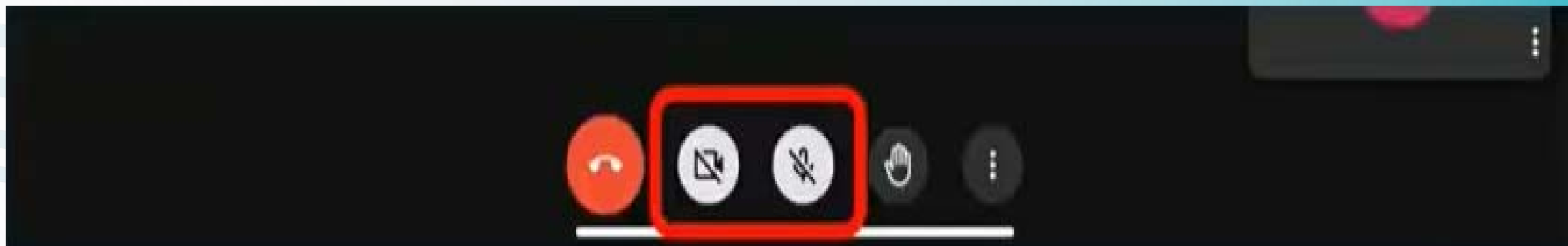


會議準備中

請參與人員關閉
視訊鏡頭及麥克風





顧問諮詢

BCCS 漢昕科技

資安整備專家



僑光科技大學

個人資料保護教育訓練課程

梁秋玲

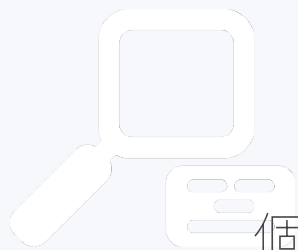
漢昕科技

2025-08-08 (Fri)





目錄 Contents



個人資料保護法

個人資料保護法
沿革與重點

個人資料識別

認識與識別個人資料

1

2

個資保護要求

私立學校個人資料保
護要求與規範

3

個資洩漏案例

個人資料洩漏案例
分享與說明

4

個資查檢表說明

個人資料查檢表說明
與問答

5



個人資料識別

認識與識別個人資料

個人資料定義與範圍

規範/標準	個人資料定義與範圍
個人資料保護法	<ul style="list-style-type: none">● 與自然人姓名、出生年月日、身分證字號、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、社會活動等及「其他得以直接或間接方式識別該個人」之資料● 特種個資（敏感性個資）：病歷、醫療、基因、性生活、健康檢查、犯罪前科等
歐盟 GDPR	<ul style="list-style-type: none">● 凡是「關於已識別或可識別之自然人」的任何資訊皆屬，舉凡姓名、身分證號、位置資料、網路識別碼（IP、Cookie）、電子郵件、裝置ID、基因、生物特徵、醫療資訊等均涵蓋在內。強調只要該資料可單獨或結合其他資訊辨識個人，不論是否傳統資料型態皆屬（包括線上紀錄、行為分析等）● 特種個資包括種族、政治、宗教、工會、基因、生物特徵、健康、性生活與性取向等。
ISO 27701	<ul style="list-style-type: none">● 「個人可識別資訊」（PII, Personally Identifiable Information）為核心，參照ISO 27001與27002，範圍包括所有可直接或間接識別特定個人的資訊，包含傳統資料與數位資料（如網路識別碼、裝置資訊、Cookie、IP、行為資料、生物特徵、基因、醫療等）
BS 10012	<ul style="list-style-type: none">● 所有可指向、識別個人的資訊，含姓名、出生年月日、身分證號、地址、電子郵件、職業、財務狀況、醫療、家庭等。針對高風險（高敏感）個資如醫療、基因、性生活等

(個資法) 個人資料 定義

與現活著的自然人相關，且能據此識別出是特定個人的資料

個人資料

特種個資

➤ 個人資料：＜個資法第2條＞

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。

➤ 個人：＜個資法施行細則第1條＞

本法所稱個人，指現生存之自然人。

➤ 間接方式識別：＜個資法施行細則第3條＞

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。

常見的個人資料

◆ 可以直接識別出某人的資料

- 透過資料本身，可以直接連結到某一個特定的人
- 例如：姓名、身分證號碼、照片、指紋等

◆ 可以和其他資訊結合，間接識別出某人的資料

- 除了資料本身以外，還需要將資料跟其他的資訊互相對照、組合或連結，才能辨識出某一個特定的人
- 例如：地址、電話、車牌號碼、照片、出生年月日、特徵、職業、婚姻、財務狀況等

