離你最近的資安專家

BCCS 漢昕科技

115年一般人員個資通識

個人資料保護實務

個資保護的重要性

漢昕科技股份有限公司
管理顧問部　　梁秋玲

2026-10-15（Thur）

一站式資安防護

©2025, BCCS. All rights reserved.

個人資料保護跟資安有什麼關係？

個人資料保護（個資法）

規範「怎麼蒐集、使用、保存、傳輸、提供個人資料」以保障當事人的權益。

- 保障當事人的隱私與權益
- 要求合法、正當、必要的蒐集與使用
- 規範資料的管理、保存、處理及當事人權利（查詢、更正、刪除等）

個人資料保護（個資法）

重點在「人的權益」

共同目標

保護個人資料免於未經授權的取得、使用、洩漏、竄改或毀損

資訊安全（資安）

重點在「資料的安全」

資訊安全（資安）

透過技術、管理與程序，保護各類資訊資產的機密性、完整性與可用性，避免被未經授權取得或不當利用。

- **機密性**：防止未經授權的存取
- **完整性**：防止資料被竄改
- **可用性**：確保資料在需要時能正常使用

資安是達成個人資料保護的重要手段

沒有資安防護，個人資料很容易被竊取、洩漏或濫用，也就無法保障當事人的權益。

個資保護 + 資安
共同守護學校的信任與安全的學習環境

課程大綱

01. 看見個資：什麼是個資？那些資料容易被忽略
02. 個資為何重要：學生、家長、教職員與學校的影響
03. 個資常見案例：名冊、成績、健康、照片、Email、雲端
04. 正確處理：最少蒐集、最小權限、安全傳遞、適當保存
05. AI 與新風險：生成式 AI、提示詞與權限控管
06. 事件通報：不要自行處理、立即通報、保留證據
07. 課後測驗

©2025, BCCS. All rights reserved.

AGENDA

01. 看見個資

- 什麼是個人資料？
- 哪些資料容易被忽略？

©2025, BCCS. All rights reserved.

什麼是個人資料？

在校園中有哪些常見的個人資料？

個人資料

是指可直接或間接識別特定個人的任何資訊。

校園中常見的個人資料

學籍資料

姓名、學號、系所、入學、註冊、畢業等

成績資料

各科成績、學業表現、排名等

缺曠紀錄

請假、缺課、出缺勤、獎懲紀錄等

住宿資料

宿舍申請、住宿紀錄、房號等

家長聯絡資料

家長姓名、關係、電話、地址等

獎助學金資料

申請紀錄、補助金額、審核結果等

健康資料

健康檢查、疾病紀錄、疫苗接種等

輔導紀錄

心理諮商、輔導紀錄、特殊需求等

電腦與帳號資料

校務系統帳號、使用紀錄、IP 位址等

影像資料

校園監視器畫面、門禁進出紀錄等

哪些資料最容易被忽略

課堂截圖

畫面中的姓名、帳號、頭像、評語、聊天室訊息。

名單片段

只截一欄電話或學號，但仍能回推到特定學生。

活動照片

照片搭配標題、系級、地點與時間就可能辨識個人。

對話記錄

Email、LINE、AI 提示詞中常含有完整個資。

容易忽略，主要是因為資料看起來零碎

校園環境中，零碎資訊彼此高度連結，很容易指向特定個人

©2025, BCCS. All rights reserved.

