教育部國民及學前教育署

115 年度私立高級中等學校個人資料管理人、專責人員、稽核人員知能研習

目 錄

115 年度私立高級中等學校個人資料管理人、專責人員、稽核人員知能研習實施計畫

壹、依據

一、教育部國民及學前教育署 115 年國立高級中等以下學校資通安全輔導計畫。

二、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。

貳、目的

一、建立校園資訊安全與個人資料保護管理教育訓練制度及提升整體人才素養，藉由引導學校達成自主管理永續發展之目的。

二、實施校園個人資料管理人、專責人員、稽核人員課程訓練，提升校園資訊安全與個人資料保護管理人員之能力。

參、辦理單位

一、指導單位：教育部

二、主辦單位：教育部國民及學前教育署

三、承辦單位：國立成功大學附屬臺南工業高級中等學校

肆、研習日期、地點

一、研習日期：115 年 3 月 27 日（星期五）

二、研習資訊網站：https://reurl.cc/067zG3

三、研習地點：線上與實體併行

（一）線上研習：https://meet.google.com/ypd-npep-rke

（二）實體研習：成大南工力行大樓 3 樓第一會議室（臺南市永康區中山南路 193 號）

四、報名方式：線上報名（https://forms.gle/zfwnUGRXPPaP8ECa6）

五、聯絡資訊：

國立成大南工 鄭先生 06-2322131 #6712

國立成大南工 楊小姐 06-2322131 #6715

伍、參加人員：私立高級中等學校個人資料管理人、專責人員、稽核人員（**視需要自由參加**，人員定義請參考「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 3 條、第 5 條，如：**學生資料管理人員、教職人員資料管理人員、個資事件申訴管道處理人員等**）

陸、研習課程表：如下表

私立高級中等學校個人資料管理人、專責人員、稽核人員知能研習日程表

時 間	會 議 程 序	主 持 人/主 講 人
09:30-10:00	報 到(線上簽到)	國立成大南工團隊
10:00-10:10	開幕式	教育部國民及學前教育署長官

時 間	會 議 程 序	主 持 人/主 講 人
10:10-12:00	專題演講(一)	主　題：從盤點到防護——個資風險分析與管理實務 講　師：國立台北商業大學　徐國鈞主任
12:00-13:00	中午休息	-
13:00-14:30	專題演講(二)	主　題：證據說話——內部稽核實務與軌跡紀錄管理 講　師：國立台北商業大學　徐國鈞主任
14:30-15:00	休息	–
15:00-16:30	專題演講(三)	主　題：資安防禦網——事故應變演練與技術檢測解析 講　師：國立台北商業大學　徐國鈞主任
16:30-17:00	綜合座談	主持人：教育部國民及學前教育署長官

教育部國民及學前教育署 115 年度校園資通安全業務管理輔導團
教育部國民及學前教育署人員名錄

服務機關	職稱	姓名
教育部國民及學前教育署	署　　長	彭富源
教育部國民及學前教育署	副　署　長	許麗娟
教育部國民及學前教育署	資訊中心主任	林錦德
教育部國民及學前教育署	資訊中心副主任	林郁珊
教育部國民及學前教育署	設 計 師	林凱儀

教育部國民及學前教育署 115 年度校園資通安全業務管理輔導團
成員名錄

編號	服務單位	職稱	姓名	備註
機關及計畫代表				
01	教育部國民及學前教育署	副署長	許麗娟	召集人
02	教育部國民及學前教育署資訊中心	主任	林錦德	副召集人
03	教育部國民及學前教育署資訊中心	副主任	林郁珊	執行秘書
04	教育部國民及學前教育署資訊中心	設計師	林凱儀	
05	教育部國民及學前教育署政風室	辦事員	吳怡璇	
06	教育部國民及學前教育署高中組	行政組員	孔于瑄	
07	教育部國民及學前教育署高中組	科員	鄭智豪	
08	教育部資科司網路暨資通安全科	高級分析師	裴善成	
09	國立成功大學附屬臺南工業高級中等學校	校長	黃耀寬	
專家學者				
10	國立華南高級商業職業學校	圖書館主任	劉耀明	稽核員
11	國立高級中等以下學校 DNS、學校網頁向上集中計畫	博士	林守仁	
12	國立陽明交通大學電算中心	副主任	高義智	資安技術稽核
13	教育機構資安驗證中心(國立中興大學)	主任	陳育毅	主任
14	國立成功大學資通安全研究與教學中心	專案人員	鍾沛原	主導稽核員
15	崑山科技大學資訊管理系	副教授	徐國鈞	主導稽核員
16	長榮大學圖書資訊處	組長	俞怡中	主導稽核員
17	亞洲大學資訊發展處	技正/組長	陳偉嵩	主導稽核員
18	國立中正大學資訊處資源管理組	技術師	黃柏森	主導稽核員
學校代表				
19	國立臺東高級中學	技服組長	巫培爾	高中職代表
20	國立新化高級工業職業學校	圖書館主任	曾鏹毅	高中職代表
21	國立臺南高級商業職業學校	圖書館組長	歐俊男	高中職代表
22	國立南投高級商業職業學校	設備組長	涂淵維	高中職代表
23	國立苗栗高級商業職業學校	資訊媒體組長	洪郁婷	高中職代表

教育部國民及學前教育署 115 年度校園資通安全業務管理輔導團
地區輔導員名錄

序號	姓名	服務學校	地區	職務	Email
1	巫培爾	國立台東高中	台東	圖書館技服組組長	peierh@gm.pttsh.ttct.edu.tw
2	陳宗元	國立台南二中	台南	專任教師	cwtan@mail.tnssh.tn.edu.tw
3	蕭名宏	國立台南特教	台南	教務處機房管理	info@tnmr.tn.edu.tw
4	歐俊男	國立台南高商	台南	資訊媒體組組長	jyunnan@mail.tncvs.tn.edu.tw
5	曾鏘毅	國立新化高工	台南	圖書館主任	tseng@ms.hhvs.tn.edu.tw
6	黃俊宏	國立蘇澳海事	宜蘭	電算科教師	twelanfreeman@gmail.com
7	黃楨喻	國立花蓮高中	花蓮	教師/資訊媒體組長	chenyuh@mail.edu.tw
8	吳振銘	國立花蓮高商	花蓮	設備組組長	wjm@hlbh.hlc.edu.tw
9	涂淵維	國立南投高商	南投	設備組長	uwtu@mails.pntcv.ntct.edu.tw
10	吳家華	國立屏東高工	屏東	設備組長	rexadair@ptivs.ptc.edu.tw
11	童信源	國立屏東高工	屏東	電子科教師	tung@ptivs.ptc.edu.tw
12	洪郁婷	國立苗栗高商	苗栗	技能檢定組長	septemyu@gmail.com
13	吳松達	國立苗栗高商	苗栗	圖書館主任	sdw_mlvs@mail.edu.tw
14	廖文賢	國立苗栗高商	苗栗	資處科主任	wshian1223@mail.edu.tw
15	張偉勤	國立北科大附工	桃園	研發處主任	cwchtyai@mail.edu.tw
16	邱詩育	國立北科桃農	桃園	資訊組長	41chiu@gmail.com
17	林博民	國立海大附中	基隆	圖書館主任	linpomin@mail.edu.tw
18	林欣穎	國立海大附中	基隆	數學科專任教師	mhou148@mail.edu.tw
19	李右任	國立土庫商工	雲林	專任教師	leeyr@tkvs.ylc.edu.tw
20	王佳瑜	國立新竹特教	新竹	設備組長	wingermany@mail.edu.tw
21	洪建楓	國立嘉大附小	嘉義	總務主任	t000082@mail.edu.tw
22	劉錫禎	國立嘉義高中	嘉義	試務組長	icegoofy@mail.edu.tw
23	戴余庭	國立員林家商	彰化	設備組長	talency@mail.edu.tw
24	廖茂松	國立彰師附工	彰化	技工	eric_liao@mail.edu.tw

NOTE

一、 從盤點到防護—個資風險分析與管理實務

主講人：國立臺北商業大學 徐國鈞主任

從盤點到防護——個資風險分析與管理實務

國立臺北商業大學 資訊與網路中心 徐國鈞 主任

目錄

01 個資盤點實務

- 個人資料定義
- 個資保護法源依據
- PDCA
- 個資法罰則及個資外洩案例
- 個人資料檔案清冊

01 個資盤點實務：個人資料

- 基本定義：個人資料是指**自然人**之姓名、出生年月日、國民身分證統一編號、護照號碼、婚姻、家庭、教育、職業、聯絡方式、財務情況，以及社會活動。
- 識別性：個人資料分為**直接識別**與**間接識別**，直接識別為如姓名、身份證號、照片、指紋等；間接識別為可透過比對、組合等方式，足以識別特定個人的資料。

01 個資盤點實務：個人資料

- **特種個資**：包括醫療、健康、基因、性生活、健康檢查及犯罪前科資料，受更嚴格的保護規範。
- 生物特徵：指具個人專屬性足以識別個別身分之個人生理特徵資料（如指紋、臉部特徵、虹膜、聲音、掌紋，以及靜脈等）。

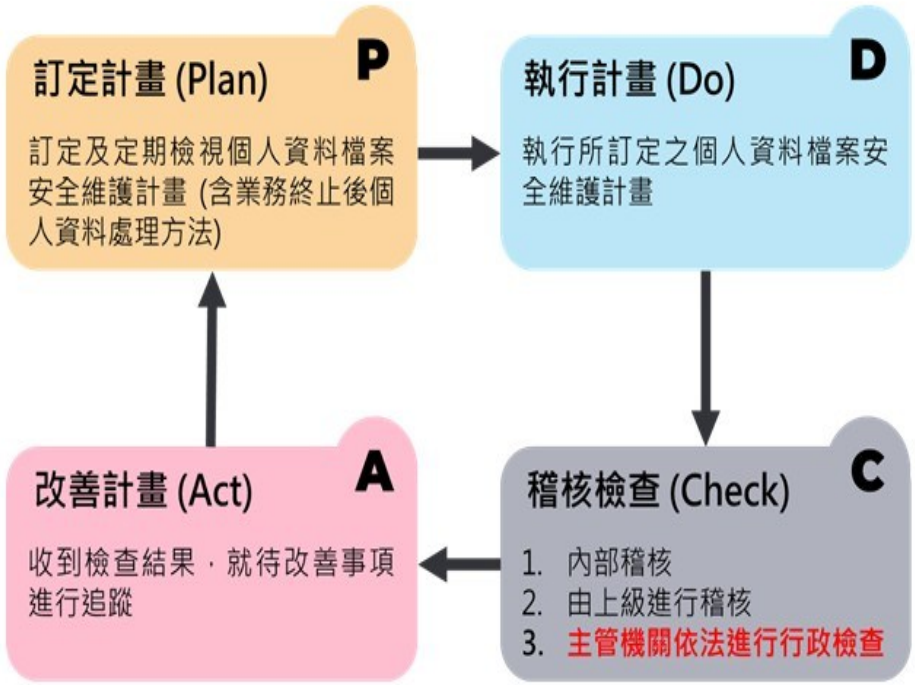
01 個資盤點實務：法源依據

- 個人資料保護法
- 個人資料保護法施行細則
- 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

01 個資盤點實務：法源依據

個人資料保護法 第 20-1 條	1. 非公務機關保有個人資料檔案者，應辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 2. 前項個人資料檔案安全維護事項、管理機制、應採取之措施及其他相關事項之辦法，由主管機關定之。
個人資料保護法施行細則 第 12 條	明確提出涵蓋個人資料檔案安全維護十一款措施之相關事項。
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 8 條	學校及幼兒園應依已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能產生之風險，訂定適當之管控措施。

01 個資盤點實務：PDCA



01 個資盤點實務：PDCA (個資法施行細則§12)

訂定計畫 (Plan)

1. 配置管理之人員及相當資源
2. 界定個人資料之範圍 (個資盤點清冊)
3. 個人資料之風險評估及管理機制 (風險評鑑表)
4. 事故之預防、通報及應變機制
5. 個人資料蒐集、處理及利用之內部管理程序

執行計畫 (Do)

6. 資料安全管理及人員管理
7. 認知宣導及教育訓練
8. 設備安全管理

稽核檢查 (Check)

9. 資料安全稽核機制
10. 使用紀錄、軌跡資料及證據保存

改善計畫 (Act)

11. 個人資料安全維護之整體持續改善

01 個資盤點實務：個資法罰則

- 個人資料保護法第 50 條：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。
- 2023 年立法院三讀通過個資法修正案：修正個資法第 48 條非公務機關違反安全維護義務之裁罰方式及額度，改為逕行處罰同時命改正，並提高罰鍰上限，處新臺幣 (下同) 2 萬元以上，200 萬元以下罰鍰；情節重大者，處 15 萬元以上，1,500 萬元以下罰鍰；屆期未改正者，按次處 15 萬元以上，1,500 萬元以下罰鍰。

01 個資盤點實務：個資外洩案例 (1)

案例 1：某私立科大 Excel 排序災難

承辦人員在處理學生體檢報告時，使用 Excel 進行資料排序，但操作錯誤導致姓名與報告內容錯位，結果將 A 學生的體檢報告寄給 B 學生，造成嚴重的隱私侵害。

問題根源：

- 缺乏標準作業程序 (SOP)。
- 沒有雙重檢核機制。
- 未進行抽樣檢查。
- 過度依賴單一承辦人。

01 個資盤點實務：個資外洩案例 (1)

案例 1 某私立科大 Excel 排序災難 改善方案：

- 建立標準作業程序 (SOP)：明確規範資料處理的每個步驟
- 建立雙重檢核：輸出前必須有第二人確認
- 抽樣檢查：隨機抽取 5-10 筆資料核對
- 使用郵件合併：避免手動複製貼上
- 測試寄送：先寄給自己測試格式

01 個資盤點實務：個資外洩案例 (2)

案例 2：某私立科大過度蒐集個資

學生發生意外，好心人代墊醫療費用。承辦人員為了幫忙處理退款，向代墊者索取身分證字號，涉及過度蒐集個資。

問題根源：

- 違反必要性原則，行政人員常因「以為對方需要」或「便民」而過度蒐集個資。每次蒐集個資前，都要問自己三個問題：

1. 這個個資是法律規定必須蒐集的嗎?
2. 沒有這個個資，業務就無法進行嗎?
3. 有沒有其他替代方案，可以蒐集更少的個資?