個人資料定義之實務見解

◆ 拍攝他人照片（臺灣高等法院刑事判決109年度上訴字第1020號）

- 按自然人之臉部容貌、聲音，均為足以具體識別其身分之特徵，...，而為該法所規範之保護客體。從而拍攝他人之照片，縱該照片並未註記任何有關被拍攝者之姓名、身分證字號、護照號碼、指紋等資料，然由照片所顯示之臉部容貌，已足以區別與其他人容貌外型之不同而可資識別其個人者，該照片即屬個人資料保護法所規範之個人資料，非必以據該照片即得以直接知悉該照片上之人為何姓名、為何具體之特定人為必要。

◆ 國民身分證背面（臺灣高等法院臺中分院刑事判決109年度上訴字第2613號）

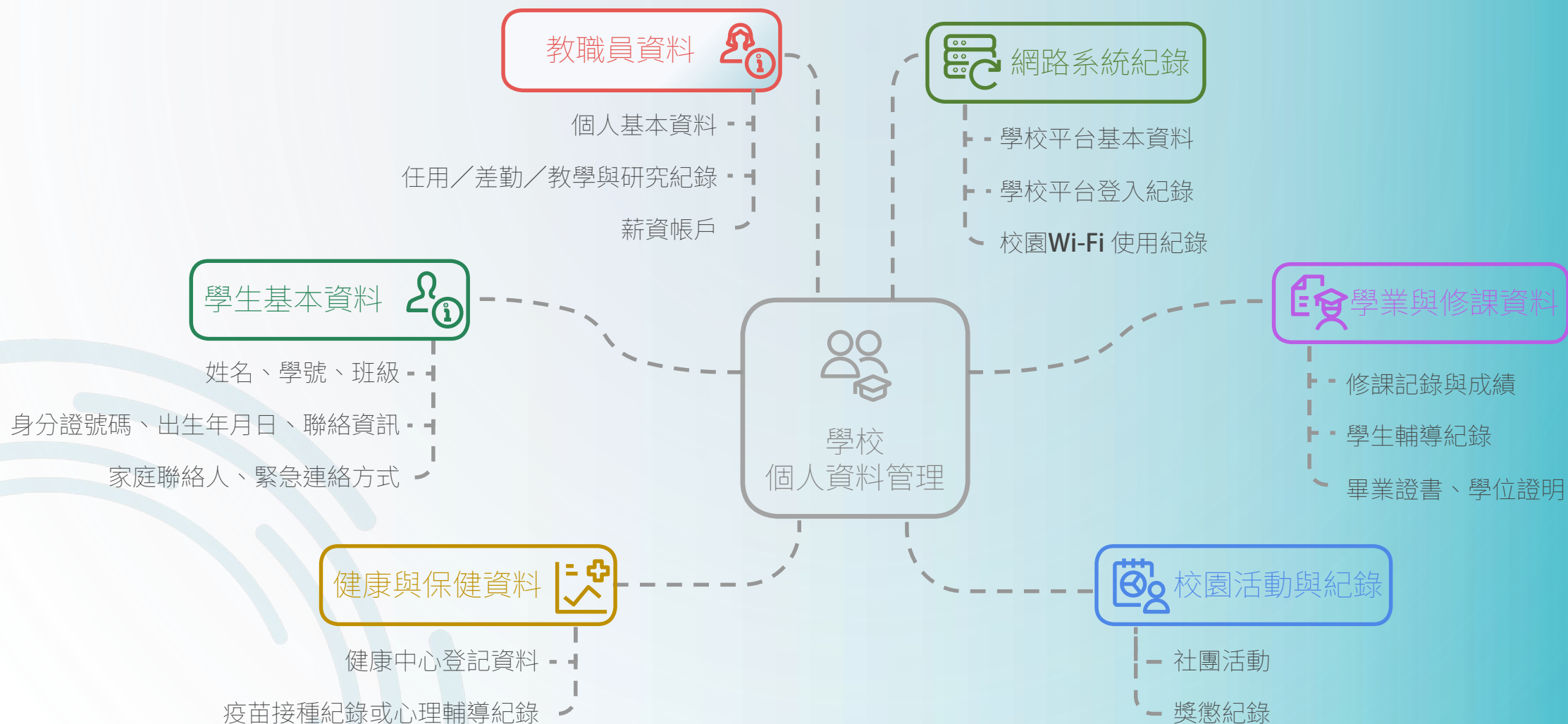
- 國民身分證背面照片，其上雖無姓名、性別、身分證號、電話號等個人資料，然其上載有告訴人父、母、役別、出生地、住址等個人資料，被告同時留言「....她先生叫張OO」等字句，仍可輕易得知係告訴人本人，自屬於「個人資料」

個人資料—特種資料

◆ 個人資料保護法第6條 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。

- 病歷：指醫療法第67條第二項所列之各款資料
- 醫療：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。
- 基因：指由人體一段去氧核糖核酸構成，為人體控制特定功能之遺傳單位訊息。
- 性生活：指性取向或性慣行之個人資料。
- 健康檢查：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
- 犯罪前科：指經緩起訴、職權不起訴或法院判決有罪確定、執行紀錄