個人資料的直接辨識 VS 間接辨識

直接辨識：可以直接識別出特定個人的資料

姓名

王小明

學號

身分證字號

電話號碼

0912-345-678

電子郵件

student@univ.edu.tw

地址

臺北市大安區
和平東路二段1號

個人照片

帳號

學校系統帳號
xmwang

簽名

王小明

間接辨識：需要與其他資訊組合，才可能識別出特定個人的資料

課程資訊組合

課程名稱：資訊安全
上課時間：週二 10:00
授課老師：陳○○
出席名單第3位

單獨看可能無法識別，但結合名單、時間、授課老師就能推斷是特定學生。

名單片段

B1123***
資工系大一
男生

雖只有部分學號，但結合系級、年級、性別等資訊，可能識別出特定學生。

活動照片

照片本身或許不含姓名，但結合活動名稱、時間、地點、系級，就可能辨識出特定人。

對話紀錄片段

下週三要繳交
王同學的實習同意書

雖未寫全名，但結合實習、時間、課程或系所，可能識別出特定學生。

電腦使用紀錄

IP 位址：140.112.**.**
登入時間：2025/10/01 09:32
使用系統：選課系統

單獨的 IP 或時間可能無法辨識，但結合帳號、時間、系統與其他紀錄，可可識別出特定學生。

住宿與其他資訊組合

宿舍：A 棟
房號：305
入住時間：2025/09/01
社團：攝影社

單獨的房號可能不明確，但結合入住時間、社團或課程資訊，可能辨識出特定學生。

只要單獨或與其他資訊組合後，可以識別出特定個人，就屬於個人資料，都需要依法保護。

這算個資嗎？

情境	建議判斷	說明
資訊管理系一年級學生	需看情境	單獨資訊較模糊，但結合班級、活動、照片後可能辨識。
學生證照片與姓名	是	可直接辨識特定人。
校慶遠景大合照	需看情境	若無法辨識個人，風險較低；若可清楚放大辨識則不同。
成績表含學號與分數	需看情境	學號可連回特定學生，但若學號有部分遮蔽，則風險較低
去識別化統計圖	不一定	若無法回推個人，可不是個資；若樣本過小仍需注意。

©2025, BCCS. All rights reserved.

辨識個資的三個問題

看得出是誰嗎

直接看到姓名、照片、帳號、學號，即屬高辨識性。

和別的資料拼得起來嗎

零碎資料整合後，也可能變成可辨識個資。

真的需要處理嗎

非必要不蒐集、不分享、不留存，先降低風險。

©2025, BCCS. All rights reserved.

AGENDA

02. 個資為何重要？

- 學校為什麼必須保護個資？
- 個資外洩對學生、家長、教職員與學校的影響

©2025, BCCS. All rights reserved.

為什麼個人資料保護很重要？

保護學生與教職員的權益

避免個人資料被不當蒐集、使用或外洩，
維護當事人的隱私與基本權利。

維護學校的信任與聲譽

妥善保護個人資料，展現負責任的管理，
維持學生、家長及社會大眾對學校的信任。

符合相關法規要求

遵守個人資料保護法、資通安全相關規定
及教育部相關規範，避免違法裁罰與
行政責任。

保障校務正常運作

降低資料外洩、遭竄改或勒索等風險，
避免影響教學、行政與研究等各項業務。

**個人資料保護，不只是避免資料外洩，
更是保障每一位學生與教職員的尊嚴、權益與未來發展。**

大專院校掌握的學生資料

學籍資料
入學、註冊、學籍異動等

成績資料
各科成績、學業表現等

缺曠紀錄
請假、缺課、出缺勤等

住宿資料
宿舍申請、住宿紀錄等

家長聯絡資料
家長姓名、電話、地址等

獎助學金資料
申請紀錄、補助金額等

健康資料
健康檢查、疾病紀錄等

輔導紀錄
輔導諮商、心理評估等

若資料被不當揭露，可能造成的影響

遭遇詐騙
個資被用於假冒身分、詐騙電話或網路詐騙。

標籤化
特定健康、輔導或樹枝資訊被不當貼標籤，影響同儕或師長觀感。

霸凌
敏感資訊被散布，可能導致言語或網路霸凌。

心理壓力
個資外洩可能造成當事人焦慮、不安，影響學習與生活。

個資保護的本質

是尊重當事人對自己資訊的合理期待與控制權。

個人資料外洩對學校的影響

01 信任受損

家長與學生對學校資料治理失去信任。

02 行政負擔

需調查、通報、回應申訴與說明後續處置。

03 校譽風險

事件若擴散到社群或媒體，影響招生與品牌形象。

04 資安延伸

個資常成為社交工程、釣魚與帳號攻擊的入口。

一份名冊的連鎖風險

1. 為方便聯絡寄出完整名冊
   - 姓名、手機、Email、住宿與緊急聯絡人，寄給多位班級幹部。
2. 附件被轉傳了~~
   - 件人再轉到群組，資料擴散到非必要人員。
3. 詐騙利用資料
   - 冒宿舍退費、獎助學金補件、學雜費通知，對學生與家長下手。
4. 學校進入危機處理
   - 須釐清範圍、通報、回應質疑與採取補救措施。

©2025, BCCS. All rights reserved.