01 個資盤點實務：個資外洩案例 (2)

案例 2 某私立科大過度蒐集個資 改善方案：

錢是賠給學生的，不是賠給代墊者的。代墊者只是「先付款的人」，不需要提供個資，只需要代墊者的帳戶資訊 (用於轉帳)，不需要身分證字號。

01 個資盤點實務：個資外洩案例 (3)

案例 3：某私立大學教職員帳號被盜

教職員帳號被盜用後，駭客利用該帳號轉寄含有個資的信件給外部人員，造成大規模資料外洩。

問題根源：

- 單一驗證機制脆弱
- 密碼強度不足
- 缺乏資安警覺與應變機制

01 個資盤點實務：個資外洩案例 (3)

案例 3 某私立大學教職員帳號被盜 改善方案：

- 開啟雙重驗證 (2FA)
- 定期更換密碼
- 不使用簡單密碼
- 發現異常立即通報

01 個資盤點實務：個資盤點

- 目的：盤點**機關目前內部所存有的個人資料檔案**，並鑑別其**內容、數量、蒐集方式、處理方式、利用方式、保存期限，以及揭露方式等**資訊，以評估個資保護之風險及制定後續改善計畫，以降低風險。

01 個資盤點實務：個資盤點

- 個人資料檔案清冊應包含：**盤點單位、個人資料檔案名稱、個人資料檔案型態、特定目的、個人資料類別、有無特種個資、保有數量、蒐集的依據（法源）、蒐集方式、處理方式、利用方式、保存期限、控制（保護）措施、銷毀方式、有無委外處理，以及對外接露**等。

01 個資盤點實務：個資盤點

- 執行頻率：**每年至少進行一次個資盤點**，期間若是遇到重大業務變動，應再次執行個資盤點。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

個人資料檔案名稱：識別機關內部工作流程中，每一項作業所保有的個人資料，如電子郵件帳號管理系統、學籍系統等。

個人資料檔案型態：依照所保有之個資型態不同去分類，如電子檔案為電腦裡的檔案（含備份檔案）；資料庫為資訊系統中的檔案；紙本檔案等。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

特定目的：保有個資時，蒐集、處理、利用之目的，若是超過特定目的範圍，則需重新取得同意（單一個資檔案可以有多個特定目的）。

個人資料類別：個人資料檔案中，欄位的歸類。

01 個資盤點實務：特定目的

- 教育體系常用到的特定目的：
  - 人身保險 (001)
  - 人事管理 (002)
  - 全民健康保險、勞工保險、農民保險、國民年金保險或其他社會保險 (031)
  - 存款與匯款 (036)
  - 兵役、替代役行政 (042)
  - 志工管理 (043)

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：特定目的

- 教育體系常用到的特定目的：
  - 非公務機關依法定義務所進行個人資料之蒐集處理及利用 (063)
  - 保健醫療服務 (064)
  - 契約、類似契約或其他法律關係事務 (069)
  - 計畫、管制考核與其他研考管理 (078)
  - 教育或訓練行政 (109)
  - 產學合作 (110)
  - 場所進出安全管理 (116)

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：特定目的

- 教育體系常用到的特定目的：
  - 稅務行政 (120)
  - 資 (通) 訊與資料庫管理 (136)
  - 圖書館管理 (146)
  - 調查、統計與研究分析 (157)
  - 學生 (員) (含畢、結業生) 資料管理 (158)
  - 學術研究 (159)
  - 其他經營合於營業登記項目或組織章程等，為辦理教學、研究、行政及服務等相關事宜所需 (181)

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：個人資料類別

- 教育體系常用到的個人資料類別：

C001 辨識個人者：
姓名、職稱、住址、工作地址、以前地址、住家電話號碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊及戶籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡序號、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及其他任何可辨識資料本人者等。

C002 辨識財務者：
金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼、保險單號碼、個人之其他號碼或帳戶等。

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：個人資料類別

- 教育體系常用到的個人資料類別：

C003 政府資料中之辨識者：
身分證統一編號、統一證號、稅籍編號、保險憑證號碼、退休證之號碼、證照號碼、護照號碼等。

C011 個人描述：
年齡、性別、出生年月日、出生地、國籍、聲音等。

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：個人資料類別

- 教育體系常用到的個人資料類別：

C052 資格或技術：
學歷資格、專業技術、特別執照 (如飛機駕駛執照等)、政府職訓機構學習過程、國家考試、考試成績或其他訓練紀錄等。

C061 現行之受僱情形：
僱主、工作職稱、工作描述、等級、受僱日期、工時、工作地點、產業特性、受僱之條件及期間、與現行僱主有關之以前責任與經驗等。

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：個人資料類別

- 教育體系常用到的個人資料類別：

C081 收入、所得、資產與投資：
總收入、總所得、賺得之收入、賺得之所得、資產、儲蓄、開始日期與到期日、投資收入、投資所得、資產費用等。

C111 健康紀錄：
醫療報告、治療與診斷紀錄、檢驗結果、身心障礙種類、等級、有效期限、身心障礙手冊證號及聯絡人等。

法規參考：個人資料保護法之特定目的及個人資料之類別

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

有無特種個資：所保有之個資檔案中有無病歷、醫療、基因、性生活、健康檢查，以及犯罪前科等特種個資，如身心障礙手冊屬於醫療的一部份，為特種個資。

保有數量：清查目前所盤點之該項個人資料檔案的所有筆數，沒有銷毀的都要清查。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

蒐集的依據（法源）：目前所盤點之個人資料檔案，是依據哪一個法規留存的，如主管機關的法規或命令、機關本身的規定等，配合個人資料告知同意書。

蒐集方式：個資的蒐集方式，如當事人直接提供或間接從其他機關取得。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

處理方式：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。（個人資料保護法第二條第四點）

利用方式：除蒐集、處理以外的其他動作皆為利用，需在原本宣告之特定目的內。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

保存期限：所有個人資料檔案都應依據相關法規要求，設有保存年限。如學籍資料依據高級中等學校學生學籍管理辦法，需永久保存。

銷毀方式：保存期限已屆，需定期執行銷毀作業，並留下銷毀紀錄。不同的資料類型有不同的銷毀方式，如紙本檔案使用碎紙、水銷；電子檔、資料庫使用刪除等方式。銷毀紀錄需留存五年備查。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

控制（保護）措施：不同的資料類型有不同的控制（保護）措施，如紙本檔案使用上鎖的櫃子、有門禁管理的儲藏室等；電子檔使用加密存放；資料庫使用定期備份等措施。

委外處理：指由機關以外的單位、廠商處理，需有契約書，包含雙方之權利、義務及罰則；合約結束後資料的刪除與返還等。

01 個資盤點實務：個人資料檔案清冊

- 建立個人資料檔案清冊：

對外揭露：指將資料提供給機關以外的第三方，如上傳給主管機關等。

02 風險評估操作

- 個人資料檔案風險值
- 個人資料檔案清冊範例
- 個人資料檔案風險評估表範例

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

個人資料檔案價值	內容
高 (3)	含有直接或間接識別之個人資料與**特種個資**者。
中 (2)	• 含有直接或間接識別之個人資料與**財務資訊（如薪資、局帳號等）**，但不含特種個人資料者。 • 含有個人資料類別 **C003 政府資料中之辨識者（如身分證統一編號、統一證號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等）**者。
低 (1)	含有**姓名、員工編號、學號等**直接或間接識別個人之資料。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

衝擊程度	對當事人損害影響
高 (3)	個資檔案外洩造成當事人身心受到危害、社會地位受到損害，或衍生財物損失，當事人個人權益非常嚴重受損。
中 (2)	個資檔案外洩導致當事人隱私遭冒犯，當事人個人權益嚴重受損。
低 (1)	個資檔案外洩僅導致個人權益輕微受損。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

衝擊程度	對組織財務影響
高 (3)	個資檔案 2,000 筆以上。
中 (2)	個資檔案 30 筆以上，未滿 2,000 筆。
低 (1)	個資檔案未滿 30 筆。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

衝擊程度	對組織營運影響
高 (3)	遭禁止蒐集、處理或利用個人資料，或經命令刪除、沒入、銷毀個人資料時，對組織聲譽及**關鍵業務運作**造成影響。
中 (2)	遭禁止蒐集、處理或利用個人資料，或經命令刪除、沒入、銷毀個人資料時，對組織聲譽及**單一部門業務運作**造成影響。
低 (1)	遭禁止蒐集、處理或利用個人資料，或經命令刪除、沒入、銷毀個人資料時，對組織聲譽及**該業務流程運作**造成影響。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

可能性	作業管理規定
高 (3)	未建立相關作業管理規定及文件，亦無任何安全控管。
中 (2)	• 已建立相關作業管理規定及文件，但部分未落實安全控管。 • 未建立相關作業管理規定及文件，但已有實施部份安全控管。
低 (1)	已建立相關作業管理規定及文件，且已落實安全控管。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

可能性	教育訓練
高 (3)	單位內人員前一年度接受教育訓練的達成率低於 60%。
中 (2)	單位內人員前一年度接受教育訓練的達成率低於 61% 至 90%。
低 (1)	單位內人員前一年度接受教育訓練的達成率 91% 以上。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

可能性	個資檔案不當存取
高 (3)	單位過去一年內曾發生一次 (含) 以上個資檔案不當存取事件。
中 (2)	單位過去三年內曾發生一次 (含) 以上個資檔案不當存取事件。
低 (1)	單位過去三年內不曾發生資檔案不當存取事件。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

可能性	個資盤點落實度
高 (3)	前一年度稽核發現： • 個資檔案未納入盤點達9項 (含) 以上。 • 未執行個資盤點作業。
中 (2)	前一年度稽核發現： • 個資檔案未納入盤點達3-6項。 • 已執行個資盤點作業，但內容不完整，達6項 (含) 以上。
低 (1)	前一年度稽核發現： • 個資檔案未納入盤點有2項 (含) 以下。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

可能性	個資保存
高 (3)	前一年度稽核發現： • 個資檔案未依程序保存達7項 (含) 以上。 • 單位未有可上鎖存放區域。
中 (2)	前一年度稽核發現： • 個資檔案未依程序保存達3-6項。 • 單位已有可上鎖存放區域，但個資檔案未置於該處。
低 (1)	前一年度稽核發現： • 個資檔案未依程序保存有2項 (含) 以下。

02 風險評估操作：個人資料檔案風險值

- 個人資料風險值之計算方式：

個人資料風險值 = 個人資料檔案價值 * Max (衝擊程度) * Max (可能性)

可能性	個資銷毀
高 (3)	前一年度稽核發現： • 個資檔案未依程序銷毀達7項（含）以上。 • 未執行個資銷毀作業。
中 (2)	前一年度稽核發現： • 個資檔案未依程序銷毀有3-6項。 • 已執行個資銷毀作業，但未留存相關紀錄。
低 (1)	前一年度稽核發現： • 個資檔案未依程序銷毀有2項（含）以下。

- 個人資料檔案清冊範例（部分）

盤點單位	個資檔案名稱	個資檔案型態	特定目的	個人資料類別	有無特種個資	保有數量（總數）	蒐集的依據（法源）	蒐集方式	處理方式
系統網路組	電子郵件帳號管理系統	資料庫	109 135 137	C001 C051 C073	無	2,250	校園網路管理辦法、通訊與作業管理程序書	直接蒐集	輸入、編輯、更正、複製、檢索、刪除、輸出、連結、紀錄、儲存、內部傳送

利用方式	保存期限	控制（保護）措施	銷毀方式	委外處理	對外揭露
聯絡、統計、分析、帳號驗證、通知	教職員離校後5年	資料庫保存	資料庫紀錄刪除	無	教育部社交工程演練

https://reurl.cc/zq3EAV

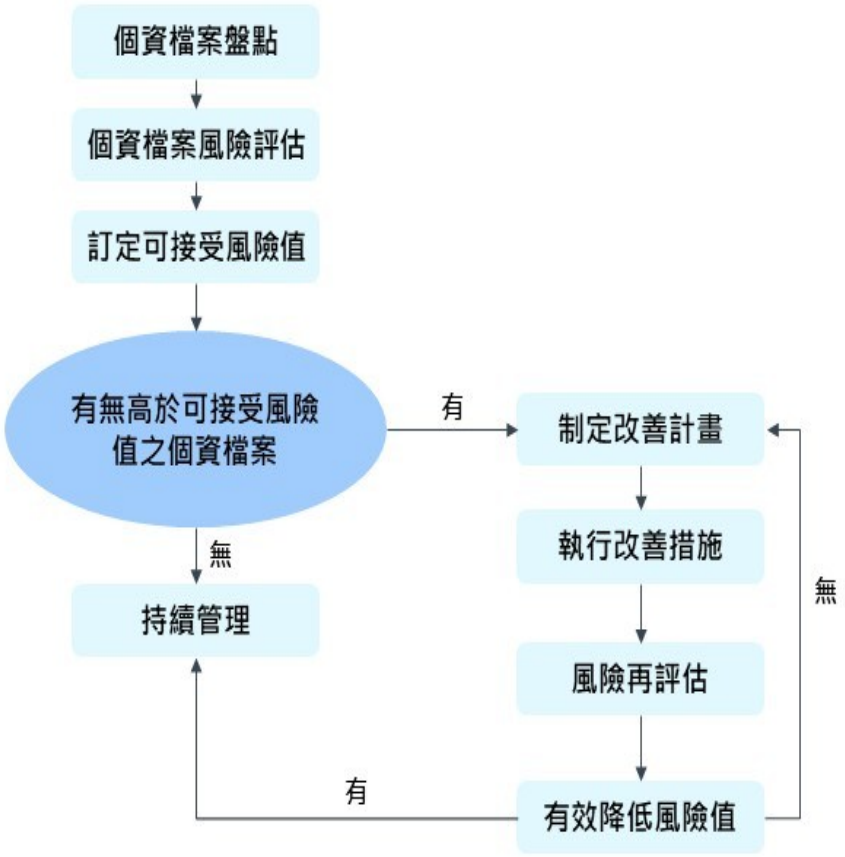
- 個人資料檔案風險評估表範例（部分）

個資檔案名稱	個資價值 (V)	衝擊程度評估 (I)				可能性評估 (P)				風險值 (R) = V*I*P
		對當事人損害影響 (1)	對組織財務影響 (2)	對組織營運影響 (3)	評估值 Max (1,2,3)	作業管理規定 (4)	教育訓練 (5)	個資檔案不當存取 (6)	評估值 Max (4,5,6)	
電子郵件帳號管理系統	1	1	3	1	3	1	2	1	2	6

02 風險評估操作：個人資料檔案風險值

- 根據上述所估算出的個人資料風險值會落在 1-27 分之間。
- **可接受風險值**之設定，得依現有資源、管理規範及政策重點加以考量，並經會議決議後予以確定；亦可採風險值分群方式，優先處置屬高風險等級之項目。

風險等級	風險值
高	19-27
中	10-18
低	1-9



03 制定改善計畫

- 風險改善計畫表
- 風險評鑑彙整表

03 制定改善計畫：風險改善計畫表

- 制定風險改善計畫，經主管審核後實施改善措施；
- 追蹤改善成果。
- 風險改善計畫表範例（部分）：

個資檔案名稱	風險現況說明	改善建議措施	執行人員	預計完成日期	備註
電子郵件帳號管理系統	部分帳號權限設定未依人員職務即時調整，退離職人員帳號停用流程未完全落實，存在不當存取風險。	• 建立即時異動通知機制，確保人員異動時帳號權限同步更新。 • 每月進行帳號清查並紀錄。 • 制定帳號管理作業程序並加強人員教育訓練。	系統網路組承辦人	2026 年 6 月 30 日	-

03 制定改善計畫：風險評鑑彙整表

- 將大於可接受風險值或高風險等級個資檔案彙整於風險評鑑彙整表；
- 完成改善措施後，再次評估風險值是否降低。
- 風險評鑑彙整表範例（部分）：

個資檔案名稱	風險再評估									
	個資價值 (V)	衝擊程度評估 (I)				可能性評估 (P)				風險值 (R) = V*I*P
		對當事人損害影響 (1)	對組織財務影響 (2)	對組織營運影響 (3)	評估值 Max (1,2,3)	作業管理規定 (4)	教育訓練 (5)	個資檔案不當存取 (6)	評估值 Max (4,5,6)	
電子郵件帳號管理系統	1	1	1	1	1	1	1	1	1	1