學校常蒐集的個人資料項目





個人資料保護法

個人資料保護法沿革與重點

個人資料保護法立法及修法歷程

2010.04.27	2010.05.26	2012.09.26	2012.10.01	2015.12.30	2016.03.15	2023.05.16
個資法三讀通過	總統令公布個資法	個資法施行細則正式公告	個資法施行	個資法修正	個資法修正條文暨細則施行	個資法修正三讀通過
個人資料保護法全面施行						



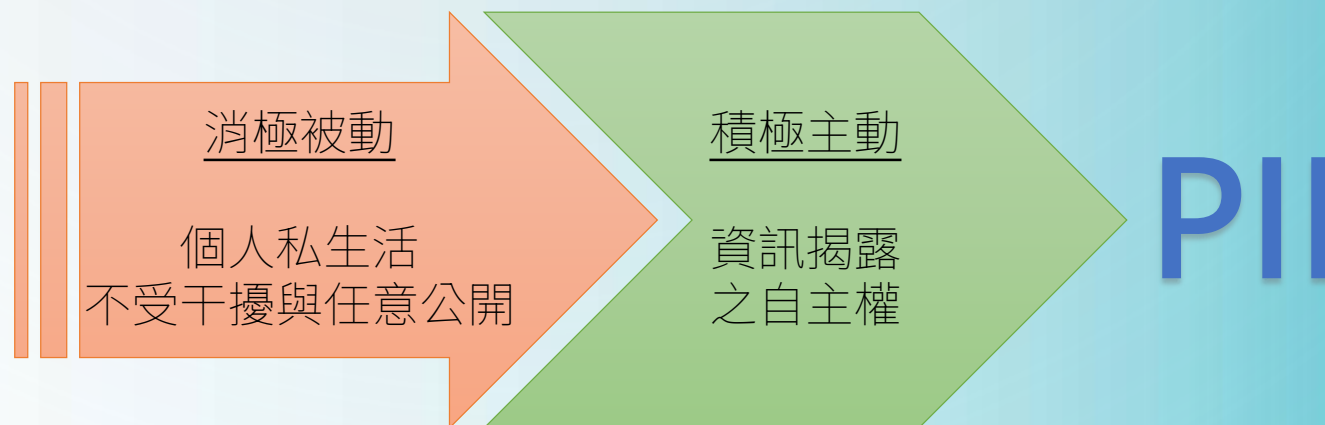
個人資料保護法架構

章節	章節名稱	說明
第一章	總則	個資法之共通義務及原則
第二章	公務機關對個人資料之蒐集、處理及利用	蒐集、處理利用個資時應盡之義務
第三章	非公務機關對個人資料之蒐集、處理及利用	
第四章	損害賠償及團體訴訟	違法時所負刑事、民事、行政責任
第五章	罰則	
第六章	附則	其他相關規定

資訊隱私權的概念

◆ 個人自主控制個人資料之權利

- 個人有決定是否**揭露其個人資料**、及在**何種範圍內**、於**何時**、以**何種方式**、**向何人揭露之決定權**
- 個人對其個人資料之使用有**知悉與控制權**及**資料記載錯誤之更正權**(釋字第603號)
- 個人縱於公共場域中，亦應享有依社會通念**得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域**及**個人資料自主**，而受法律所保護。惟在公共場域中個人所得主張不受此等侵擾之自由，以得合理期待於他人者為限(釋字第689號)





隱私權政策相關原則

APEC 隱私權保護綱領

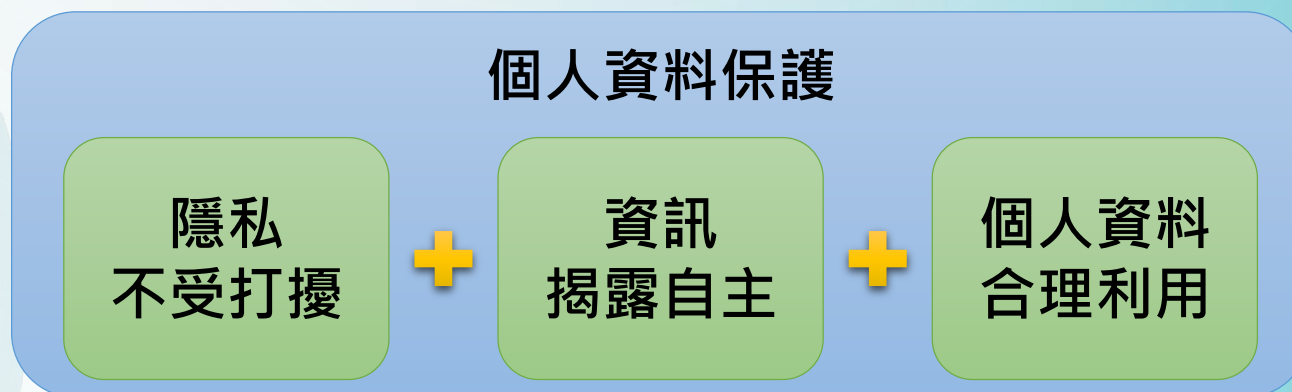
- ◆ 預防損害原則
- ◆ 告知原則
- ◆ 蒐集限制原則
- ◆ 個人資料利用原則
- ◆ 當事人自主原則
- ◆ 個人資料完整性原則
- ◆ 安全管理原則
- ◆ 查閱及更正
- ◆ 責任原則