個資保護除了法遵之外.....

◆教學面

- ➢學生若因資料外流遭羞辱、騷擾或不公平對待
- ➢直接影響學習權與校園安全感

◆治理面

- ➢個資保護展現的是學校治理能力
- ➢能區分必要與非必要
- ➢是設計出正確流程與權限

©2025, BCCS. All rights reserved.

關於個人資料保護.....私立大專院校適用的規定

- 個人資料保護法：共同規定與非公務機關適用規定
- 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
- 教育部對所有大專院校的具體要求
  - 教職員、學生會及社團不得任意取得學生名單，依據教育部於民國114年6月20日以「臺教資通字第1140065023號函」要求
  - 教育體系資通安全暨個人資料管理規範

©2025, BCCS. All rights reserved.

教育部_個資行政檢查作業

有鑑於教育服務對資訊系統的依賴度提升，個人資料跨單位的流通也日益頻繁，為深植資安意識並落實個資保護，教育部針對私立學校、幼兒園、補習班、課後照顧中心及運動體育團體等與民眾接觸頻繁的單位，啟動個資保護查核作業，以協助各機構落實個資安全管理，防範資料外洩或遭不當使用，進一步保障學生、家長與教職員的相關權益。

教育部自112年起持續辦理「個資行政檢查作業」，以確保教育機構的個資管理更具保障。115年度的查核工作預計5月開跑，並持續執行至10月。透過「書面審查」與「實地走訪」雙管齊下，協助各級機構檢視防護措施，提升大眾提供個資時的信任感與安心感。

本次查核的核心重點在於確認各單位是否已建立並落實「個資安全維護計畫」，且在個資的蒐集、處理、利用、保存及刪除等各階段，皆須符合《個人資料保護法》的規範。教育部期望透過此機制提早察覺潛在漏洞，輔導單位即時修正並強化管理制度。查核結束後，教育部要求未達標單位限期改善，並定期召開檢討會議，依執行現況滾動式修正策略，持續增進教育機構的資安防禦力。

除查核外，教育部也同步提供多元化的教育訓練課程，協助基層人員深入掌握法規要求及標準作業流程，目標是將「個資保護」從制度層面落實到日常操作的每個細節中。

教育部亦呼籲，各教育事業應主動進行定期自我檢視，並投入資源於內部培訓與制度升級。未來，教育部將視實務需求持續優化查核機制，協助教育界應對資安挑戰，共同營造一個更安全、更值得信賴的學習與服務環境。

©2025, BCCS. All rights reserved.

AGENDA

03. 個資常見案例

□ 校園常見外洩情境與案例

©2025, BCCS. All rights reserved.

案例一 誤寄完整名單

一封誤寄的信，可能造成個資外洩風險

1 事件情境

2024 年，國防部在處理高階人員財產申報相關作業時，原應個別傳送的資料檔，卻被誤寄給多名申報人員及其所屬單位。經調查，外洩資料涉及姓名、職稱、服務單位及申報年度等基本個資；主管機關後續要求收件者返還文件並進行風險管控。