04 實作練習

- 辨識校園常見個資風險情境

實作練習：辨識校園常見個資風險情境

情境 1：成績單誤寄造成個資外洩

導師在寄送段考成績單電子檔給家長時，不慎將整班的成績總表附在信件中，導致所有學生的姓名、學號、成績等資料被所有家長看到。

練習目標：

- 辨識外洩原因（作業流程疏失、未使用密件副本等）。
- 分析受影響資料類型與風險高低。
- 討論改善流程（檔案權限、寄信前檢查、分批寄信等）。

實作練習：辨識校園常見個資風險情境

情境 2：委外廠商未落實資安措施

委外廠商受託維護校內資訊系統，但工程師使用個人USB隨身碟存放學生資料，且未加密。隨身碟遺失後，可能包含學生名冊、聯絡資料及特殊身分記載。

練習目標：

- 辨識委外風險與責任分工。
- 確認風險屬性（資料未加密、設備未受控、違反契約要求）。
- 討論應加入的委外管理規範與稽核措施。

實作練習：辨識校園常見個資風險情境

情境 3：學務處公告遺失物時誤將學生資訊曝光

學務處在公布遺失物認領資訊時，將拾獲的學生證拍照放上校務系統公告欄，照片中清楚顯示學生姓名、照片、學號及班級等資料，導致不必要的個資曝露。

練習目標：

- 辨識公告資訊是否超出必要範圍。
- 判斷哪些資料屬個資、是否已涉及「目的外利用」。
- 討論公告時的匿名化方式（遮蔽學號、僅描述物品特徵等）。
- 研擬改善措施（公告流程、審核機制、人員教育訓練）。

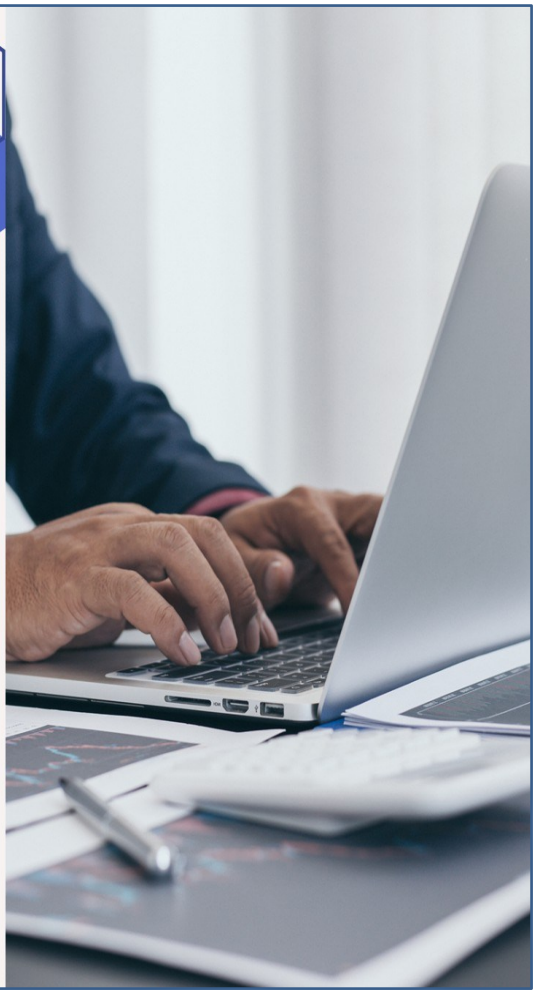
感謝聆聽

二、證據說話—內部稽核實務與軌跡紀錄管理

主講人：國立臺北商業大學 徐國鈞主任

證據說話——內部稽核實務與軌跡紀錄管理

國立臺北商業大學 資訊與網路中心 徐國鈞 主任

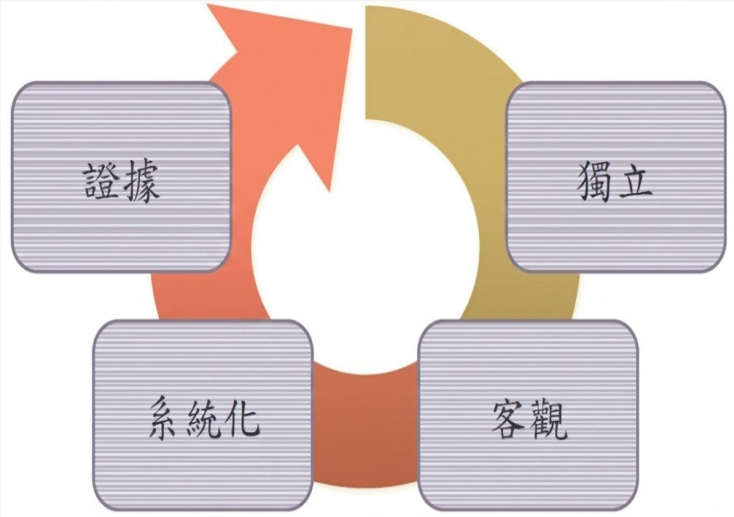


目錄

01 稽核之基本定義、類型及流程

稽核之基本定義、類型及流程

ISO 19011 所定義的**稽核**是指透過**系統化**、**文件化**及具**獨立性**的流程取得稽核證據，並透過**客觀**地評估，以鑑別其稽核準則所涵蓋的範圍是否達成。



稽核之基本定義、類型及流程

稽核類型：

內部稽核
(第一方)

- 由組織內部自行發起的稽核
- 確保管理制度的維護、發展及改善，以達成目標

委外稽核
(第二方)

- 由組織對其供應商或外包商所進行的稽核
- 評估供應商、外包商或下游單位是否符合契約要求或規定

外部稽核
(第三方)

- 由具有公信力且獨立的機構對組織進行稽核
- 驗證組織是否符合建立、施行並維護文件化之管理制度標準

稽核之基本定義、類型及流程

稽核流程：

前置作業

- 確認稽核範圍
- 進行稽核小組、人員任務分配

→

稽核作業

- 召開稽核起始會議
- 蒐集客觀證據
- 召開稽核總結會議

→

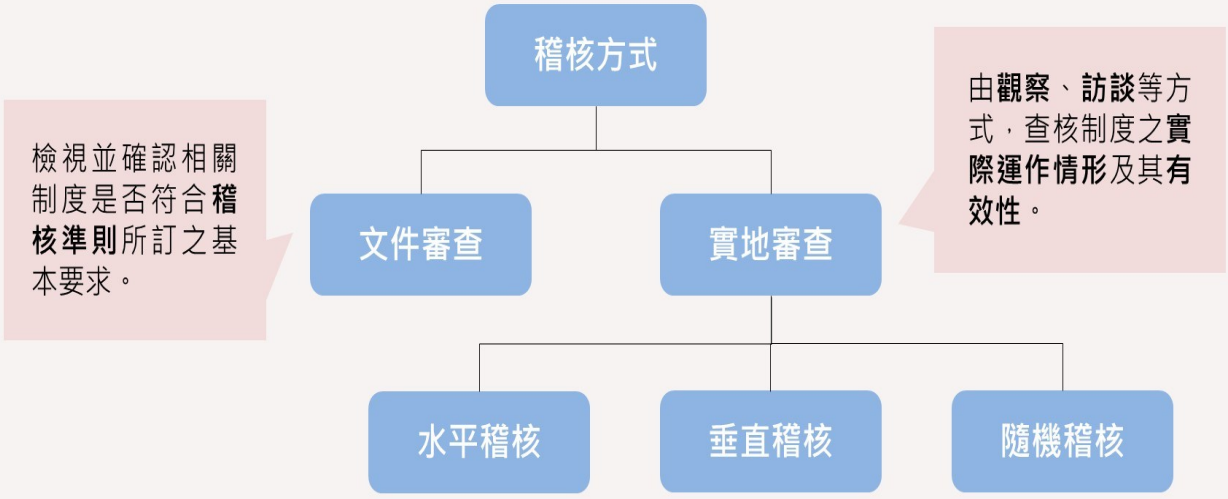
矯正追蹤作業

- 依稽核結果，針對受稽核單位進行矯正改善
- 改善追蹤

稽核前　　稽核中　　稽核後

稽核之基本定義、類型及流程

稽核方式：



稽核之基本定義、類型及流程

實地審查：

水平稽核

依據**內稽底稿**或**查檢表**所列項目逐一提問，並依查檢表之設計於橫向欄位記錄稽核發現；確認該項查核完成後，再進行下一項查核。

垂直稽核

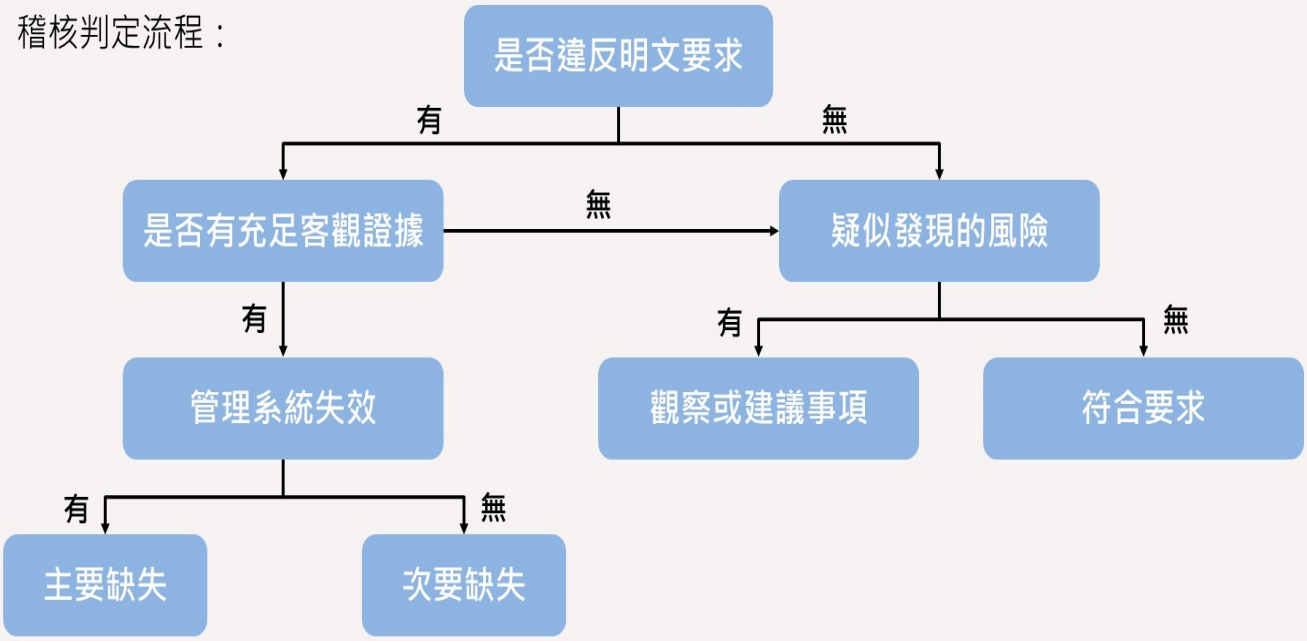
針對**特定議題**或**業務流程**，對相關人員或跨單位訪談對象進行查核，以追蹤並確認相關政策、規範、作業程序、管制措施及相關紀錄之落實情形。

隨機稽核

於稽核範圍內進行**抽樣查核**，例如以前次稽核日至本次稽核日期間之相關作業或紀錄為抽樣範圍。

稽核之基本定義、類型及流程

稽核判定流程：



稽核之基本定義、類型及流程

稽核判定類別：

主要缺失

- 部分程序、作業流程或實際實施情形已完全失效。必要要求項目中，有項目未予以任何實施。
- 多項次要不符合之累積已導致整體系統功能失效或崩潰。
- 前次稽核所列之次要不符合事項於本次稽核仍再度發生。
- 驗證標章或認證標章之使用方式不符規定。

次要缺失

- 部分程序、流程或操作上存在輕微偏離之情形。
- 單一、偶發且非連續性的不符合狀況。

稽核之基本定義、類型及流程

稽核判定類別：

觀察事項

- 雖未發現不符合稽核準則之具體證據，惟仍存在潛在風險，屬應予特別關注與審慎考量之事項。

建議事項

- 有助於組織管理系統持續精進之改善建議，並包含可供參考之業界良好實務。

稽核之基本定義、類型及流程

缺失開立原則：

- **5W1H**

- 發生地點 (Where)
- 發生時間 (When)
- 在場人員或權責部門 (Who)
- 發生之事實或現象 (What)
- 構成不符合事項的原因 (Why)
- 如何發生 (How)

02 個人資訊管理系統 (PIMS) 稽核

個人資訊管理系統 (PIMS) 稽核

稽核依據：

要求文件化之資訊

- 內外部議題及利害關係人（關注方）之要求
- 管理政策
- 管理目標
- 個人資料流識別（含高風險）
- 隱私衝擊及風險評鑑流程（含風險評估及處理計畫）
- 隱私保護設計相關活動及其成果資訊
- 人員勝任能力之證據
- 管理審查資料（含有效性評估之佐證）
- 不符合項目及其矯正措施

- 管理制度執行之相關證據（包括個人資料之蒐集、處理、利用、資料分享及委外管理等事項）
- 當事人權利行使之相關紀錄
- 制度規劃與運作所需之外來文件

個人資訊管理系統 (PIMS) 稽核

權責：

資訊安全暨個人資料保護推動委員會

負責審核**「個人資料管理制度內部稽核計畫」**及**「個人資料管理制度內部稽核報告」**。

資訊安全暨個人資料保護稽核小組

負責擬訂**「個人資料管理制度內部稽核計畫」**、辦理**內部稽核作業**並產出**「個人資料管理制度內部稽核報告」**。

受稽單位

配合各項稽核作業。

個人資訊管理系統 (PIMS) 稽核

內部稽核計畫架構：

一、稽核目的與範圍

- 稽核目的：主動檢核校內個資管理制度 (PIMS) 執行現況，確認各單位是否落實法規要求，並發現潛在風險以進行改進。
- 稽核範圍：包含所有蒐集、處理，以及利用個資的單位（如教務處、學務處、資網中心），以及委外廠商的管理狀況 。

二、稽核頻率

- 稽核頻率：建議至少每年度辦理一次。

個人資訊管理系統 (PIMS) 稽核

內部稽核計畫架構：

三、稽核重點項目

- 技術安全：是否有採取隱碼機制 、加密機制，以及防止入侵對策。
- 作業程序：個資生命週期（蒐集、處理、利用、刪除）是否皆有適法依據與紀錄。
- 委外管理：委外契約是否包含違規責任、罰則，並要求廠商提供應變計畫。
- 事故應變：是否具備個資事故通報流程 、是否定期進行事故實體演練。
- 教育訓練：相關人員是否定期參與個資安全認知教育訓練。

個人資訊管理系統 (PIMS) 稽核

內部稽核計畫架構：

四、稽核團隊組成

為確保稽核過程之客觀性與獨立性，稽核作業應由非受稽單位人員執行。稽核團隊得以下列方式組成，以辦理各項個人資料保護稽核事務：

1. 聘請外部個資保護顧問協助執行稽核。
2. 由經審定具備資格之稽核人員擔任，例如具備 ISO/IEC 27701 個人資料隱私管理系統主導稽核員訓練證書，或已接受個人資料保護內部稽核相關訓練者。

個人資訊管理系統 (PIMS) 稽核

內部稽核計畫架構：

五、稽核結果之處理

- 異常發現紀錄：詳細記錄不符合項 (Non-conformity) 的事實與證據。
- 開立矯正措施單 (CAR)：要求受稽單位限期提出改善措施與預防措施。
- 追蹤改善：確認改善措施已確實執行且有效。
- 管理審查報告：將稽核結果彙報至「資安暨個資保護推動委員會」。