OECD 個人資料保護八大原則

- ◆ 限制蒐集原則
- ◆ 資訊內容完整正確原則
- ◆ 目的明確化原則
- ◆ 限制利用原則
- ◆ 安全保護原則
- ◆ 公開原則
- ◆ 個人參加原則
- ◆ 責任原則

個人資料保護法立法目的

- ◆ 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
 - 避免人格權受侵害
 - 促進個人資料合理利用
 - 2018年7月個人資料保護業務，由法務部移交國家發展委員會辦理，國發會成立個人資料保護專案辦公室，並定位為法律主政機關
 - 行政院為籌設個人資料保護委員會，以落實資訊隱私權保障，並促進個人資料之合理利用，特設個人資料保護委員會籌備處，並於2023年12月5日正式成立，為中央三級機關



個人資料處理流程



個人資料保護法規範主體

◆ 公務機關

- 依法行使公權力之**中央**或**地方機關**
- 行政法人
- 公立學校 (法務部法律字第10200571790號函)

◆ 非公務機關

- 公務機關定義之外之**自然人**、**法人**或**其他團體**
- 全面適用，取消電腦處理個人資料保護法之行業別限
- 國營事業 (法務部法律字第0999027871號函) 、私

立學校 (法務部法律字第10200571790號函)

◆ 受委託處理個資者 (個人資料保護法第4條)

- 受規範主體委託蒐集、處理或利用個人資料者
- 於本法適用範圍內，視為委託機關

會議休息中

10:10 開始上課

如參與人員
有相關課程問題
歡迎開啟麥克風或留言區討論

如參與人員
尚未簽到
請在留言區留下
單位+姓名



個資保護要求

私立學校個人資料保護要求與規範

教育部對專科以上學校的個人資料保護要求

- ◆ 依『個人資料保護法』第27條第3項，教育部訂有『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』，公私立大學與專科院校皆須依規範執行

- 私立學校的個人資料安全維護計畫範圍廣泛，應涵蓋蒐集、處理、利用、保存、刪除等全流程，並針對人員管理、技術措施、事件通報、委外控管以及法定權益保障等面向制定完整的作業機制，落實教育部及個資法相關規定，以守護所有資料主體的權益和資訊安全

僑光科技大學個人資料安全保護基本措施 + 僑光科技大學個人資料保護管理辦法 + 僑光科技大學個人資料蒐集、處理、利用與安全管理程序書

專科以上學校的個人資料保護要求

依據『[資訊安全管理暨個人資料保護委員會設置辦法](#)』設置資訊安全管理暨個人資料保護委員會

1
安全維護計畫
的建立

2
明確組織責任
分工

3
資料類別與
目的管理

4
風險評估與控管

資料安全與
事故通報
5

委外處理與
國際傳輸管理
6

當事人權利
落實
7

教育宣導與
稽核控管
8

僑光科技大學個人資料保護作業要求，可參照『[僑光科技大學個人資料安全保護基本措施](#)』、『[僑光科技大學個人資料保護管理辦法](#)』、『[僑光科技大學個人資料蒐集、處理、利用與安全管理程序書](#)』

私立學校個人資料安全維護計畫範圍



0. 訂定個人資料檔案安全維護計畫

◆ 法源依據

1. 個人資料保護法 (第27條第2款中央目的事業主管機關得指定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。)
2. 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

◆ 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3條

1. 依私立學校法核准設立之私立專科以上學校 (以下簡稱學校) 及依學術研究機構設立辦法核准設立之私立學術研究機構 (以下簡稱機構) 應訂定個人資料檔案安全維護計畫 (以下簡稱安全維護計畫) ，**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。**
2. 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。**

1. 計畫適用對象與資料範圍

◆ 適用對象

- 在校學生、教職員工、外聘 / 約聘人員、志工 / 義工、校友等之個人資料

◆ 適用資料範圍

- 所有型態之個人資料檔案，如：紙本、電子、影像、聲音、網路等
- 校方自有、與第三方共用或委外管理的各類個人資料

◆ 如何識別個資？進行個資盤點，識別各類個資資料、儲存型態、擁有者等相關重要資訊

2. 管理機制與實施內容

◆ 組織制度建構

『[僑光科技大學資訊安全管理暨個人資料保護委員會設置辦法](#)』

- 須有明確的資料管理人、稽核負責人，不得由同一人兼任
- 設立專責管理單位，負責計畫執行與成效檢討

◆ 資料生命周期管理

『[僑光科技大學個人資料蒐集、處理、利用與安全管理程序書](#)』

- 從個人資料的蒐集、處理、利用到使用終止和銷毀，皆需納入控管
- 明定用途，取得資料前應完成告知義務 『[個資蒐集、處理及利用告知聲明](#)』
- 僅於達成特定目的範圍內，處理所需資料