申報名單.xlsx

姓名	職稱	服務單位	申報年度
王○○	少將	○○司	113
林○○	上校	○○處	113
陳○○	中校	○○室	113
⋮	⋮	⋮	⋮

2 情境分析

事件不是駭客攻擊，
而是**行政傳遞流程與收件範圍控制失誤**。

原本應採**「一人一份」**或**系統個別查詢**的資料，被改以較方便的**集中檔案處理**。

即使未包含財產明細，姓名、職稱、單位與年度等資料仍可被用於**身分辨識、社交工程或針對性騷擾**。

3 可能風險

收件人取得不屬於自己業務必要範圍的資料。

資料被**轉寄、截圖、下載**或長期留存在個人信箱與裝置。

攻擊者可利用職稱、單位與姓名製作更具可信度的**釣魚信件**。

對高風險職務人員，基本身分資料也可能**增加人身安全**與**針對性攻擊風險**。

4 應對方式

1. 立即**停止後續寄送**，確認誤寄範圍、收件人與附件版本。
2. 立即依內部流程**通報**主管、個資保護與資安窗口。
3. 請誤收者依正式指示停止使用、**刪除或返還**資料；保留往來紀錄。
4. **改善流程**，例如採**個別寄送**、受權限控管的查詢系統、寄件前覆核與敏感附件加密。
5. 對大量寄送設定**延遲送出**、**附件名稱檢查及收件人雙重確認**。

學校中可能發生類似的情境~~~

- 教師或助教把全班姓名、學號、電話、Email 上傳到課程平台或寄給所有學生，方便聯繫與分組
- 將全班成績表、獎助學金資格名單、住宿名單或家長聯絡資料寄給所有班代、導師或行政窗口，而非僅提供各自需要處理的資料
- 風險點：超出必要範圍揭露，資料被下載、轉寄、另作他用，甚至流向校外。
- 適合做法：
  - 只提供必要欄位，優先用系統分權限查詢
  - 依照對象提供其必要的資料
  - 避免公開手機、地址、緊急聯絡人

©2025, BCCS. All rights reserved.

案例二 大規模戶役政資料疑似外流

超過 2,300 萬筆台灣民眾戶籍相關資料在網路論壇被販售，引發社會高度關注

1 事件情境

2022 年底，網路論壇出現宣稱包含超過 2,300 萬筆台灣民眾戶籍相關資料的販售資訊。相關報導指出，資料可能包含姓名、身分證字號、家庭關係、戶籍、原住民族身分、兵役及遷徙日期等高價值資訊。

2 情境分析

風險不只是單一系統是否被入侵，也包含資料介接、外部查詢、資料交換與存取紀錄是否受到妥善治理。

資料愈完整、可交叉比對的欄位愈多，對詐騙集團、跟蹤騷擾者或社交工程攻擊者的價值愈高。

大規模資料外流後，即使來源被關閉，已外流資料仍可能被複製、轉售、重新整併，難以真正回收。

3 可能風險

冒名申辦、身分驗證詐騙與精準釣魚。

以家庭關係、住址、兵役或遷徙資訊進行騷擾、跟監或人身威脅。

與其他平台資料交叉比對，形成更完整的個人輪廓。

民眾對政府與服務機構的信任下降。

4 應對方式

1. 建立資眾最少化原則，避免跨系統或跨單位交換超出業務必要的欄位。
2. 對高敏感資料採更嚴格的角色權限、申請核准、查詢目的與期限控管。
3. 建立可追溯日誌，定期檢查大量查詢、異常下載、非上班時間存取等異常行為。
4. 對外部介接、委外服務與資料交換，建立契約要求、存取紀錄、定期稽核與終止後資料刪除機制。
5. 事件發生後，依規定迅速通知受影響當事人，通知內容應包括事件事實與已採取的應對措施。

學校中可能發生類似的情境~~~

- 校務系統、招生系統、學務系統、宿舍系統、輔導系統與人事系統之間，若長期以完整 Excel、共享資料夾或未受控 API 交換資料，就可能形成相同類型的風險。

©2025, BCCS. All rights reserved.

案例三 大學學生資料與研究資料遭公開兜售

學生資料、聯絡人資料、研究論文檔案出現在駭客論壇，引發高度關注

1 事件情境

2026 年 9月，媒體報導駭客論壇出現宣稱與國立中央大學有關的資料樣本與販售資訊，內容包括**學生註冊資料、聯絡人資料及研究論文相關檔案**；樣本涉及姓名、Email、電話、地址、生日、學籍、學費、獎助學金、住宿與研究資料等。校方表示已知悉網路貼文並展開查證，但當時尚無足夠證據確認資料係由校內系統遭入侵取得，也不排除公開或其他來源資料被蒐集、整併。