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

一、界定個人資料之範圍

- 查核項目 (1)：是否已建立與維護一份個人資料檔案清冊？
- 稽核重點：以**「個人資料流」**所識別單位之個資資產
- 佐證資料：**個人資料檔案清冊**、**個人資料流程識別表**
- 查核項目 (2)：是否已公告本校保有個人資料檔案公開項目彙整表？
- 稽核重點：依個資法第 17 條，公開單位之**「個人資料檔案公開項目彙整表」**
- 佐證資料：**個人資料檔案公開項目彙整表**至少包含**個資檔案名稱**、**保有機關名稱及聯絡方式**、**個資檔案保有依據及特定目的**，以及**個人資料之類別**

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

二、個人資料保護之風險評估及管理機制

- 查核項目 (1)：是否已建立與執行風險評鑑作業，以確保本校能瞭解在處理各種特定類型之個人資料所可能產生的風險？
- 稽核重點：組織之**個資風險評鑑**的評估方式
- 佐證資料：**個人資料風險評鑑表 (包含衝擊影響 / 可能性 / 風險值)**
- 查核項目 (2)：是否已定義可接受風險與進行高風險處理及風險再評鑑？
- 稽核重點：如何定義「可接受風險」方式；高風險項目處理的狀況；風險「再評鑑」的方式及結果
- 佐證資料：**可接受風險值評估紀錄**、**高風險處理紀錄 (風險改善計畫)**、**再評鑑評估紀錄**

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

三、個人資料蒐集、處理及利用之內部管理程序

- 查核項目 (1)：蒐集、處理及利用個人資料時，是否已符合「適當、相關且符合資料極小化」的原則？
- 稽核重點：由業務職掌，了解所設計的機制或表單是否符合**「適當、相關且符合資料極小化」**之原則
- 佐證資料：**「適當、相關且符合資料極小化」之討論、審核紀錄**
- 查核項目 (2)：是否維護個人資料之正確且保持更新？
- 稽核重點：當事人資料變更之處理機制，以證明資料之處理、利用時為正確資料
- 佐證資料：**當事人變更紀錄**、**業管單位處理紀錄**

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

三、個人資料蒐集、處理及利用之內部管理程序

- 查核項目 (3)：是否已建立與執行相關程序，以確保組織保留個人資料所需的保存期限？
- 稽核重點：保存期限設定之佐證
- 佐證資料：個人資料檔案清冊中的**「保有依據」**
- 查核項目 (4)：是否已建立並實作個人資料檔案銷毀作業，當特定目的消失或保存期限屆滿時，合理地銷毀個人資料檔案？
- 稽核重點：屆滿個資銷毀之現況
- 佐證資料：**個資銷毀紀錄**、**委外銷毀之協議**、**保密文件**

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

三、個人資料蒐集、處理及利用之內部管理程序

- 查核項目 (5)：是否已建立與執行相關程序，確保當個人資料以電子或人工方式在組織內外傳輸的過程中，皆施予合適之控管措施，進而提供資料傳遞之安全防護？
- 稽核重點：電子或紙本個資傳輸控管方式
- 佐證資料：**電子**：Email 加密；**紙本**：專人親送、彌封等

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

四、資料安全管理及人員管理

- 查核項目 (1)：是否對存放於系統上之備份資料已定期執行回復測試？個人資料的授權與存取作業是否已在合法目的下執行？
- 稽核重點：了解系統之相關管控措施，如備份、授權存取、帳號清查等
- 佐證資料：**系統之管控執行紀錄**

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

四、資料安全管理及人員管理

- 查核項目 (2)：是否已建立與執行委外安全管理？是否定期審查或稽核委外廠商有關個資安全之遵循性？與委外廠商之契約是否已考慮個人資料保護要求？
- 稽核重點：委外狀況或項目；監督責任之履行；合約內容之個資管控要求
- 佐證資料：**委外合約**、**保密切結書**、**監督紀錄**
- 查核項目 (3)：針對可攜式、行動裝置或雲端服務，是否已建立並執行相關管理規定？
- 稽核重點：可攜式、行動裝置或雲端服務相關管控規定
- 佐證資料：**實地隨機抽查**是否符合規定

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

五、認知宣導與教育訓練

- 查核項目 (1)：是否已進行教育訓練或觀念宣導等方式來強化組織內人員對於個資安全的意識？辦理個人資料保護認知宣導活動完畢後，是否留存相關紀錄備查？
- 稽核重點：依要求規劃、執行、評估教育訓練
- 佐證資料：**教育訓練簽到表**等相關紀錄

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

六、設備安全管理

- 查核項目 (1)：所有涉及個人資料的資訊設備、文件與紀錄，是否皆位於良好實體環境安全管制之區域，且攜出入實體環境皆有管制？
- 稽核重點：依要求管理實體環境
- 佐證資料：**檔案櫃上鎖照片**、**人員出入紀錄表**等相關紀錄

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

七、使用紀錄、軌跡資料，以及證據保存

- 查核項目 & 佐證資料：

1. 提供當事人行使權利之紀錄
2. 建立並維持當事人同意紀錄及其保存機制
3. 所有涉及個人資料的伺服器作業系統、應用系統、資料庫權限，任何存取紀錄皆已妥善保存
4. 資料正確性及更正之紀錄
5. 個人資料刪除、銷毀之紀錄
6. 文件化程序或機制或紀錄
7. 隱私權公告紀錄，如公告時間或公告版本，予以當事人易於了解
8. 個人資料管理安全事故處理相關紀錄等

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

八、個人資料安全維護之整體持續改善

- 查核項目 (1)：是否定期舉辦管理審查會議？是否已建立與執行矯正處理措施，並持續追蹤確認？
- 稽核重點：管理審查辦理狀況；內外稽矯正情況；年度目標達成情況
- 佐證資料：**管理審查紀錄**、**內外稽矯正及追蹤紀錄**、**年度目標評估及追蹤紀錄**

個人資訊管理系統 (PIMS) 稽核

矯正預防處理單填寫重點(節錄)：

https://docs.google.com/spreadsheets/d/184xjw4ow5lW4yzqKJkkhJEnMRZ5OiilDpY6Rd6Yj508/edit?usp=sharing

提出單位		提出人員		提出日期	
處理單位		處理人員		處理日期	
缺失分類： 內部稽核：□建議 □缺失 外部稽核：□建議 □觀察 □次要缺失 □主要缺失			事件來源： □稽核作業 □個資事故 □自行發現 □其它：		
問題或缺失說明	*(詳加說明事件來源所揭示之問題事項)*				
原因分析	*(請就現行作業方式導致本次事件發生之原因，予以明確說明)*				
矯正措施	*(用以控制事件擴大或降低其影響程度之處置作法)*				
	預定完成日期：	追蹤人：	追蹤日期：	確認結果：	
預防措施	*(旨在消除事件成因，並防止同類事項再次發生之矯正措施)*				
	預定完成日期：	追蹤人：	追蹤日期：	確認結果：	

實作練習：個資稽核常見缺失分析

案例1 親師溝通與個資過度蒐集（紙本與程序）：

情境：某班級導師為建立家長聯絡網，要求全班學生填寫「家庭狀況調查表」，內容包含家長的身分證字號、職業、年收入及病史。

實作任務：檢視該調查表是否符合個資法「最小化原則」？

實作練習：個資稽核常見缺失分析

案例1 親師溝通與個資過度蒐集（紙本與程序）：

稽核發現（缺失點）：

- 蒐集範圍過大：親師聯絡通常不需要「身分證字號」與「精確年收入」，此舉違反比例原則。
- 告知義務缺失：表單下方未註明個資蒐集的目的、利用期間及當事人權利（如：可要求刪除）。
- 存放環境不安：導師將回收的紙本隨手放在辦公桌上，且辦公室門禁未管制，學生可輕易翻閱。

正確作法：

重新設計表單，僅保留必要聯繫資訊，並加上個資告知條款，紙本必須入櫃上鎖。

實作練習：個資稽核常見缺失分析

案例2 成績單傳送與權限漏洞（數位軌跡）：

情境：教務處職員為了方便，將全校學生的「期末成績大表（含姓名、學號、成績）」上傳至 Google Drive 雲端資料夾，並設定為「知道連結的人皆可檢視」，隨後將連結貼在校內教職員群組。

實作任務：分析此種分享方式的風險，並檢查系統 Log 能否追蹤洩密來源？

實作練習：個資稽核常見缺失分析

案例2 成績單傳送與權限漏洞（數位軌跡）：

稽核發現（缺失點）：

- 存取控制失效：設定為「公開連結」意味著連結一旦外流，全世界都能看見，不具備身分驗證。
- 缺乏軌跡紀錄：由於是公開連結，系統 Log 僅會顯示「匿名使用者」存取，發生外洩時無法追蹤是哪位教職員將連結流出。
- 敏感資料未加密：檔案本身未設密碼，且包含全校學生個資。

正確作法：

應限定特定帳號（限定教職員 E-mail）存取，並開啟「禁止下載/列印」功能，且檔案應加密處理。

實作練習：個資稽核常見缺失分析

案例3 委外「線上學習平台」的監管缺失（委外管理）：

情境：學校向某科技公司採購「數位學習平台」，並將全校學生的姓名、身分證字號匯入該系統以建立帳號。

實作任務：檢查學校對該廠商的「年度監督」紀錄。

實作練習：個資稽核常見缺失分析

案例3 委外「線上學習平台」的監管缺失（委外管理）：

稽核發現（缺失點）：

- 合約漏洞：檢視合約發現，未載明「廠商發生資安事件時的通報時限」及「合約終止後資料如何銷毀」。
- 缺乏實地或書面稽核：學校保存五年紀錄中，完全沒有廠商的「資安自我檢查表」或「弱點掃描報告」。
- 權限黑洞：廠商工程師為了維修方便，直接使用一個「萬用管理帳號」進出資料庫，學校卻無此存取紀錄。

正確作法：

補足委外合約中的個資處理協議，並要求廠商每年回傳資安檢核報告，且所有遠端維護必須申請並記錄個人身分。

03 軌跡資料與證據留存

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **紙本調閱紀錄**

1. 實體機房進出登記表：

確保所有進入機房的行為皆可追溯，防止未授權的硬體更動或資料竊取。

必填欄位：日期與時間 (進場/出場)；進場人員姓名 (若是外部廠商需註明公司名稱)；進場事由 (如：更換硬碟、系統維護、例行檢查)；陪同人員 (機房通常要求「雙人進出」，需有一名內部員工陪同)。

稽核重點：檢查員會抽查特定的「系統維護日誌」，比對當時是否真有對應的人員在機房內。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **紙本調閱紀錄**

2. 紙本文件調閱申請單 (含主管核准簽名)：

建立「知其必要」的證據軌跡，證明敏感紙本文件 (如客戶契約、人事檔案) 未被隨意翻閱。

必填欄位：申請人單位及姓名；文件名稱/編號；調閱目的；主管核准簽名 (證明程序合規)；歸還日期與簽收。

稽核重點：確認是否有「逾期未還」的情況，以及調閱程序是否早於實際拿到文件的時間。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **紙本調閱紀錄**

3. 訪客登記簿：

管理辦公室整體的邊界安全，區分「內部員工」與「外部人員」。

必填欄位：

身分驗證：訪客需出示證件 (如身分證、駕照) 供櫃檯比對，並登記證件末三碼 (符合個資法最小化原則)。

標示配戴：登記後應發放「訪客證」，並要求全程配戴於胸前顯眼處。

被訪人確認：訪客不能自行進入，必須由該業務承辦人 (被訪人) 親自到櫃檯帶領。

禁止區域規範：登記簿後方可加註「訪客禁區須知」(如：辦公區嚴禁拍照、禁止操作未授權設備)。

稽核重點：檢查員會查看登記簿是否有漏填 (例如有進場沒出場)，或訪客停留時間是否異常過長。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **系統存取 Log (軌跡資料)**

1. 身分驗證：

這是最基礎的「門禁卡」。除了記錄誰進來了，「失敗紀錄」更是資安防禦的重點，可用於偵測暴力破解攻擊。

關鍵紀錄欄位：

使用者帳號、來源 IP 與設備名稱、時間戳記至秒、結果代碼 (成功、密碼錯誤、帳號遭停用、多因子驗證 MFA 失敗)。

實務建議：

應設定告警機制。例如：同一 IP 在 1 分鐘內登入失敗超過 5 次，系統應自動鎖定並發送通知給資安管理員。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **系統存取 Log (軌跡資料)**

2. 特權帳號：

「管理者」擁有最高權限，其行為必須受到最嚴格的監控。這類日誌稱為「操作日誌」，用以預防「內部舞弊」或「帳號遭盜用後的大規模破壞」。

關鍵紀錄欄位：

權限變更、設定異動、高風險操作。

實務建議：

推動「代行權限」制度，管理者執行高風險指令時，系統應要求輸入「工單編號」或「審核代碼」，以便日後與申請文件比對。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **系統存取 Log (軌跡資料)**

3. 存取行為：

這是行政檢查 (特別是個資法檢查) 的重中之重。僅有登入紀錄是不夠的，稽核員會要求證明：「當員工進到資料庫後，他看了哪些個資？有沒有大量帶走？」

關鍵紀錄欄位：

查詢：針對身分證字號、病歷、薪資等敏感欄位的查詢行為；匯出：將查詢結果存成 CSV 或 Excel 的動作；大量存取：短時間內讀取超過常規數量的行為。

實務建議：

查詢結果應預設遮罩（如：A123***789），若要查看明文或匯出，必須觸發「二次審核」或留下「專項事由說明」；若資料庫本身效能負荷不了詳細日誌，建議導入第三方稽核工具來側錄所有 SQL 指令。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **監視器畫面**

1. 機房影像監控：

機房是資訊心臟，監控重點在於「設備接觸」與「操作行為」。影像必須能清楚辨識進入者的面貌，以及其在機房內停留的位置 (如：在哪個機櫃前操作)。

監控要點：

機櫃前後門：確認是否有未授權插拔硬碟、接取 USB 或筆電的行為。

環控設備：避免人員誤觸空調、電力開關或滅火系統。

實務建議：

應具備動態偵測錄影功能，節省硬碟空間，但需確保人員進入前 5 秒至離開後 5 秒皆有完整截錄

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **監視器畫面**

2. 文件庫房影像監控：

針對存放機密合約、個人資料申請書、傳票等紙本資料的區域。此處影像旨在防止「未經授權的攜出」或「現場翻拍」。

監控要點：

存取動線：記錄人員領取文件與歸還文件的完整過程。

禁止行為偵測：監控是否有在內使用手機拍攝文件或影印資料的動作。

實務建議：

庫房內應維持足夠照明，避免夜間或昏暗環境下影像模糊，導致檢查時無法辨識人員身分。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **監視器畫面**

3. 出入口影像監控：

包含大樓門廳、辦公區入口及後門。這是建立「人員軌跡」的第一道數據，用來與訪客登記簿或門禁刷卡紀錄進行交叉比對。

監控要點：

尾隨進場：檢查是否有人趁前面同事刷卡時溜進場。

異常時段進出：記錄非上班時間、週末或假日的進出人員。

實務建議：

鏡頭角度應設在與人眼平視或略高處，確保能清楚拍攝面部，且需涵蓋門禁讀卡機位置。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **同意書與合約**

1. 客戶個資蒐集同意書：

這是合規的起點。根據個資法，蒐集資料前必須明確告知並取得同意。檢查員會核對你的資料庫欄位 (如：出生年月日、電話) 是否超出了同意書宣稱的範圍。

核心要素：

告知義務：包含蒐集目的、類別、利用期間、地區、對象及方式。

當事人權利：明確告知客戶可以要求查詢、閱覽、製給複製本、補充、更正、停止蒐集或刪除。

勾選機制：必須是「主動勾選」或「簽名」，不可預設同意。

實務建議：

若為數位同意書，系統需記錄「點擊同意時的 IP」與「精確時間戳記」作為保存五年的電子軌跡。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **同意書與合約**