◆ 檔案分類與盤點

- 須明確辨識所保存的各類資料檔案，定期清查更新
- 檔案分類管理，標註資料敏感等級

3. 風險評估與安全控管

◆ 風險評估

- 對系統辦公流程、資訊設備、外包服務評估可能個資風險並實施防護措施
- 定期評估個資蒐集、處理、利用流程中之安全風險，並依評估結果調整管理措施

◆ 安全控管

- 存取控制與授權管理
 - 限定具業務需求人員存取個資，落實帳號密碼控管
 - 定期檢視授權名單及異動管理

➤ 系統安全管理措施

- 定期備份資料、系統安全更新
- 採用加密、入侵偵測等技術防護措施
- 紙本檔案儲存於加鎖空間，管理出入紀錄

➤ 資料銷毀與去識別化

- 定期檢視保存期限，逾期即依程序銷毀或去識別化
- 詳列實體與電子檔案銷毀流程

4. 事故通報與應變

◆ 通報機制

- 資料外洩或安全事件發生時
 - 24小時內內部通報
 - 72小時內主動通報主管機關

◆ 應變程序

- 明訂事故調查、損害控管及事後改進的處理流程
- 建立調查、補救、預防再發的事故處理流程，將法遵、風險控管與組織回饋緊密結合
- **完成事故處理**須於**一個月內**提交報告備查

5. 委外與第三方管理

- ◆ 委由第三方管理資料時，須有明確契約約定安全責任並監督執行
 - 定義資料委外流程、審查制度及安全責任
 - 與受託團隊簽訂合約，要求其符合相關法規及校內規範
- ◆ 定期查核委外單位或合作單位之安全維護措施
- ◆ 涉及國際傳輸時，檢查法定限制並告知當事人資料流向，監督資料接收方安全措施

6. 資料主體權利保障

◆ 明訂提供當事人查詢、更正、刪除與異議等行使方式與處理流程

- 設立聯絡窗口，保障查詢、更正、停止利用、刪除等權利

[『個人資料權利行使申請表』](#)

- 明確處理時程與結果告知程序

◆ 訂有資料使用、保存期限與刪除等標準作業程序

[『僑光科技大學個人資料蒐集、處理、利用與安全管理程序書』](#)

7. 教育訓練與宣導

- ◆ 定期對全校教職員生辦理個資保護教育訓練及防護宣導
- ◆ 保留培訓紀錄與成果，作為稽核和持續改進依據

8. 稽核檢查與追蹤改進

- ◆ 建立內部稽核制度，定期或不定期檢查計畫執行情形
 - 定期/不定期自我檢查、保存檢查紀錄與結果追蹤
 - 計畫修訂須經管理階層審核
- ◆ 對於缺失事項採取查核、回饋、改善與追蹤機制

9. 文件化與保存

- ◆ 全程規劃、執行政序、調查流程、教育訓練及稽核紀錄須保存於學校文件系統，確保可追溯性與稽核便利
- ◆ 各項資料文件保存年限及程序，紀錄保留需符合相關規範

20大專校院類檔案保存年限基準表

中華民國106年5月17日國家發展委員會檔案管理局
檔徵字第1060009095號函訂頒

大專校院類檔案保存年限基準適用於公立大專校院，包括大學校院、技職校院、空中大學、軍警校院及專科學校產生之檔案，範圍含括校務發展、教學事務、學生事務、研究發展、國際事務、師資培育、圖書館管理、資訊管理、體育事務、環境衛生及校園安全、進修推廣及教育、校史文物、公共關係及服務、性平教育及事務、軍警教育、法令規章等16項主題。至大專校院之人事、主計及行政類檔案之保存年限應依相關類別之檔案保存年限基準表判定。

『大專校院類檔案保存年限基準表』



個資洩漏案例

個人資料洩漏案例分享與說明

學校個資組合洩漏的判斷標準

◆ 直接識別個資，單一資料即可識別特定個人

- 姓名（在特定範圍內，如班級、系所）
- 身份證字號
- 學號（在特定學校內）
- 護照號碼
- 指紋、照片等生物特徵

◆ 間接識別個資組合：須與其他資料結合才能識別特定個人

- 高風險組合（極易識別）
 - 學號 + 姓名：校內最常見組合

- 姓名 + 出生年月日：結合性別更易識別
- 姓名 + 聯絡電話：高度識別性
- 姓名 + 住址：精確識別個人

➤ 中風險組合（可能識別）

- 系所 + 年級 + 性別 + 出生年月：在小系所中具識別性
- 成績排名 + 課程選修記錄：可推測出特定學生
- 住址 + 電話號碼：可間接識別居住者
- 家長姓名 + 學生年級 + 系所：可推測學生身分