2 情境分析

即使尚未確認入侵來源，資料樣本中若有可驗證的真實個資，仍必須以**高風險事件**方式處理與查證。

大學資料不只包含學生基本資料，也可能進結住宿、學費、獎助學金與研究成果，**資料價值與影響範圍**比單一聯絡名冊高。

資料可能不是從單一核心系統直接外洩，而是從**多個**公開、半公開、舊系統、委外平台或**人員副本被整併而成**。

3 可能風險

對學生進行「學費退費」「宿舍補件」「獎助學金資格確認」等**精準詐騙**。

以學生姓名、Email、系所及研究主題進行**釣魚信件與帳號攻擊**。

研究資料、審查資訊、共同作者或經費來源外洩，**影響學術倫理、研究競爭與合作關係**。

學生家庭經濟、住宿或補助資料被揭露，可能造成**標籤化、歧視或騷擾**。

4 應對方式

1. 立即啟動**事件分級、資安鑑識與資料比對**，釐清樣本是否真實、來源可能在哪裡、影響範圍多大。
2. 保全**系統日誌**、雲端存取紀錄、管理者帳號活動、資料庫查詢與大量下載紀錄。
3. 盤點公開網站、舊網站、研究平台、招生系統、委外服務與共享雲端中是否存在**重複或過度公開的資料**。
4. 對學生與教職員發布**防詐與防釣魚提醒**，特別提醒勿因來信掌握真實學籍或住宿資訊就直接信任。
5. 依調查結果採取**密碼重設、多因素驗證、權限收斂、弱點修補、資料下架、通知與後續監控**。

在學校中應該要問的~~~

- 主系統有沒有被駭？
- 資料是否曾被下載到個人電腦、Google Drive、USB、Email 附件、委外平台或研究協作工具？
- 資料有沒有通過社群軟體分享出去？

©2025, BCCS. All rights reserved.

案例四 電商資料遭未授權接觸

超過 20 萬名台灣用戶資料外洩，涉及姓名、Email、電話、配送地址及部分訂單紀錄等資訊

1 事件情境

2026 年，台灣媒體報導酷澎台灣用戶資料外洩事件，經第三方資安鑑識確認，有超過 20 萬名台灣用戶資料曾遭未授權接觸，涉及姓名、電子郵件、電話、配送地址及部分訂單紀錄等資訊。

2 情境分析

聯絡資料、地址與訂單資訊單看可能不是最高敏感度資料，但**結合後可形成非常有效的詐騙素材**。

攻擊者若知道使用者購買過什麼、住在哪裡、電話與 Email 是什麼，就能**假冒客服、物流、退款或付款平台**。

這類事件說明：不是只有身分證字號或金融帳戶才值得保護；可用於建立**可信情境的資料**，同樣**具有高風險**。

3 可能風險

假冒物流、客服或退款通知的**精準詐騙**。

偽造釣魚信件或簡訊，誘導當事人**輸入帳密、信用卡或驗證碼**。

地址與聯絡資料被用於**騷擾、跟蹤**或其他**人身安全風險**。

資料被與社群資料、公開資料交叉整併，**提升冒名與社交工程成功率**。

4 應對方式

1. 立即確認未授權存取的**資料種類、時間範圍、帳號範圍**與**可能的外流途徑**。
2. 強化帳號保護措施，例如**密碼重設、多因素驗證、異常登入偵測**與 API 金鑰輪替。
3. 對受影響者提供**明確通知**，說明已知事實、可能風險及可採取的自我保護措施。
4. 透過客服、網站、Email 與社群提醒使用者**防範假冒客服、物流與退款詐騙**。
5. 改善資料**存取權限**、第三方存取管理、**日誌監控**與異常大量匯出偵測。

學校中可能發生類似的情境~~~

- 學生名冊若包含姓名、電話、住宿地址、繳費或補助狀態，也同樣可能被用來製作「學雜費補繳」「宿舍費退費」「獎助學金補件」等高可信度詐騙
- 學生的緊急聯絡資訊中，如果包含姓名、電話、地址等，可能也會讓緊急聯絡人陷入詐騙風險

©2025, BCCS. All rights reserved.