2. 員工保密協定：

用於建立內部人員的法律約束力。證明公司已盡到「管理責任」，若發生員工洩密，公司可舉證已事先告誡並要求保密，從而釐清公司與個人的法律責任。

核心要素：

保密範圍：定義哪些資訊屬於機密 (如：薪資、技術規格、客戶清單)。

離職後義務：約定離職後仍需負擔保密義務的期限。

違約賠償：明確違反協定時的法律後果與賠償機制。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **同意書與合約**

2. 員工保密協定：

實務建議：

除了入職簽署，建議每年進行「資安宣導」並讓員工簽署當年度的復訓確認書，這在行政檢查中能展現公司有持續落實教育訓練。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **同意書與合約**

3. 委外廠商的資安合約與個資處理協議：

當將資料交給雲端商、物流商或廣告商處理時，仍負有監管責任。

核心要素：

複委託限制：廠商若要再轉包給其他公司，必須事先取得你的書面同意。

安全性要求：要求廠商必須具備加密儲存、定期掃毒、人員權限控管等措施。

稽核權力：合約須載明「甲方有權派員或委託第三方至乙方 (廠商) 處所進行實地檢查」。

事故通報：明確規定廠商若發生資安事件，必須在幾小時內通報你公司。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **同意書與合約**

3. 委外廠商的資安合約與個資處理協議：

實務建議：

行政檢查時，檢查員常會問：「你們怎麼監督委外廠商？」此時除了拿出合約，若能附上「年度委外稽核報告」，專業度會大幅提升。

感謝聆聽

三、資安防禦網—事故應變演練與技術檢測解析

主講人：國立臺北商業大學 徐國鈞主任

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

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

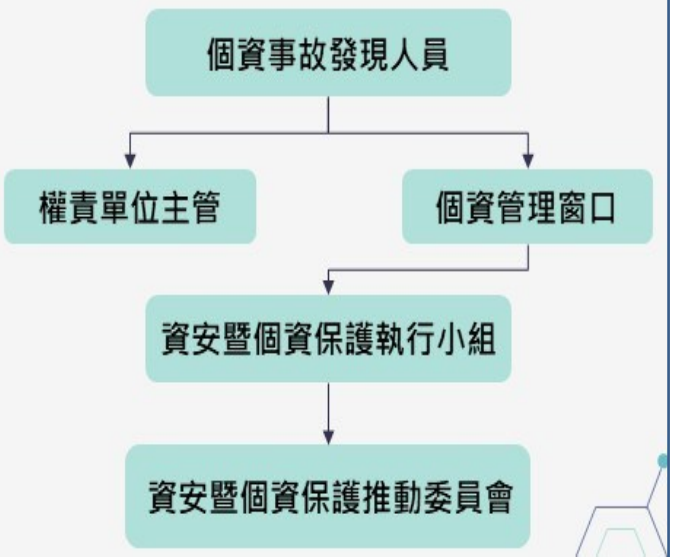
- 學校、機構應訂定應變機制，在發生個人資料被竊取、洩露、竄改或其他侵害事故時，迅速處理以保護當事人之權益。其應變機制，應包括下列事項：

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：○年○月○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○筆/受影響人數○人/財物損失金額○元/公司帳務損失約○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：○○ (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	□個人資料檔案遭通竊取、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：

十三、單位個人資料管理窗口分派業務權責單位

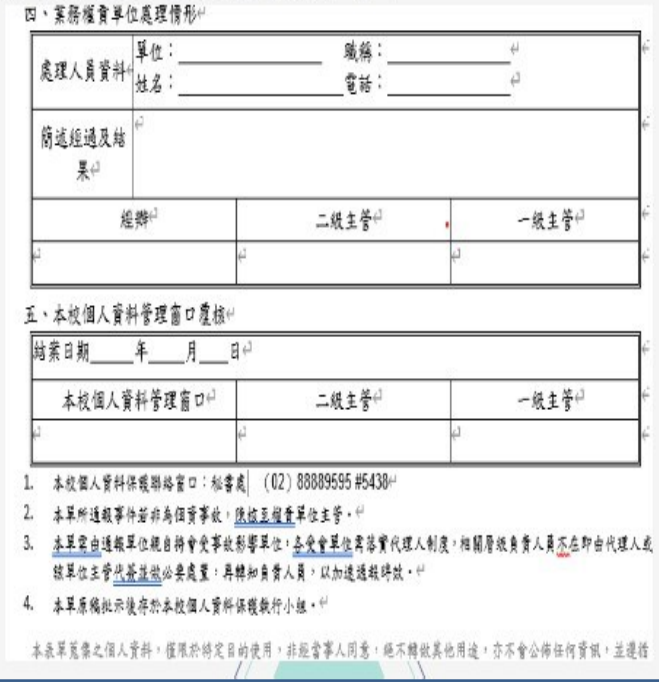
業務權責單位：＿＿＿＿＿＿單位

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. 本單完成通報單位親自將會受事故影響單位，告知會單位實際代理人制度，相關層級負責人員不在即由代理人或
   該單位主管代為處理必要處置；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

NOTE

肆、附錄

一、地區輔導員對應教育部所屬學校分組一覽表

組別	地區輔導員	委員	縣市	機關名稱	縣市	機關名稱
1	林博民	徐國鈞	基隆	國立基隆女子高級中學	基隆	二信高中
			基隆	國立基隆高級中學	基隆	光隆家商
			基隆	國立基隆特殊教育學校	基隆	培德工家
			基隆	國立基隆高級商工職業學校	基隆	輔大聖心高中
			基隆	國立臺灣海洋大學附屬基隆海事高級中等學校		
2	林欣穎	徐國鈞	台北	國立臺灣師範大學附屬高級中學		
			台北	國立政治大學附設實驗國民小學		
			台北	國立政治大學附屬高級中學		
			台北	國立臺北教育大學附設實驗國民小學		
			新北	國立華僑高級中等學校		
3	張偉勤	徐國鈞	桃園	國立中央大學附屬中壢高級中學	新竹	內思高工
			桃園	國立臺北科技大學附屬桃園農工高級中等學校	新竹	光復高中
			新竹	國立新竹高級工業職業學校		
			新竹	國立清華大學附設實驗國民小學		
4	王佳瑜	周冠吉	新竹	國立新竹特殊教育學校	新竹	磐石高中
			新竹	國立竹東高級中學	新竹	曙光女中
			新竹	國立新竹女子高級中學	新竹	世界高中
			新竹	國立新竹高級中學	新竹	仰德高中
					新竹	義民高中
5	洪郁婷	周冠吉	苗栗	國立苑裡高級中學	苗栗	中興商工
			苗栗	國立卓蘭高級中等學校	苗栗	君毅高中
			苗栗	國立竹南高級中學	苗栗	育民工家
			苗栗	國立苗栗特殊教育學校		
			苗栗	國立苗栗高級商業職業學校		
6	邱詩育	周冠吉	新竹	國立關西高級中學	新竹	忠信高中
			新竹	國立竹北高級中學	新竹	東泰高中
			新竹	國立新竹科學園區實驗高級中等學校		
			新竹	國立新竹高級商業職業學校		
7	吳松達	周冠吉	苗栗	國立大湖高級農工職業學校	苗栗	建臺高中
			苗栗	國立苗栗高級中學	苗栗	全人實驗高中
			苗栗	國立苗栗高級農工職業學校	苗栗	賢德工商
					苗栗	龍德家商
8	廖文賢	陳偉嵩	台中	財團法人中華幼兒教育發展基金會		
			台中	財團法人台灣省中小學校教職員福利文教基金會		
			台中	國立中興大學附屬高級中學		
			台中	國立臺中教育大學附設實驗國民小學		
			台中	國立中興大學附屬臺中高級農業職業學校		
			台中	國立中科實驗高級中學		
9	涂淵維	陳偉嵩	南投	國立南投高級商業職業學校	南投	普台高中
			南投	國立中興高級中學	南投	五育高中
			南投	國立仁愛高級農業職業學校		
			南投	國立竹山高級中學		
			南投	國立暨南國際大學附屬高級中學		
			南投	國立南投特殊教育學校	南投	同德高中
			南投	國立草屯高級商工職業學校	南投	弘明實驗高中
			南投	國立南投高級中學	南投	三育高中
			南投	國立水里高級商工職業學校		
			南投	國立埔里高級工業職業學校		
10	廖茂松	黃攸德	彰化	國立彰化女子高級中學		
			彰化	國立二林高級工商職業學校		
			彰化	國立永靖高級工業職業學校		

組別	地區輔導員	委員	縣市	機關名稱	縣市	機關名稱
			彰化	國立和美實驗學校		
			彰化	國立彰化師範大學附屬高級工業職業學校		
			彰化	國立鹿港高級中學		
			彰化	國立彰化高級商業職業學校		
			彰化	國立秀水高級工業職業學校		
			彰化	國立彰化高級中學		
			彰化	國立彰化特殊教育學校		
11	戴余庭	黃攸德	彰化	國立員林高級中學	彰化	文興高中
			彰化	國立北斗高級家事商業職業學校	彰化	大慶商工
			彰化	國立員林高級農工職業學校	彰化	正德高中
			彰化	國立溪湖高級中學	彰化	精誠高中
			彰化	國立員林高級家事商業職業學校	彰化	達德商工
			彰化	國立員林崇實高級工業職業學校		
12	李右任	黃攸德	雲林	國立雲林特殊教育學校	雲林	大德工商
			雲林	國立虎尾高級中學	雲林	巨人高中
			雲林	國立西螺高級農工職業學校	雲林	義峰高中
			雲林	國立斗六高級中學	雲林	正心高中
			雲林	國立土庫高級商工職業學校	雲林	福智高中
			雲林	國立斗六高級家事商業職業學校	雲林	大成商工
			雲林	國立北港高級農工職業學校	雲林	文生高中
			雲林	國立虎尾高級農工職業學校	雲林	永年高中
			雲林	國立北港高級中學	雲林	揚子高中
					雲林	維多利亞實驗高中
13	劉錫禎	黃柏森	嘉義	國立嘉義高中	嘉義	立仁高中
			嘉義	國立嘉義高級商業職業學校	嘉義	協同高中
			嘉義	國立嘉義特殊教育學校		
			嘉義	國立嘉義高級家事職業學校		
			嘉義	國立華南高級商業職業學校		
			嘉義	國立嘉義女子高級中學		
			嘉義	國立嘉科實驗高級中等學校		
14	洪建楓	黃柏森	嘉義	國立新港藝術高級中學	嘉義	輔仁高中
			嘉義	國立東石高級中學	嘉義	興華高中
			嘉義	國立嘉義高級工業職業學校	嘉義	同濟高中
			嘉義	國立民雄高級農工職業學校	嘉義	東吳工家
			嘉義	國立嘉義大學附設實驗國民小學	嘉義	萬能工商
					嘉義	嘉華高中
15	陳宗元	俞怡中	台南	國立南科國際實驗高級中學	台南	六信高中
			台南	國立北門高級農工職業學校	台南	港明高中
			台南	國立北門高級中學	台南	陽明工商
			台南	國立臺南第二高級中學	台南	慈幼工商
			台南	國立善化高級中學	台南	新榮高中
			台南	國立臺南大學附設實驗國民小學		
			台南	國立臺南大學附屬高級中學		
			台南	國立後壁高級中學		
			台南	國立新營高級工業職業學校		
			台南	國立白河高級商工職業學校		
			台南	國立新營高級中學		
16	曾鏞毅	鐘沛原	台南	國立臺南高級海事水產職業學校	高雄	中山工商
			台南	國立臺南女子高級中學	高雄	正義高中
			台南	國立新化高級工業職業學校	高雄	普門高中
			台南	國立玉井高級工商職業學校	高雄	旗美商工
			台南	國立曾文高級家事商業職業學校	台南	長榮高中
			台南	國立曾文高級農工職業學校	台南	德光高中
			高雄	國立旗山高級農工職業學校		
			高雄	國立旗美高級中學		
			高雄	國立岡山高級農工職業學校		
			高雄	國立岡山高級中學		

組別	地區輔導員	委員	縣市	機關名稱	縣市	機關名稱
17	蕭名宏	俞怡中	台南	國立成功大學附屬臺南工業高級中等學校	台南	興國高中
			台南	國立臺南家齊高級中等學校	台南	明達高中
			台南	國立臺南第一高級中學	台南	南光高中
			台南	國立臺南特殊教育學校	台南	光華高中
			台南	國立臺南大學附屬啟聰學校	台南	育德工家
			台南	國立新化高級中學	台南	亞洲餐旅職業學校
					台南	南英商工
					台南	崑山高中
					台南	聖功女中
					台南	慈濟高中
18	歐俊男	鐘沛原	台南	國立臺南高級商業職業學校	台南	黎明高中
			台南	國立新豐高級中學	台南	長榮女中
			高雄	國立高雄師範大學附屬高級中學	台南	瀛海高中
			高雄	國立鳳新高級中學	高雄	高苑工商
			高雄	國立中山大學附屬國光高級中學	高雄	高英工商
			高雄	國立高雄餐旅大學附屬餐旅高級中等學校	高雄	華德工家
			高雄	國立鳳山高級中學	高雄	義大國際高中
			高雄	國立鳳山高級商工職業學校	高雄	新光高中
			高雄	國立高科實驗高級中等學校		
19	吳家華	鐘沛原	屏東	國立屏東高級中學	屏東	屏榮高中
			屏東	國立屏北高級中學	屏東	陸興高中
			屏東	國立屏東女子高級中學		
			屏東	國立內埔高級農工職業學校		
			屏東	國立潮州高級中學		
			屏東	國立屏科實驗高級中等學校		
20	童信源	鐘沛原	屏東	國立屏東大學附設實驗國民小學	屏東	日新工商
			屏東	國立東港高級海事水產職業學校	屏東	民生家商
			屏東	國立佳冬高級農業職業學校	屏東	美和高中
			屏東	國立恆春高級工商職業學校		
			屏東	國立屏東特殊教育學校		
			屏東	國立屏東高級工業職業學校		
21	巫培爾	劉耀明	台東	國立成功商業水產職業學校	台東	公東高工
			台東	國立臺東大學附設實驗國民小學	台東	育仁高中
			台東	國立臺東大學附屬體育高級中學	台東	均一高中
			台東	國立臺東女子高級中學		
			台東	國立臺東大學附屬特殊教育學校		
			台東	國立臺東高級商業職業學校		
			台東	國立關山高級工商職業學校		
			台東	國立臺東高級中學		
22	吳振銘	陳應南	花蓮	國立東華大學附設實驗國民小學	花蓮	上騰工商
			花蓮	國立花蓮女子高級中學	花蓮	四維高中
			花蓮	國立光復高級商工職業學校		
			花蓮	國立花蓮特殊教育學校		
			花蓮	國立花蓮高級商業職業學校		
23	黃楨喻	陳應南	花蓮	國立玉里高級中學	花蓮	慈濟大學附中
			花蓮	國立花蓮高級中學	花蓮	海星高中
			花蓮	國立花蓮高級農業職業學校		
			花蓮	國立花蓮高級工業職業學校		
24	黃俊宏	曾國旭	宜蘭	國立羅東高級工業職業學校	宜蘭	慧燈高中
			宜蘭	國立蘭陽女子高級中學	宜蘭	中道高中
			宜蘭	國立宜蘭特殊教育學校		
			宜蘭	國立羅東高級中學		
			宜蘭	國立宜蘭高級商業職業學校		
			宜蘭	國立羅東高級商業職業學校		
			宜蘭	國立頭城高級家事商業職業學校		
			宜蘭	國立宜蘭高級中學		
			宜蘭	國立蘇澳高級海事水產職業學校		