➤ 低風險組合（較難識別）

- 年齡 + 性別：僅統計資料，難以識別
- 系所 + 年級：範圍過大，識別困難
- 興趣愛好 + 社團參與：需更多資料才可識別

案例一：7所高中校務系統遭駭（2024年3月）

- ◆ 事件概要：駭客透過某校系統漏洞入侵主機，竊取該校帳號密碼後，成功登入其他6校使用亞昕公司的校務行政系統，共7校學生個資外洩
- ◆ 洩漏資料類型：學生個人基本資料、家長姓名電話等
- ◆ 影響範圍：7所高中，數千名學生，合計約2萬筆資料
- ◆ 處理方式：72小時內通報、組成專案小組清查26校學習歷程檔案
- ◆ 原因分析：系統漏洞、帳號密碼管理不當、缺乏即時監控

案例二：中正大學個資誤寄事件（2020年10月）

- ◆ 事件概要：通識教育中心向200多位學生寄出學習講座通知，夾帶了學校104~108學年所有入學學生個資
- ◆ 洩漏資料類型：新生個人基本資料
- ◆ 影響範圍：8,495名學生個資
- ◆ 處理方式：依個資法告知當事人，提供法律諮詢管道
- ◆ 原因分析：人為疏失、電子郵件管理不當、缺乏發送前檢核機制

案例三：華航會員資料外洩（2023年1月）

- ◆ 事件概要：華航會員資料遭駭客揭露，多位台灣政界、商界、明星等知名人士個資陸續在國外論壇被揭露
- ◆ 洩漏資料類型：會員個人資料、行程資訊
- ◆ 影響範圍：包含高知名度人士在內的大量會員，超過百萬筆
- ◆ 原因分析：勒索攻擊、資安防護不足

案例四：iRent個資外洩（2023年1月）

- ◆ 事件概要：發現資料庫未加密，導致百萬個信用卡號碼、至少10萬名以上客戶資料流出
- ◆ 洩漏資料類型：信用卡號碼、客戶個人資料（包含身份證明文件、自拍、簽名和租車情況等訊息）
- ◆ 影響範圍：超過10萬名客戶，資料多達40萬筆
- ◆ 法律後果：公路總局要求改正，並依個人資料保護法第48條第4款規定處最高罰鍰新臺幣20萬元，倘後續查有違反個人資料保護法情事，將按次處以罰鍰。如未改正將按次處罰。

案例五：微風百貨個資外洩（2023年2月）

- ◆ 事件概要：收到匿名網路勒索信件，駭客論壇有人聲稱竊取內部資料與90萬用戶個資
- ◆ 洩漏資料類型：用戶個人資料、內部資料
- ◆ 影響範圍：約90萬用戶
- ◆ 原因分析：資料庫遭人「打包帶走」

案例六：性平案當事學生資訊洩漏（2025年4月）

- ◆ 事件概要：教育部政務次長葉丙成在 Facebook 帖文中，提及臺大性平案當事學生，且附有截圖，涉及洩漏當事人個資的疑慮。
- ◆ 洩漏資料類型：涉及性平案學生的個資
- ◆ 影響範圍：涉案學生
- ◆ 原因分析：人為疏失

會議休息中

11:10 開始上課

如參與人員
有相關課程問題
歡迎開啟麥克風或留言區討論

如參與人員
尚未簽到
請在留言區留下
單位+姓名



個資查檢表說明

個人資料查檢表說明與問答

個人資料安全稽核查檢表【簡易版】1 / 9

查檢項目		查檢內容	查核說明
1	人員及權限配置	1.1 已配置專責人員或組織，負責管理及維護保有之個人資料	1. 學校已有個人資料保護的組織 2. 查核的單位已配置專職或專責人員，負責管理及維護保有之個人資料
		1.2 已考量人員職務屬性授予不同權限，避免個人資料檔案遭不當接觸及使用，維護個人資料安全	1. 學校存放個人資料的系統，依照使用者職權，授予不同權限 2. 紙本資料儲存、借閱或取用，有明確規範

