人流程）

實作練習：教育體系個資事故模擬演練

情境 2：學生證遺失並遭不當使用

學生遺失附有姓名、學號、圖書館條碼資料的學生證，後續發現有人使用該學生證在校內設備（圖書館、宿舍門禁）刷卡紀錄。

演練重點：

- 研判遺失是否造成個資被冒用
- 啟動校內報告與事故紀錄程序
- 門禁系統查閱刷卡紀錄（佐證用途）
- 通知當事學生並協助掛失與補發
- 評估校內門禁與學生證資料展示方式是否需改善

實作練習：教育體系個資事故模擬演練

情境 3：委外廠商作業疏失導致學生個資外洩

委外廠商在執行系統維護或資料處理作業時，因誤將含學生個資的檔案放置於未受保護的位置（如公開資料夾）或錯誤寄送，造成資料可能遭未授權存取。

演練重點：

- 確認委外廠商回報之個資外洩事件
- 啟動「外部委外廠商事故」通報程序
- 與廠商確認外洩資料範圍、是否被下載、資料是否可追蹤
- 要求廠商提出初步原因分析與緊急處置（移除公開檔案、封鎖存取、提供存取 Log）
- 校內個資事故應變小組召開會議釐清是否屬重大個資事故；是否需向主管機關通報；是否需通知受害當事人
- 法務審視委外契約是否含違規責任、罰則及要求改善報告
- 後續改善措施（例如：加強資料加密、廠商權限控管、委外作業稽核）

02 弱點掃描

- 什麼是弱點掃描？
- 弱點掃描目的
- 弱點掃描怎麼運作？
- 為什麼學校需要做弱點掃描？

弱點掃描

什麼是弱點掃描？

- 弱點掃描是一種資訊安全檢測方法，透過自動化工具找出系統、伺服器、網站中的弱點，用於協助組織提前發現安全風險並降低被攻擊的可能性。

弱點掃描目的

- 找出系統中的已知漏洞或設定錯誤
- 評估弱點的風險程度
- 協助擬定修補或改善的措施
- 加強整體資訊安全防護能力

弱點掃描

弱點掃描怎麼運作？

- 自動化工具掃描目標系統或網站
- 與資料庫比對已知漏洞（如常見弱密碼、開放的服務、過期版本）
- 產出掃描報告，列出偵測到的弱點與風險等級
- 提供後續修補建議

弱點掃描

為什麼學校需要做弱點掃描？

- 學校掌握大量個資，屬高風險環境：學校系統中存有學生、家長、教職員的大量個人資料，例如：學籍資料、成績、聯絡方式、健康紀錄、補助資料等。一旦系統存在漏洞，被外部攻擊者利用，可能導致個資外洩與嚴重法律風險。
- 教育機關為常見攻擊目標：駭客常利用弱密碼、未更新系統或網站漏洞發動攻擊，包含勒索病毒、未授權存取、植入惡意程式等。弱點掃描能提前發現這類風險，避免被攻擊後才處理、造成更高成本。
- 符合法規要求：學校屬公立機關或非公務機關，依法都需負責妥善保護個資。弱點掃描是建立「合理安全維護措施」的重要證明，可作為法遵證據、個資安全維護計畫中的實際防護措施，降低違規責任的風險。

弱點掃描

為什麼學校需要做弱點掃描？

- 提升資安韌性與日常防護能力：透過定期弱點掃描，學校能確認各系統是否有更新與修補的需求；避免因外包或歷史系統遺留造成安全黑洞；模擬從駭客視角來檢查系統安全性；建立長期資安管理流程（預防、偵測、改善）。
- 保護校務運作不中斷：一旦遭受攻擊，全校系統可能停擺，弱點掃描可協助提前發現問題，避免校務中斷造成大規模影響。

03 滲透測試

- 什麼是滲透測試？
- 滲透測試目的
- 滲透測試怎麼運作？
- 為什麼學校需要做滲透測試？

滲透測試

什麼是滲透測試？

- 滲透測試模擬駭客攻擊方式，以測試系統是否能被入侵，屬於進階資安檢測方法，比弱點掃描更深入。

滲透測試目的

- 確認弱點是否能被實際攻擊成功
- 評估攻擊者可到達的權限與可能造成的影響
- 協助組織改善系統架構、設定與防護機制
- 強化整體資安能力與事故防範

滲透測試

滲透測試怎麼運作？

流程一般包含：

- 資訊蒐集
- 弱點分析與利用
- 權限提升與橫向移動
- 報告與修補建議
- 透過人工與工具結合，模擬真實攻擊行為

滲透測試

為什麼學校需要做滲透測試？

- 學校擁有大量敏感個資，是高價值攻擊目標：學校管理的資訊系統包含大量敏感資料，駭客會以此類大型資料庫為目標，滲透測試可提前驗證系統是否真的能被入侵，以降低資料外洩風險。
- 常見弱點可能被真正利用，須以實際攻擊驗證：弱點掃描只能說明「可能」有弱點，但滲透測試能回答更關鍵的問題：弱點是否真的能被攻擊者利用？能取得什麼權限？能否進入資料庫或竄改資料？系統的防禦是否足以阻擋不同類型攻擊？
- 配合法規與行政查核要求，落實合理安全措施：滲透測試是許多組織用來強化資安的實務作法，學校若能定期執行，可作為證明。

滲透測試

為什麼學校需要做滲透測試？

- 防止校務運作受到攻擊中斷：一旦遭受入侵，學校系統可能無法正常運作，滲透測試可協助事先揭露攻擊路徑，避免校務全面受影響。
- 強化學校整體資安成熟度與應變能力：透過滲透測試，學校可以建立完整的攻擊面盤點；了解自身最脆弱的環節；改善系統配置、網路架構與權限管理；提升資訊人員的資安管理能力，讓校園資訊環境更安全、更穩定。

感謝聆聽