組別	地區 輔導員	委員	縣市	機關名稱	縣市	機關名稱
25	劉耀明	劉耀明	離島	國立金門高級農工職業學校		
			離島	國立金門高級中學		
			離島	國立馬公高級中學		
			離島	國立澎湖高級海事水產職業學校		
			離島	國立馬祖高級中學		

二、個人資料保護法

修正日期：民國 114 年 11 月 11 日

第 一 章 總則

第 1 條

為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。

第 1-1 條

本法之主管機關為個人資料保護委員會。

第 1-2 條

1 中央及地方各級政府應致力配合推動達成本法立法目的之具體措施，確保其所轄公務機關及所管非公務機關，於執行職務及業務時遵守本法規定，共同建構安全可信賴之個人資料保護環境。

2 為落實個人資料保護相關事項，主管機關得召開個人資料保護政策推進會議；其運作方式及其他相關事項之辦法，由主管機關定之。

第 2 條

本法用詞，定義如下：

一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

三、蒐集：指以任何方式取得個人資料。

四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

五、利用：指將蒐集之個人資料為處理以外之使用。

六、國際傳輸：指將個人資料作跨國（境）之處理或利用。

七、公務機關：指依法行使公權力之中央或地方機關或行政法人。

八、非公務機關：指前款以外之自然人、法人或其他團體。

九、當事人：指個人資料之本人。

第 3 條

當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

一、查詢或請求閱覽。

二、請求製給複製本。

三、請求補充或更正。

四、請求停止蒐集、處理或利用。

五、請求刪除。

第 4 條

受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。

第 5 條

個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，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。

第 6 條

1 有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

一、法律明文規定。

二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

2 依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。

第 7 條

1 第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。

2 第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。

3 公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。

4 蒐集者就本法所稱經當事人同意之事實，應負舉證責任。

第 8 條

1 公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

一、公務機關或非公務機關名稱。

二、蒐集之目的。

三、個人資料之類別。
四、個人資料利用之期間、地區、對象及方式。
五、當事人依第三條規定得行使之權利及方式。
六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

2 有下列情形之一者，得免為前項之告知：
一、依法律規定得免告知。
二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
三、告知將妨害公務機關執行法定職務。
四、告知將妨害公共利益。
五、當事人明知應告知之內容。
六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

第 9 條

1 公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。

2 有下列情形之一者，得免為前項之告知：
一、有前條第二項所列各款情形之一。
二、當事人自行公開或其他已合法公開之個人資料。
三、不能向當事人或其法定代理人為告知。
四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。
五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

3 第一項之告知，得於首次對當事人為利用時併同為之。

第 10 條

公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：
一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
二、妨害公務機關執行法定職務。
三、妨害該蒐集機關或第三人之重大利益。

第 11 條

1 公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。

2 個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。

3 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

4 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

5 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

第 12 條

1 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。

2 前項情形符合一定通報範圍者，公務機關或非公務機關應通報下列機關：

一、公務機關：向主管機關及依第二十一條之一第一項規定收受其實施情形之機關通報。

二、非公務機關：向主管機關通報。主管機關受理通報後，並轉知其目的事業主管機關。

3 第一項情形，公務機關或非公務機關應採取即時有效之應變措施，防止事故之擴大，及記載相關事實、影響、已採取之因應措施，並保存相關紀錄，以備主管機關查驗。

4 前三項應通知或通報之內容、方式、時限與通報範圍、應變措施、紀錄保存及其他相關事項之辦法，由主管機關定之。

第 13 條

1 公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

2 公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

第 14 條

查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收必要成本費用。

第 二 章 公務機關對個人資料之蒐集、處理及利用

第 15 條

公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

一、執行法定職務必要範圍內。

二、經當事人同意。

三、對當事人權益無侵害。

第 16 條

公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：

一、法律明文規定。

二、為維護國家安全或增進公共利益所必要。

三、為免除當事人之生命、身體、自由或財產上之危險。

四、為防止他人權益之重大危害。

五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

六、有利於當事人權益。

七、經當事人同意。

第 17 條

公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同：

一、個人資料檔案名稱。

二、保有機關名稱及聯絡方式。

三、個人資料檔案保有之依據及特定目的。

四、個人資料之類別。

第 18 條

1 公務機關應置個人資料保護長，由機關首長指派適當人員兼任，並配置適當人力及資源，負責統籌推動及督導考核本機關、所屬或所監督公務機關之個人資料保護相關事務。

2 公務機關應指定專人辦理個人資料檔案安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏；其安全維護、管理機制、應採取之措施及其他相關事項之辦法，由主管機關定之。

3 公務機關不得因所屬人員依法執行個人資料保護職務而予以不利之處分或管理措施。

4 主管機關應妥善規劃推動第一項及第二項相關人員之職能訓練，增進其個人資料保護專業知能。

5 第一項、第二項相關人員之職掌、職能條件、訓練及其他相關事項之辦法，由主管機關定之。

第 三 章 非公務機關對個人資料之蒐集、處理及利用

第 19 條

1 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

一、法律明文規定。

二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

五、經當事人同意。

六、為增進公共利益所必要。

七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

八、對當事人權益無侵害。

2 蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

第 20 條

1 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：

一、法律明文規定。
二、為增進公共利益所必要。
三、為免除當事人之生命、身體、自由或財產上之危險。
四、為防止他人權益之重大危害。
五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
六、經當事人同意。
七、有利於當事人權益。

2 非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

3 非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

第 20-1 條

1 非公務機關保有個人資料檔案者，應辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

2 前項個人資料檔案安全維護事項、管理機制、應採取之措施及其他相關事項之辦法，由主管機關定之。

第 21 條

非公務機關為國際傳輸個人資料，而有下列情形之一者，主管機關得限制之：
一、涉及國家重大利益。
二、國際條約或協定有特別規定。
三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。
四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。

第 三 章之一 行政監督

第 一 節 對公務機關之監督

第 21-1 條

1 公務機關應每年向上級機關或監督機關提出個人資料保護管理事項實施情形；無上級機關或監督機關者，依下列各款規定辦理：
一、總統府、國家安全會議及五院，向主管機關提出。
二、直轄市政府、直轄市議會、縣（市）政府及縣（市）議會，向主管機關提出。
三、直轄市山地原住民區公所、直轄市山地原住民區民代表會，向直轄市政府提出；鄉（鎮、市）公所、鄉（鎮、市）民代表會，向縣政府提出。

2 公務機關應督導及稽核其所屬、所監督之公務機關、所轄鄉（鎮、市）公所、直轄市山地原住民區公所及鄉（鎮、市）民代表會、直轄市山地原住民區民代表會之個人資料保護管理事項實施情形。

3 依前項規定稽核後，發現受稽核機關實施情形有缺失或待改善者，受稽核機關應向稽核機關提出改善報告，並由稽核機關審查後，連同稽核結果送交主管機關。

4 稽核機關或主管機關認有必要時，得要求受稽核機關進行說明或調整。

5 前四項實施情形之必要內容、稽核之頻率、內容與方法、結果之交付、改善報告之提出及其他相關事項之辦法，由主管機關定之。

第 21-2 條

1 主管機關應定期或不定期稽核公務機關之個人資料保護管理事項實施情形；必要時，得請求前條第二項所定稽核機關協助。

2 依前項規定稽核後，發現受稽核機關實施情形有缺失或待改善者，受稽核機關應提出改善報告，送交依前條第一項規定收受其實施情形之機關審查後，由該審查機關送交主管機關。

3 前項審查機關或主管機關認有必要時，得要求受稽核機關進行說明或調整。

4 前三項稽核之頻率、內容與方法、改善報告之提出及其他相關事項之辦法，由主管機關定之。

5 依前條及本條參與稽核之人員，對於因執行稽核所知悉或持有之資料，負保密義務。

第 21-3 條

1 公務機關有違反本法規定之虞時，主管機關得請公務機關提出資料及說明，或派員攜帶執行職務證明文件進行實地檢查，除依法規規定有保密之必要者外，公務機關及其相關人員有配合之義務。

2 前項實地檢查，必要時得請求第二十一條之一第二項所定稽核機關協助。

3 參與檢查之人員，對於因執行檢查所知悉或持有之資料，負保密義務。

第 21-4 條

1 公務機關有違反本法規定之情事者，由主管機關令其限期改正，該公務機關應依限為適當之改正，並應將改正情形以書面答覆主管機關。

2 公務機關未依前項規定改正者，主管機關得公布其名稱及其違法情形。

3 公務機關所屬人員未依本法規定辦理者，應按其情節輕重，依相關法令規定予以懲戒、懲處或懲罰。

第 21-5 條

本節之規定，於情報機關不適用之。

第 二 節 對非公務機關之監督

第 22 條

1 主管機關認非公務機關有違反本法規定之虞，或為檢視其落實本法情形而認有必要時，得依下列方式進行檢查：

一、通知非公務機關或其相關人員陳述意見。

二、通知非公務機關或其相關人員提供必要之文書、資料、物品或為其他配合措施。

三、自行或會同中央目的事業主管機關、直轄市、縣（市）政府或其他有關機關派員攜帶執行職務證明文件進入檢查，並得令相關人員為必要之說明、配合措施或提供相關證明資料。

2 前項檢視落實本法情形檢查作業之規劃、評估方式、考量因素、中央目的事業主管機關、直轄市、縣（市）政府或有關機關之協力事項及其他相關事項之辦法，由主管機關定之。

3 主管機關為第一項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。對於應扣

留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。

4 對於依第一項或前項所為之通知、進入、檢查或處分，非公務機關及其相關人員無正當理由不得規避、妨礙或拒絕。

5 主管機關為第一項第三款檢查時，得率同資訊、電信、法律或其他專業人員共同為之。

6 參與檢查之人員，對於因執行檢查所知悉或持有之資料，負保密義務，並應注意被檢查者之名譽。

7 第一項檢查之執行，主管機關於必要時得請求中央目的事業主管機關、直轄市、縣（市）政府或其他相關機關（構）配合採取有效措施或提供協助。

第 23 條

1 對於前條第三項扣留物或複製物，應加封緘或其他標識，並為適當之處置；其不便搬運或保管者，得命人看守或交由所有人或其他適當之人保管。

2 扣留物或複製物已無留存之必要，或決定不予處罰或未為沒入之裁處者，應發還之。但應沒入或為調查他案應留存者，不在此限。

第 24 條

1 非公務機關、物之所有人、持有人、保管人或利害關係人對前二條之要求、強制、扣留或複製行為不服者，得向主管機關聲明異議。

2 前項聲明異議，主管機關認為有理由者，應立即停止或變更其行為；認為無理由者，得繼續執行。經該聲明異議之人請求時，應將聲明異議之理由製作紀錄交付之。

3 對於主管機關前項決定不服者，僅得於對該案件之實體決定聲明不服時一併聲明之。但第一項之人依法不得對該案件之實體決定聲明不服時，得單獨對第一項之行為逕行提起行政訴訟。

第 25 條

1 非公務機關有違反本法規定之情事者，主管機關除依本法規定裁處罰鍰外，並得為下列處分：

一、禁止蒐集、處理或利用個人資料。

二、命令刪除經處理之個人資料檔案。

三、沒入或令銷毀違法蒐集之個人資料。

四、公布違法情形，及其姓名或名稱與負責人。

2 主管機關為前項處分時，應於防制違反本法規定情事之必要範圍內，採取對該非公務機關權益損害最少之方法為之。

第 26 條

主管機關依第二十二條規定檢查後，未發現有違反本法規定之情事者，經該非公務機關同意後，得公布檢查結果。

第 27 條

（刪除）

第 四 章 損害賠償及團體訴訟

第 28 條

1 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。

2 被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。

3 依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。

4 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。

5 同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。

6 第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

第 29 條

1 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。

2 依前項規定請求賠償者，適用前條第二項至第六項規定。

第 30 條

損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。

第 31 條

損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定。

第 32 條

依本章規定提起訴訟之財團法人或公益社團法人，應符合下列要件：

一、財團法人之登記財產總額達新臺幣一千萬元或社團法人之社員人數達一百人。

二、保護個人資料事項於其章程所定目的範圍內。

三、許可設立三年以上。

第 33 條

1 依本法規定對於公務機關提起損害賠償訴訟者，專屬該機關所在地之地方法院管轄。對於非公務機關提起者，專屬其主事務所、主營業所或住所地之地方法院管轄。

2 前項非公務機關為自然人，而其在中華民國現無住所或住所不明者，以其在中華民國之居所，視為其住所；無居所或居所不明者，以其在中華民國最後之住所，視為其住所；無最後住所者，專屬中央政府所在地之地方法院管轄。

3 第一項非公務機關為自然人以外之法人或其他團體，而其在中華民國現無主事務所、主營業所或主事務所、主營業所不明者，專屬中央政府所在地之地方法院管轄。

第 34 條

1 對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人二十人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。當事人得於言詞辯論終結前以書面撤回訴訟實施權之授與，並通知法院。

2 前項訴訟，法院得依聲請或依職權公告曉示其他因同一原因事實受有損害之當事人，得於一定期間內向前項起訴之財團法人或公益社團法人授與訴訟實施權，由該財團法人或公益社團法人於第一審言詞辯論終結前，擴張應受判決事項之聲明。

3 其他因同一原因事實受有損害之當事人未依前項規定授與訴訟實施權者，亦得於法院公告曉示之一定期間內起訴，由法院併案審理。

4 其他因同一原因事實受有損害之當事人，亦得聲請法院為前項之公告。

5 前二項公告，應揭示於法院公告處、資訊網路及其他適當處所；法院認為必要時，並得命登載於公報或新聞紙，或用其他方法公告之，其費用由國庫墊付。

6 依第一項規定提起訴訟之財團法人或公益社團法人，其標的價額超過新臺幣六十萬元者，超過部分暫免徵裁判費。

第 35 條

1 當事人依前條第一項規定撤回訴訟實施權之授與者，該部分訴訟程序當然停止，該當事人應即聲明承受訴訟，法院亦得依職權命該當事人承受訴訟。

2 財團法人或公益社團法人依前條規定起訴後，因部分當事人撤回訴訟實施權之授與，致其餘部分不足二十人者，仍得就其餘部分繼續進行訴訟。

第 36 條

各當事人於第三十四條第一項及第二項之損害賠償請求權，其時效應分別計算。

第 37 條

1 財團法人或公益社團法人就當事人授與訴訟實施權之事件，有為一切訴訟行為之權。但當事人得限制其為捨棄、撤回或和解。

2 前項當事人中一人所為之限制，其效力不及於其他當事人。

3 第一項之限制，應於第三十四條第一項之文書內表明，或以書狀提出於法院。

第 38 條

1 當事人對於第三十四條訴訟之判決不服者，得於財團法人或公益社團法人上訴期間屆滿前，撤回訴訟實施權之授與，依法提起上訴。

2 財團法人或公益社團法人於收受判決書正本後，應即將其結果通知當事人，並應於七日內將是否提起上訴之意旨以書面通知當事人。

第 39 條

1 財團法人或公益社團法人應將第三十四條訴訟結果所得之賠償，扣除訴訟必要費用後，分別交付授與訴訟實施權之當事人。

2 提起第三十四條第一項訴訟之財團法人或公益社團法人，均不得請求報酬。

第 40 條

依本章規定提起訴訟之財團法人或公益社團法人，應委任律師代理訴訟。

第 五 章 罰則

第 41 條

意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。

第 42 條

意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。

第 43 條

中華民國人民在中華民國領域外對中華民國人民犯前二條之罪者，亦適用之。

第 44 條

公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。

第 45 條

本章之罪，須告訴乃論。但犯第四十一條之罪者，或對公務機關犯第四十二條之罪者，不在此限。

第 46 條

犯本章之罪，其他法律有較重處罰規定者，從其規定。

第 47 條

非公務機關有下列情事之一者，由主管機關處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：

一、違反第六條第一項規定。

二、違反第十九條規定。

三、違反第二十條第一項規定。

四、違反依第二十一條規定所為限制國際傳輸之命令或處分。

第 48 條

1 非公務機關有下列情事之一者，由主管機關令其限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：

一、違反第八條或第九條規定。

二、違反第十條、第十一條或第十三條規定。

三、違反第十二條第一項或依第四項所定辦法中有關通知之內容、方式或時限之規定。

四、違反第二十條第二項或第三項規定。

2 非公務機關違反第十二條第二項、第三項或依第四項所定辦法中有關通報之內容、方式、時限、應變措施、紀錄保存之規定者，由主管機關處新臺幣二萬元以上二十萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處罰。