案例五 內部人員越權取得資料

利用系統後門取得員工個資，涉及身分證字號、健保相關資訊等，並與他人分享

1 事件情境

2026 年媒體報導，前國家資通安全研究院人員被指控利用人資系統後門取得員工個資，涉及員工的身分證字號與健保相關資訊等，並與其他人分享。

2 情境分析

個資風險不只來自外部駭客，也可能來自**內部人員**的越權、濫用、好奇查詢或不當分享。

內部人員熟悉系統、帳號、資料位置與作業流程，若缺乏權限管理、日誌監控與職務分離，風險更難及早發現。

系統存在**後門**、共用管理帳號、權限**未定期檢視**或離職未停權，都可能放大內部威脅。

3 可能風險

人事、薪資、健康、考核與聯絡資料被不當查閱或散布。

可識別資料被用於**冒名**、詐騙、騷擾或針對性攻擊。

組織內部信任與員工**安全感受損**。

因資料被不當存取卻未及時偵測，影響範圍持續擴大。

4 應對方式

1. 落實最**小權限與職務分離**，避免單一人員同時具備查詢、匯出、修改與刪除大量資料的權限。
2. **禁止共用帳號**，管理者帳號應具名、強化驗證並受嚴格監控。
3. 對高敏感資料的查詢、下載、匯出**建立日誌**，並**針對異常**查詢量與非正常時段存取產生告警。
4. **定期進行權限覆核**；人員調職、離職、專案結束時立即收回權限。
5. 設置內部**通報與吹哨機制**，讓同仁發現可疑**查詢**、**資料外帶**或不當分享時**能安全回報**。

學校中可能發生類似的情境~~~

- 教師、系辦、學務、輔導、人事或資訊人員因工作可存取學生與教職員資料，不代表可以基於好奇、私人關係或非職務目的查詢、下載或分享
- 有權限的人在公用電腦下載學生與教職員資料列印後，未刪除資料，讓之後的使用者可以看到這些學生與教職員的資料

©2025, BCCS. All rights reserved.

學校環境中常見的個資外洩

- **學生名冊**

  教師或助教把全班姓名、學號、電話、**Email** 上傳到課程平台或寄給所有學生，方便聯繫與分組

- **成績公告**

  將全班成績表寄給所有學生，或在教室外張貼姓名與成績

- **家長與緊急聯絡資料**

  LINE 群組貼上家長電話名單、導師交接時直接轉傳完整名單、志工或學生幹部取得家長資訊

- **健康與輔導資料**

  病假證明、診斷書、身心狀況、諮商與特教需求等寄到共用信箱

- **Google Drive / 雲端硬碟**

  錯誤設定，像是知道連結的任何人都可看、多人皆可編輯、專案結束權限未移除

- **個人裝置與 USB**

  學校的資料被下載到私人筆電、手機、隨身碟

©2025, BCCS. All rights reserved.

從每個案例中記住以下五個問題

1 資料是從哪裡來的？

系統、Email、紙本、雲端、AI、委外或內部人員。

2 誰本來應該可以看？

只有業務必要人員，而不是所有同事、群組成員或合作對象。

3 資料為什麼會擴散？

誤寄、過度權限、公開連結、未加密副本、內部濫用或外部入侵。

4 當事人可能受到什麼傷害？

詐騙、騷擾、標籤、歧視、名譽與人身安全風險。

5 第一時間怎麼做？

停止擴散
立即中止後續寄送、關閉公開連結或收回權限。

立即通報
依內部流程通報主管、個資保護與資安窗口。

保留證據
保全相關郵件、檔案、系統日誌與存取紀錄。

配合調查
提供必要資料，協助釐清事件與影響範圍。

統一處置
依規定進行通知、補救與後續監控。

事件通知重點（依台灣個資保護規範要求）

對受影響當事人的事件通知，應包含：**外洩事實** 及 **已採取的應對措施**。

AGENDA

04. 正確處理

◘ 正確處理個資的日常方法

©2025, BCCS. All rights reserved.