1.1 填寫專責單位名稱或專責(職)人員名稱

1.2 主要提供擁有個資單位組織圖、人員、職務或分工說明

- ✓ 分工說明：人員所協助之各項個資保護工作事項
- ✓ 如個資存儲以系統作業，可提供系統的權限設定或權限管控紀錄

個人資料安全稽核查檢表【簡易版】2 / 9

查檢項目	查檢內容	查核說明
2 個人資料蒐集、處理、利用作業	個人資料蒐集、處理、利用時，已 2.1 明確告知當事人特定目的之範圍及目的外之利用，並取得書面同意	各單位蒐集個人資料時，在蒐集的表單上註明：『我已詳細閱讀僑光科技大學『個資蒐集、處理及利用告知聲明』，了解並同意本聲明所有內容，且我瞭解此同意符合個人資料保護法及相關法規之要求，具有書面同意本校蒐集、處理及利用您個人資料。_____ (簽章)』
	2.2 個人資料之利用，如為目的外之利用，已確認符合法定要件	1. 檢核單位個人資料的利用，是否在『個資蒐集、處理及利用告知聲明』中列出的範圍之內 2. 如有超過上述範圍，則必須在確認是否符合個人資料保護法第8條第2項中所列六種情形之一者，如符合則得免為前項之告知。 3. 或查核利用情形是否符合第20條第1項規定，有下列七款情形之一者，得為特定目的外之利用。
	個人資料蒐集已履行告知義務，如 2.2 未履行告知義務時，為符合個資法中免告知之情形	延續2.2的查核，並檢核 1. 資料的蒐集是否有符合個資法規定的免告知狀況 2. 免告知狀況，主要依據個人資料保護法第8條第2點第一項~第六項，及個人資料保護法第9條 3. 另可再確認是否符合個人資料保護法第6條與第20條要求
	2.3 個人資料如有因當事人要求須修正、補充時，依照相關規範及規定執行作業	1. 主要確認單位是否符合「個人資料蒐集、處理、利用與安全管理程序書」中四、作業內容-(二)處理個人資料之控管原則-11及12的要求作業。 2. 主要查核個人資料是否有修正、補充的狀況發生。如有，另查核是否有相關紀錄。因當事人要求修正、補充個人資料時，必須能提交相關紀錄及證明，包含但不限於E-Mail、紙本信件、相關紙本或是電子檔等，能提供佐證，證明是由當事人提出修正、補充等要求。或是當事人提交其所填寫之「個人資料權利行使申請表」。
	2.4 個人資料如有因當事人要求須停止處理、利用、刪除、修毀，依照相關規範及規定執行作業	1. 主要確認單位是否符合「個人資料蒐集、處理、利用與安全管理程序書」中四、作業內容-(二)處理個人資料之控管原則-12.當事人行使個人資料之權利-(2)業務權責單位之處理程序-C&D&E的要求 2. 主要查核當事人提出要求時的申請表或信件，並檢視單位的回覆及相關紀錄

個人資料安全稽核查檢表【簡易版】3 / 9

查檢項目		查檢內容	查核說明
3	當事人權利行使程序	已設置當事人權利行使處理流程， 3.1 當事人提出申請時，依規定進行簽核與相關處理	<p>1. 主要確認單位是否符合「個人資料蒐集、處理、利用與安全管理程序書」中四、作業內容-(二)處理個人資料之控管原則-12.當事人行使個人資料之權利-(2)業務權責單位之處理程序-C~F的規範要求</p> <p>2. 查核資料：「個人資料權利行使申請表」及相關佐證，並檢查單位的回覆##「確認具備法定要件」是指駁回當事人申請的理由必須是法律明文允許拒絕的理由，例如基於公共利益、保護他人權益、執行職務需要等。駁回前，資料持有者要確認這些拒絕的理由真的符合法律所列的情況（法定要件），才可以依法拒絕，並要用書面說明理由與申訴途徑。</p>
		受理當事人權利行使時，確實確認身分；非當事人本人申請時，要求須須附委託同意書及相關證明文件	
		受理申請後，依規定查明申請資料正確性且具備法定要件後，進行對應作業流程，並通知當事人結果	
		3.4 延長回覆期間時，將原因以書面通知當事人	
		駁回當事人申請時，確認具備法定要件，並以書面將拒絕事由、申訴管道及相關聯絡資訊告知當事人	

個人資料安全稽核查檢表【簡易版】4 / 9

查檢項目		查檢內容	查核說明
4	個人資料保存、傳送與盤點	4.1 定期進行個資盤點，並建立個資盤點清冊	1. 查核最近一次個資盤點紀錄，包含但不限於個資清冊等 2. 本校各單位每年應執行個資盤點，檢查個資之使用狀況及存取情形
		4.2 保存個人資料的設備及環境已進行控管與保護，並實施存取的權限管控以保護個人資料安全	1. 查核單位個資存放地點與保護措施 2. 如存放於系統內，需抽查系統使用者的權限，確認權限管控狀況
		4.3 存有個人資料檔案之設備，已定期執行備份作業，並定期查核備份作業執行狀況，確保備份作業成功	1. 查核備份政策 2. 檢查備份資料
		4.4 個人資料已有適當的進行去識別化作業或加密保護	請管理者與一般使用者操作系統，確認畫面呈現資料與資料保護狀況
		4.5 以電子郵件傳送敏感個資檔案時，採加密機制，並確認加密機制之有效性	抽查使用者電腦的寄件備份與收件匣，是否有未加密即傳送的個資