3 非公務機關有下列情事之一者，由主管機關處新臺幣二萬元以上二百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處新臺幣十五萬元以上一千五百萬元以下罰鍰：

一、違反第二十條之一第一項規定。

二、違反依第二十條之一第二項所定辦法中有關個人資料檔案安全維護事項、管理機制、應採取措施之規定。

三、未依第五十一條之一第三項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

四、違反第五十一條之一第四項所定辦法中有關計畫或處理方法應具備之內容、執行方式或基準之規定。

4 非公務機關有前項各款情事之一，其情節重大者，由主管機關處新臺幣十五萬元以上一千五百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處罰。

第 49 條

非公務機關違反第二十二條第四項規定者，由主管機關處新臺幣二萬元以上二十萬元以下罰鍰。

第 50 條

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。

第 六 章 附則

第 51 條

1 有下列情形之一者，不適用本法規定：

一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。

二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

2 公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。

第 51-1 條

1 第二十二條第一項、第三項至第七項、第二十三條至第二十六條、第四十七條至第五十條所定對非公務機關之監督管理事項，於主管機關成立之日起六年內，由主管機關報請行政院公告一定範圍之非公務機關，仍由中央目的事業主管機關或直轄市、縣（市）政府管轄。

2 主管機關應每二年會商相關機關後，報請行政院調整減列前項公告所定一定範圍之非公務機關。

3 中央目的事業主管機關得指定前二項公告範圍之非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

4 前項計畫、處理方法應具備之內容、執行方式或基準及其他相關事項之辦法，由中央目的事業主管機關比照主管機關依第二十條之一第二項訂定之辦法定之；並得為更嚴格之規定。

第 52 條

1 第十二條第二項、第二十二條第一項、第三項、第五項、第七項、第二十三條及第二十四條規定由主管機關執行之權限，主管機關得委託或委辦其他機關（構）、行政法人或公益團體辦理。

2 於前條第一項及第二項公告之範圍內，中央目的事業主管機關或直轄市、縣（市）政府得將第二十二條第一項、第三項、第五項、第七項、第二十三條及第二十四條規定之執行權限，委任所屬機關、委託或委辦其他機關（構）、行政法人或公益團體辦理。

3 依前二項規定受委託、委辦或委任者，其成員對於因執行相關事務所知悉或持有之資料，負保密義務。

4 第一項及第二項之公益團體，不得依第三十四條第一項規定接受當事人授與訴訟實施權，以自己之名義提起損害賠償訴訟。

第 53 條

主管機關應訂定特定目的及個人資料類別，提供公務機關及非公務機關參考使用。

第 53-1 條

1 對主管機關依本法所為之行政處分不服者，直接適用行政訴訟程序。

2 於第五十一條之一第一項、第二項公告範圍內之非公務機關，對中央目的事業主管機關或直轄市、縣（市）政府依本法所為之行政處分不服者，向主管機關提起訴願。但行政處分係由中央行政機關組織基準法所定之獨立機關所為者，直接適用行政訴訟程序。

3 對本法中華民國一百十四年十月十七日修正之條文施行前依本法所為之行政處分不服，於修正施行後提起訴願者，應向主管機關為之。

4 本法中華民國一百十四年十月十七日修正之條文施行前已受理尚未終結之訴願事件，於修正施行後仍由原受理訴願機關依訴願法規定終結之。

第 54 條

1 本法中華民國九十九年五月二十六日修正公布之條文施行前，非由當事人提供之個人資料，於本法一百零四年十二月十五日修正之條文施行後為處理或利用者，應於處理或利用前，依第九條規定向當事人告知。

2 前項之告知，得於本法中華民國一百零四年十二月十五日修正之條文施行後首次利用時併同為之。

3 未依前二項規定告知而利用者，以違反第九條規定論處。

第 55 條

本法施行細則，由主管機關定之。

第 56 條

1 本法施行日期，由行政院定之。

2 本法中華民國九十九年五月二十六日修正公布之現行條文第十九條至第二十二條、第四十三條之刪除及一百十二年五月十六日修正之第四十八條，自公布日施行。

三、個人資料保護法施行細則

修正日期：民國 105 年 03 月 02 日

第 1 條

本細則依個人資料保護法（以下簡稱本法）第五十五條規定訂定之。

第 2 條

本法所稱個人，指現生存之自然人。

第 3 條

本法第二條第一款所稱得以間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。

第 4 條

1 本法第二條第一款所稱病歷之個人資料，指醫療法第六十七條第二項所列之各款資料。

2 本法第二條第一款所稱醫療之個人資料，指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。

3 本法第二條第一款所稱基因之個人資料，指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。

4 本法第二條第一款所稱性生活之個人資料，指性取向或性慣行之個人資料。

5 本法第二條第一款所稱健康檢查之個人資料，指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。

6 本法第二條第一款所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

第 5 條

本法第二條第二款所定個人資料檔案，包括備份檔案。

第 6 條

1 本法第二條第四款所稱刪除，指使已儲存之個人資料自個人資料檔案中消失。

2 本法第二條第四款所稱內部傳送，指公務機關或非公務機關本身內部之資料傳送。

第 7 條

受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。

第 8 條

1 委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。

2 前項監督至少應包含下列事項：

一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

二、受託者就第十二條第二項採取之措施。

三、有複委託者，其約定之受託者。

四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。

五、委託機關如對受託者有保留指示者，其保留指示之事項。

六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

3 第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。

4 受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。

第 9 條

本法第六條第一項但書第一款、第八條第二項第一款、第十六條但書第一款、第十九條第一項第一款、第二十條第一項但書第一款所稱法律，指法律或法律具體明確授權之法規命令。

第 10 條

本法第六條第一項但書第二款及第五款、第八條第二項第二款及第三款、第十條但書第二款、第十五條第一款、第十六條所稱法定職務，指於下列法規中所定公務機關之職務：

一、法律、法律授權之命令。

二、自治條例。

三、法律或自治條例授權之自治規則。

四、法律或中央法規授權之委辦規則。

第 11 條

本法第六條第一項但書第二款及第五款、第八條第二項第二款所稱法定義務，指非公務機關依法律或法律具體明確授權之法規命令所定之義務。

第 12 條

1 本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。

2 前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

一、配置管理之人員及相當資源。

二、界定個人資料之範圍。

三、個人資料之風險評估及管理機制。

四、事故之預防、通報及應變機制。

五、個人資料蒐集、處理及利用之內部管理程序。

六、資料安全管理及人員管理。

七、認知宣導及教育訓練。

八、設備安全管理。

九、資料安全稽核機制。

十、使用紀錄、軌跡資料及證據保存。

十一、個人資料安全維護之整體持續改善。

第 13 條

1 本法第六條第一項但書第三款、第九條第二項第二款、第十九條第一項第三款所稱當事人自行公開之個人資料，指當事人自行對不特定人或特定多數人揭露其個人資料。

2 本法第六條第一項但書第三款、第九條第二項第二款、第十九條第一項第三款所稱已合法公開之個人資料，指依法律或法律具體明確授權之法規命令所公示、公告或以其他合法方式公開之個人資料。

第 14 條

本法第六條第一項但書第六款、第十一條第二項及第三項但書所定當事人書面同意之方式，依電子簽章法之規定，得以電子文件為之。

第 15 條

本法第七條第二項所定單獨所為之意思表示，如係與其他意思表示於同一書面為之者，蒐集者應於適當位置使當事人得以知悉其內容並確認同意。

第 16 條

依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、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。

第 17 條

本法第六條第一項但書第四款、第九條第二項第四款、第十六條但書第五款、第十九條第一項第四款及第二十條第一項但書第五款所稱無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。

第 18 條

本法第十條但書第三款所稱妨害第三人之重大利益，指有害於第三人個人之生命、身體、自由、財產或其他重大利益。

第 19 條

當事人依本法第十一條第一項規定向公務機關或非公務機關請求更正或補充其個人資料時，應為適當之釋明。

第 20 條

本法第十一條第三項所稱特定目的消失，指下列各款情形之一：

一、公務機關經裁撤或改組而無承受業務機關。

二、非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符。

三、特定目的已達成而無繼續處理或利用之必要。

四、其他事由足認該特定目的已無法達成或不存在。

第 21 條

有下列各款情形之一者，屬於本法第十一條第三項但書所定因執行職務或業務所必須：

一、有法令規定或契約約定之保存期限。

二、有理由足認刪除將侵害當事人值得保護之利益。

三、其他不能刪除之正當事由。

第 22 條

1 本法第十二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。

第 23 條

1 公務機關依本法第十七條規定為公開，應於建立個人資料檔案後一個月內為之；變更時，亦同。公開方式應予以特定，並避免任意變更。

2 本法第十七條所稱其他適當方式，指利用政府公報、新聞紙、雜誌、電子報或其他可供公眾查閱之方式為公開。

第 24 條

公務機關保有個人資料檔案者，應訂定個人資料安全維護規定。

第 25 條

1 本法第十八條所稱專人，指具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員。

2 公務機關為使專人具有辦理安全維護事項之能力，應辦理或使專人接受相關專業之教育訓練。

第 26 條

本法第十九條第一項第二款所定契約或類似契約之關係，不以本法修正施行後成立者為限。

第 27 條

1 本法第十九條第一項第二款所定契約關係，包括本約，及非公務機關與當事人間為履行該契約，所涉及必要第三人之接觸、磋商或聯繫行為及給付或向其為給付之行為。

2 本法第十九條第一項第二款所稱類似契約之關係，指下列情形之一者：

一、非公務機關與當事人間於契約成立前，為準備或商議訂立契約或為交易之目的，所進行之接觸或磋商行為。

二、契約因無效、撤銷、解除、終止而消滅或履行完成時，非公務機關與當事人為行使權利、履行義務，或確保個人資料完整性之目的所為之連繫行為。

第 28 條

本法第十九條第一項第七款所稱一般可得之來源，指透過大眾傳播、網際網路、新聞、雜誌、政府公報及其他一般人可得知悉或接觸而取得個人資料之管道。

第 29 條

依本法第二十二條規定實施檢查時，應注意保守秘密及被檢查者之名譽。

第 30 條

1 依本法第二十二條第二項規定，扣留或複製得沒入或可為證據之個人資料或其檔案時，應掣給收據，載明其名稱、數量、所有人、地點及時間。

2 依本法第二十二條第一項及第二項規定實施檢查後，應作成紀錄。

3 前項紀錄當場作成者，應使被檢查者閱覽及簽名，並即將副本交付被檢查者；其拒絕簽名者，應記明其事由。

4 紀錄於事後作成者，應送達被檢查者，並告知得於一定期限內陳述意見。

第 31 條

本法第五十二條第一項所稱之公益團體，指依民法或其他法律設立並具備個人資料保護專業能力之公益社團法人、財團法人及行政法人。

第 32 條

本法修正施行前已蒐集或處理由當事人提供之個人資料，於修正施行後，得繼續為處理及特定目的內之利用；其為特定目的外之利用者，應依本法修正施行後之規定為之。

第 33 條

本細則施行日期，由法務部定之。

四、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

公發布日：民國 106 年 11 月 22 日
修正日期：民國 110 年 12 月 08 日

第一條

本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。

第二條

本辦法所稱主管機關：在中央為教育部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

第三條

本辦法用詞，定義如下：

一、個人資料管理人（以下簡稱管理人）：指由校長、園長擔任或指定，負責督導個人資料檔案安全維護計畫（以下簡稱安全維護計畫）訂定及執行之人員。

二、個人資料稽核人員（以下簡稱稽核人員）：指由校長、園長指定，負責評核安全維護計畫執行情形及成效之人員。

三、所屬人員：指私立高級中等以下學校（以下簡稱學校）及幼兒園執行業務之過程，必須接觸個人資料之人員，包括定期或不定期契約人員及派遣員工。

前項第三款所定幼兒園，包括依幼兒教育及照顧法對幼兒提供教育及照顧服務之幼兒園、社區互助教保服務中心及部落互助教保服務中心。

第一項第一款管理人與第二款稽核人員不得為同一人。

第四條

學校及幼兒園應依本辦法規定訂定安全維護計畫，落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

學校及幼兒園訂定安全維護計畫時，應視其經營型態、規模、保有個人資料之性質及數量等事項，訂定適當之安全維護措施。

前項計畫，應包括業務終止後，個人資料處理方法等相關個人資料管理事項。

第五條

學校及幼兒園得指定或設管理單位，或指定專人，負責個人資料檔案安全維護；其任務如下：

一、訂定及執行安全維護計畫。

二、定期就個人資料檔案安全維護管理情形，向管理人提出書面報告。

三、依據稽核人員就安全維護計畫執行之評核，於進行檢討改進後，向管理人及稽核人員提出書面報告。

第六條

學校及幼兒園應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。

學校及幼兒園經定期檢視，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置。

第七條

學校及幼兒園於蒐集個人資料時，應檢視是否符合前條第一項所定之類別及範圍。

學校及幼兒園於傳輸個人資料時，應採取必要保護措施，避免洩漏。

第八條

學校及幼兒園應依已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能產生之風險，訂定適當之管控措施。

第九條

學校及幼兒園於蒐集個人資料時，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。

第十條

學校及幼兒園依本法第二十條第一項規定利用個人資料為宣傳、推廣或行銷時，應明確告知當事人學校及幼兒園立案名稱及個人資料來源。

學校及幼兒園於首次利用個人資料為宣傳、推廣或行銷時，應提供當事人或其法定代理人表示拒絕接受宣傳、推廣或行銷之方式，並支付所需費用；當事人或其法定代理人表示拒絕宣傳、推廣或行銷後，應立即停止利用其個人資料宣傳、推廣或行銷，並周知所屬人員。

第十一條

學校及幼兒園委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定對受託者為適當之監督，並明確約定相關監督事項及方式。

第十二條

學校及幼兒園於當事人或其法定代理人行使本法第三條規定之權利時，得採取下列方式辦理：

一、提供聯絡窗口及聯絡方式。

二、確認是否為資料當事人之本人或其法定代理人，或經其委託。

三、有本法第十條但書、第十一條第二項但書或第三項但書得拒絕當事人或其法定代理人行使權利之事由，一併附理由通知當事人或其法定代理人。

四、告知是否酌收必要成本費用及其收費基準，並遵守本法第十三條處理期限規定。

第十三條

學校及幼兒園應訂定應變機制，在發生個人資料被竊取、洩漏、竄改或其他侵害事故時，迅速處理，以保護當事人之權益。

前項應變機制，應包括下列事項：

一、採取適當之措施，控制事故對當事人造成之損害。

二、查明事故發生原因及損害狀況，並以適當方式通知當事人或其法定代理人。

三、研議改進措施，避免事故再度發生。

學校及幼兒園應自第一項事故發現時起七十二小時內，填具個人資料侵害事故通報與紀錄表（如附件），通報主管機關；通報之主管機關為直轄市、縣（市）政府者，並應副知教育部，未依時限內通報者，應附理由說明；並自處理結束之日起一個月內，將處理方式及結果，報主管機關備查。依規定通報後，主管機關得派員檢查，受檢者不得規避、妨礙或拒絕，主管機關並得依本法第二十二條至第二十五條規定，為適當之監督管理措施。

第十四條

學校及幼兒園對所保有之個人資料檔案，應設置必要之安全設備及採取必要之防護措施。

前項安全設備或防護措施，應包括下列事項：

一、紙本資料檔案之安全保護設施及管理程序。

二、電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。

三、訂定紙本資料之銷毀程序；電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。

第十四條之一

學校及幼兒園提供電子商務服務系統或本法第六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。

第十四條之二

學校及幼兒園進行個人資料國際傳輸前，應檢視有無主管機關依本法第二十一條規定為國際傳輸之限制，並告知學校學生、幼兒園幼兒、學生及幼兒之法定代理人及教職員其個人資料所欲國際傳輸之區域，同時對資料接收方為下列事項之監督：

一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。

二、當事人行使本法第三條所定權利之相關事項。

第十五條

學校及幼兒園為確實保護個人資料之安全，應對其所屬人員採取下列措施：

一、依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之適當性及必要性。

二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。

三、要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。

四、所屬人員離職時取消其識別碼，並要求將執行業務所持有之個人資料（包括紙本及儲存媒介物）辦理交接，不得攜離使用，並應簽訂保密切結書。

第十六條

學校及幼兒園應訂定個人資料檔案安全稽核機制，定期或不定期檢查安全維護計畫所定相關事項是否落實執行，並將檢查結果向管理人提出報告。

執行前項稽核之人員與第五條指定之專責人員，不得為同一人。

學校應將第一項稽核機制，納入其內部控制制度訂定作業程序、內部控制點及稽核作業規範（內部管理及稽核作業規章）規定辦理。

第十七條

學校及幼兒園執行安全維護計畫各項程序及措施，至少應保存下列紀錄：

一、個人資料之交付及傳輸。

二、個人資料之維護、修正、刪除、銷毀及轉移。

三、提供當事人或其法定代理人行使之權利。

四、存取個人資料系統之紀錄。

五、備份及還原之測試。

六、所屬人員權限之異動。

七、所屬人員違反權限之行為。

八、因應事故發生所採取之措施。

九、定期檢查處理個人資料之資訊系統。

十、教育訓練。

十一、安全維護計畫稽核及改善措施之執行。

十二、業務終止後處理紀錄。

第十八條

學校及幼兒園對於個人資料之蒐集、處理及利用，應符合本法第十九條及第二十條規定，並應定期或不定期對其所屬人員，施以教育訓練或認知宣導，使其明瞭個人資料保護相關法令規定、責任範圍、作業程序及應遵守之相關措施。

第十九條

學校及幼兒園業務終止後，其保有之個人資料之處理方式及留存紀錄如下：

一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

前項紀錄應至少留存五年。

第二十條

學校及幼兒園應參酌安全維護計畫執行狀況、技術發展、法令依據修正等因素，檢視所定安全維護

計畫是否合宜，必要時應予以修正。

第二十一條

本辦法自發布日施行。

第十三條附件

<table>
<tr><td colspan="3">個人資料侵害事故通報與紀錄表</td></tr>
<tr><td>非公務機關名稱
通報機關</td><td colspan="2">通報時間： 年 月 日 時 分
通報人： 簽名（核章）
職稱：
電話：
E-mail：
地址：</td></tr>
<tr><td>事故發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">事故發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td>個資侵害之總筆數（大約）</td></tr>
<tr><td>□一般個資 筆
□特種個資 筆</td></tr>
<tr><td>發生原因及事故摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個資侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個資外洩後 72 小時通報</td><td colspan="2">□是 □否，理由：</td></tr>
</table>

五、行政院及所屬各機關落實個人資料保護聯繫作業要點

110 年8 月11 日行政院院授發協字第 1102001106 號函訂定
112 年5 月29 日行政院院授發協字第 1122001174 號函修正
112 年8 月15 日行政院院授發協字第 1122001832 號函修正
112 年11 月28 日行政院院授發協字第 1122002626 號函修正
113 年5 月15 日行政院院授個資籌查字第 1130500182 號函修正
114 年1 月7 日行政院院授個資籌查字第 1140500004 號函修正

一、 行政院(以下簡稱本院)為防止非公務機關違反個人資料檔案安全維護義務(以下簡稱個資安維案件)，加強所屬中央目的事業主管機關(以下簡稱中央目的事業主管機關)對非公務機關個人資料保護之監管，以落實非公務機關個人資料檔案之安全維護， 特訂定本要點。

二、 本院得召開行政機關落實個人資料保護執行聯繫會議(以下簡稱聯繫會議)，執行下列任務：

(一)研議中央目的事業主管機關依個人資料保護法(以下簡稱個資法)第二十七條第三項所定個人資料檔案安全維護計畫或業務終止後個人資料處理方法之標準等相關事項之辦法（以下簡稱安全維護辦法）應予規定之相關事項。

(二)統籌個資安維案件之監督通報。

(三)就重大矚目之個資安維案件管轄權爭議，確認管轄機關，及該案件行政調查之協調。

(四)其他個人資料侵害案件之跨部會協調聯繫事務。

本要點所定重大矚目之個資安維案件，其範圍如下：

(一)本院、立法院或監察院關注之個資安維案件。

(二)經媒體顯著披露之個資安維案件，例如經平面媒體全國性版面報導、電子媒體專題討論。

三、 聯繫會議由本院院長指派政務委員一人擔任召集人；協同召集人一人至三人，由本院資訊長及本院院長指派之政務委員擔任。

聯繫會議由召集人主持；協同召集人視議題參與，並為協同主持人。召集人因故未能出席時，由召集人指定協同召集人一人代理之。

聯繫會議得視個資安維案件或其他個人資料侵害案件議題之情形，不定期召開，並得視議題需要，邀請中央行政機關、直轄市、縣(市)政府等相關機關代表或專家、學者出席。

聯繫會議之幕僚作業，由個人資料保護委員會籌備處(以下簡稱個資會籌備處)辦理。

四、 中央目的事業主管機關每年應擬定依個資法第二十二條第一項規定辦理之行政檢查計畫並立即執行之。

前項行政檢查計畫應於每年一月底前送個資會籌備處彙整， 再提聯繫會議報告。

中央目的事業主管機關應組成個資行政檢查小組，辦理第一項之年度行政檢查，及因應、處理個資安維案件；其成員得包括具有法律、資訊專業之機關資深人員及外部專家。

中央目的事業主管機關應評估所管非公務機關發生個資安維案件之風險，將其中具有高風險者優先列入第一項之年度行政檢查對象。

前項所定高風險者，得參考第六點各款情形及發生個資安維案件之次數等因素綜合考量。

五、 安全維護辦法應至少就下列事項予以規定：

(一)中央目的事業主管機關就所主管之非公務機關使用資通訊系統蒐集、處理或利用個人資料，而有下列情形之一者，應加強管理：

1. 保有消費者交易、使用商品或接受服務等過程之一般或特種個人資料，且符合中央目的事業主管機關所定應加強管理之條件。
2. 前目以外經中央目的事業主管機關認定應加強管理。

(二)就前款應加強管理者之規定，應至少包括下列資料安全管理措施：

1. 使用者身分確認及保護機制。
2. 個人資料顯示之隱碼機制。
3. 網際網路傳輸之安全加密機制。
4. 個人資料檔案與資料庫之存取控制及保護監控措施。
5. 防止外部網路入侵對策。
6. 非法或異常使用行為之監控及因應機制。

(三)非公務機關發生個資安維案件時，依安全維護辦法應通報之對象、時點、應通報事項、後續行政調查等事項；其通報地方目的事業主管機關者，並應副知中央目的事業主管機關。

中央目的事業主管機關訂定或修正發布安全維護辦法，應函知個資會籌備處。

六、 中央目的事業主管機關應就尚未訂定安全維護辦法之非公務機關，綜合考量下列情形，定期檢討訂定該辦法之必要性；其應訂定安全維護辦法者，並應於該辦法就前點第一項所定事項予以規定：

(一)非公務機關之規模、特性。

(二)保有個人資料之數量或性質。

(三)與民眾日常生活關係密切程度。

(四)個資安維案件衝擊層面廣泛程度。

(五)個資安維案件將造成當事人身心危害、社會地位受損或衍生財務危機等重大影響。

(六)個人資料存取環境。

(七)個人資料傳輸之工具及方法。

(八)國際傳輸之頻率。

七、 中央目的事業主管機關接獲非公務機關通報或副知，或非因通報或副知而自行知悉個資安維案件，經確認屬該機關管轄後，應於接獲通報、副知或知悉時起七十二小時內，填列監督通報紀錄表(如附件一)，通報個資會籌備處。但個資安維案件屬重大矚目者，依第八點規定辦理。

中央目的事業主管機關就前項本文之個資安維案件，應於接獲通報、副知或知悉時起三個月內調查完成並結案；必要時，得經資通安全長或其授權人員同意後，延期三個月，並即時通報個資會籌備處。該案件之後續行政措施及處置情形，應按季通報個資會籌備處。

八、 前點第一項但書之個資安維案件屬重大矚目者，中央目的事業主管機關經確認屬該機關管轄後，應於接獲通報、副知或知悉時起二十四小時內，填列前點第一項本文所定監督通報紀錄表，通報個資會籌備處及數位發展部。

中央目的事業主管機關針對前項重大矚目之個資安維案件及依前點第一項本文規定通報後改列為重大矚目案件者，應於接獲通報、副知或知悉時起三日內進行行政調查，十日內完成調查報告，報告完成後應送個資會籌備處及數位發展部；必要時個資會籌備處得報請本院指定之政務委員，原則於二週內召開會議，聽取行政調查辦理情形。

中央目的事業主管機關得偕同數位發展部辦理前項之行政調查。

中央目的事業主管機關應就重大矚目之個資安維案件後續行政措施及處置情形，即時通報個資會籌備處及數位發展部。

九、 中央目的事業主管機關得依個資法第二十二條至第二十六條規定，對該非公務機關為適當之監督管理措施。

中央目的事業主管機關就個資安維案件辦理行政調查，得於必要時請求警察機關或法務部調查局提供協助。

中央目的事業主管機關就個資安維案件，經查明違反個資法之規定者，應視具體調查結果，依個資法第四十七條至第五十條規定辦理；並得依情節輕重及個資安維案件造成之影響，依個資法第二十五條規定，為下列處分：

(一)禁止蒐集、處理或利用個人資料。

(二)命令刪除經處理之個人資料檔案。

(三)沒入或命銷燬違法蒐集之個人資料。

(四)公布非公務機關之違法情形，及其姓名或名稱與負責人。

中央目的事業主管機關對於非公務機關有個資法第四十八條第二項或第三項情形者，應處罰鍰，並令其限期改正，屆期未改正者，按次處罰。

十、 中央目的事業主管機關對個資安維案件之行政調查流程，除重大矚目之個資安維案件依第十一點規定確認管轄機關者外，其餘行政調查程序，依附件二流程圖辦理。

十一、個資會籌備處對於重大矚目之個資安維案件管轄權爭議，應儘速認定管轄機關，並得視需要召開跨部會協調會議。

前項被認定管轄機關如有異議，應於認定管轄文到三日內， 敘明具體理由送個資會籌備處，提請聯繫會議確認管轄機關。

聯繫會議應邀集相關機關確認前項管轄機關，必要時得邀請專家、學者出席。

經聯繫會議確認為管轄機關之中央目的事業主管機關，應於個資會籌備處指定時間內，依第八點第一項規定填列監督通報紀錄表。

十二、中央目的事業主管機關對重大矚目之個資安維案件辦理行政調查前，已依行政程序法第十九條規定向其他機關請求行政協助遭拒絕者，於規劃跨部會任務分工後，函送個資會籌備處， 提請聯繫會議進行協調。

就前項行政調查之協調，聯繫會議應邀集相關機關討論， 經請求協助機關與被請求機關說明後，評估有提供行政協助之必要者，被請求機關即應配合執行。

十三、數位發展部資通安全署、內政部警政署及法務部調查局，應適時向個資會籌備處分享個資安維案件情報。

個資會籌備處接獲前項情報後，應通知中央目的事業主管機關為必要之處理。

□警政署來函：____年____月___日____字_____號函
□非公務機關自行通報：日期____年____月___日
□其他，請敘明：_____

附件一、監督通報紀錄表

通報作業(註1)	
非公務機關名稱 通報機關(註2)	首次通報時間：　年　月　日　時　分 中央目的事業主管機關承辦人(註2)： 職稱： 電話： Email：
案件發生時間(註 3)	
案件發生種類	□竊取 □洩漏 □竄改 □毀損 □滅失 □其他侵害事故
發生原因及案件摘要	
損害狀況	個資侵害之總筆數(大約)　　筆 □一般個資　　筆 □特種個資　　筆 是否造成個資當事人財產損害： □是，財損金額 □否 □其他損害情形，說明：
擬採取之因應措施	
依個人資料保護法第 12 條及同法施行細則第 22 條，擬採通知當事人之時間及方式	
個資安維案件種類	□屬重大矚目之個資安維案件 □屬一般個資安維案件

若屬一般個資安維案件，是否於接獲通報、副知或自行知悉個資安維案件時起 72 小時內通報	□是　□否，說明：
若屬重大矚目之個資安維案件，是否於接獲通報、副知或自行知悉個資安維案件時起 24 小時內通報	□是　□否，說明：
後續行政措施及處置作業(註4)	
若首次通報為一般個資安維案件，是否改列為重大矚目之個資安維案件	□是，說明：　□否，說明：
主管機關是否有進行行政調查(含複查)	□是，說明：　□否，說明：
一般個資安維案件之行政調查是否依期限完成(註 5)	□於接獲通報、副知或知悉發生個資安維案件時起 3 個月內完成 □已裁罰，同時命　年　月　日前完成改正 □經調查判斷未違反個資法，無須裁罰 □未於接獲通報、副知或知悉個資安維案件時起 3 個月內完成，經資通安全長或 其授權人員同意，延期 3 個月。**請說明(簡要說明延期理由)**： □未於前開期限內完成行政調查。**請說明(簡要說明理由)**：
主管機關就個資安維案件判斷是否違反個資法	□是，說明：　□否，說明：
主管機關就個資安維案件之後續處置	
建議解除列管時間	□解除列管，時間　年　月　日 □不解除列管

註 1：該欄各項資訊係源自非公務機關之個資安維案件通報內容，各欄位資訊若尚未明確，得先填寫「不明」，並得於後續處置作業之通報更新補充。

註 2：倘接續通報時通報機關或承辦人異動，請自行增列填寫異動後之機關或人員資料。

註 3：案件發生時間如填寫「不明」者，請接續註明查知該非公務機關知悉個資安維案件之時間。

註 4：首次通報時，不需先填寫後續行政措施及處置作業之欄位。

註5：行政調查期限經資通安全長或其授權人員同意延期 3 個月，應即時通報個資會籌備處。

附件二、中央目的事業主管機關對個資安維案件之行政調查流程圖