個人資料安全稽核查檢表【簡易版】 5 / 9

查檢項目		查檢內容	查核說明
5	存儲個人資料設備管理	5.1 存放個人資料檔案之電腦定期執行各項漏洞修補程式或安全性更新	檢查電腦的更新紀錄
		5.2 存放個人資料檔案之電腦設備須有防毒軟體並須定期更新	檢查電腦安裝的防毒軟體及更新紀錄
		5.3 存放個人資料檔案之電腦設備委外維修或報廢時，事先移除個人資料	訪談，並抽查維修紀錄及報廢紀錄
		5.4 存放個人資料檔案之電腦設備攜出或借出時，已經權責主管授權核准	訪談，並抽查電腦設備攜出入許可相關紀錄

個人資料安全稽核查檢表【簡易版】6 / 9

查檢項目		查檢內容	查核說明
6	認知宣導、教育訓練與個人資料安全事故通報	6.1 定期進行個人資料保護的認知宣導與教育訓練，且有課後評量結果	檢查教育訓練簽名與考試成績
		6.2 新進人員的教育訓練已包含個人資料保護的認知宣導與教育訓練	抽查新進人員，並比對教育訓練紀錄
		6.3 個資被竊取、洩漏、竄改或其他侵害事故時，確實通報並採取應變措施，且在適當期間內以書面通知當事人	1. 主要確認單位是否符合「個人資料蒐集、處理、利用與安全管理程序書」中四、作業內容-(六)個資事故通報處理及應變 2. 查核「個人資料侵害事故通報與紀錄表」
		6.4 發生個人資料安全事故後，在一定時間內採取預防措施並改善	1. 主要確認單位是否符合「個人資料蒐集、處理、利用與安全管理程序書」中四、作業內容-(六)個資事故通報處理及應變 2. 查核「個人資料侵害事故通報與紀錄表」

個人資料安全稽核查檢表【簡易版】7 / 9

查檢項目		查檢內容	查核說明
7	個人資料使用紀錄、軌跡	對保存之個資進行使用紀錄，如存取及利用紀錄、調閱紀錄、軌跡資料等，並進行證據之管理措施	查核相關的紀錄，如調閱紀錄或是存取紀錄等

7.1 如有留存所有個資使用紀錄，請填寫單位所訂個資使用、相關軌跡記錄等

- ✓ 個人資料使用紀錄
- ✓ 系統主機或儲放個人資料之主機查軌跡紀錄檔截圖
- ✓ 調閱申請紀錄等

個人資料安全稽核查檢表【簡易版】8 / 9

查檢項目		查檢內容	查核說明
8	個人資料保管及刪除、銷毀	8.1 個人資料已訂定適切保管期限，且符合法定要件	1. 查核個資清冊 2. 比對保存年限是否符合20大專校院類檔案保存年限基準表或教育法規要求
		8.2 蒐集目的消失或保管期限到，確實進行個人資料的刪除或銷毀作業	1. 查核個資清冊，並抽查保管期限已到資料，是否進行個人資料刪除或銷毀作業，並有相關紀錄可供查核
		8.3 含有個人資料之存儲設備，報廢或轉作他用時，已採取適當防護措施	1. 訪談，並確認單位是否遵循符合「個人資料蒐集、處理、利用與安全管理程序書」中四、作業內容-(二)處理個人資料之控管原則-5的規範要求 2. 如有USB等，抽查是否有採取防護措施，如設定密碼等
		8.4 含有個人資料之報廢紙張，定期進行銷毀，不回收也不再利用	1. 訪談，並確認單位是否遵循符合「個人資料蒐集、處理、利用與安全管理程序書」中四、作業內容-(二)處理個人資料之控管原則-7的規範要求 2. 抽問個資之報廢紙張如何進行處理？
		8.5 個人資料進行刪除、銷毀作業，保留對應的紀錄	查核個資清冊，並訪談關於個人資料刪除或銷毀作業，是否保留紀錄可供查核

個人資料安全稽核查檢表【簡易版】9 / 9

查檢項目		查檢內容	查核說明
9 委外作業	8.1	委託他人進行資料蒐集、處理或利用時，進行適當監督	訪談並查核個資清冊，確認個人資料如何收集，是否有委外作業
	8.2	當有委外蒐集、處理或利用個人資料之情形時，有確實簽訂書面契約，並依照契約執行監管作業	承上，如有委外，需查核合約及保密切結書
	8.3	契約終止或解除時，要求受託者確實刪除、銷毀或返還相關資料	1. 查詢合約，並確認契約中是否有將此點列入合約中 2. 查核是否有簽署關於契約終止或解除時，要求受託者確實刪除、銷毀或返還相關資料的切結書



VeraCrypt 說明

VeraCrypt 說明

課後測試時間

15分鐘

BCCS 漢昕科技