個人資料的蒐集與使用原則

學校處理個資時，應先釐清下列四個問題，避免因習慣或便利而過度蒐集。

- **為何需要？** 蒐集的目的為什麼？
- **需要哪些？** 需要的資料欄位有哪些？
- **誰會使用？** 哪些人員或單位會使用？
- **會保存多久？** 資料會保存多長時間？

建議落實下列原則

1 目的明確

招生、學籍管理、成績評量、住宿管理、獎助學金、健康照護、教職員人事、研究計畫、其他業務

明確訂定蒐集目的，例如招生、學籍管理、成績評量、住宿管理、獎助學金、健康照護、教職員人事或研究計畫等。

2 最少蒐集

身分證字號 ⊘
完整家庭資料 ⊘
健康資料 ⊘

只蒐集完成業務真正需要的欄位；一般活動報名不應習慣性要求身分證字號、完整家庭資料或健康資料。

3 目的內使用

蒐集目的
- ☑ 學籍管理
- ☑ 成績評量
- ☑ 住宿管理
- ☑ 獎助學金
- ☑ 研究計畫

不得任意改作其他用途

資料應在**原蒐集目的範圍內使用**，不應因「可能以後有用」就被改作其他用途。

4 對外提供有依據

符合法源並完成核准

- 教育主管機關
- 合作學校
- 廠商
- 研究機構

提供前應**確認法源、業務必要性、核准程序及安全傳遞方式**。按照校內管理要點，對外提供前應確認依據並完成核准，且紙本與電子檔案應採取加密等措施。

5 保障權利行使

當事人權利
- ✓ 查詢
- ✓ 閱覽
- ✓ 複製
- ✓ 更正
- ✓ 停止處理利用
- ✓ 刪除

建立當事人權利申請窗口與流程，讓學生、教職員等能依法行使查詢、閱覽、複製、更正、停止處理利用及刪除等權利。

在蒐集個資時，應向當事人說明：
- ☑ 機關或單位名稱
- ☑ 蒐集目的
- ☑ 資料類別
- ☑ 利用期間／地區／對象／方式
- ☑ 當事人權利
- ☑ 不提供資料可能造成的影響

為何需要？需要那些

- 蒐集的目的是甚麼？
  - 確認真正的蒐集目的與應該蒐集內容
- 對應對應目的，需要的資料欄位有哪些？蒐集最小化
- 常見過度蒐集
  - 活動報名就要求身分證字號
  - 一般聯繫卻蒐集家長完整資料
  - 先收再說，因為未來可能會用到
- 正確思維
  - 欄位逐一檢視，刪除非必要項目
  - 只蒐集完成業務所需資料
  - 特殊資料要有清楚處理理由

©2025, BCCS. All rights reserved.

誰會使用？

- 那些人員或單位需要使用或需要看？
  - 使用權限要依角色與案件，而不是依關係方便
  - 檢視、留言、編輯與管理者權限應分開
  - 人員異動後若未收回權限，風險會持續存在
- 傳送的方式及可能的風險
  - E-Mail：直接寄完整附件給多人
  - 通訊軟體：群組公開個人資料
  - 雲端：公開連結，不限下載
  - 紙本：交辦後任意放置

©2025, BCCS. All rights reserved.

會保存多久？

- 資料需要保存多久時間？
- 常見問題
  - 桌面下載區、郵件附件、歷史資料夾、舊 USB、私人電腦與共用雲端，都可能留下副本
- 管理原則
  - 依校內保存年限與業務需求保存
  - 專案或作業結束後，移轉、封存或刪除，不無限累積。

©2025, BCCS. All rights reserved.

關於學校對個資的日常保護措施

從日常作業做起，保護學生、教職員與學校的個人資料

Email 與通訊軟體

- 大量寄送學生或家長通知時，**使用密件副本（BCC）或校方核准的群發工具**。
- 寄送前**核對收件人、附件、附件版本及 CC／BCC 設定**。
- 不在 LINE、Teams、Facebook 或班級群組公開未繳費、缺課、成績、健康、輔導或家長聯絡資料。
- 敏感資料優先使用**校務系統或權限控管連結**，不任意寄送完整 Excel 名冊。
- 含敏感資料的電子檔，依**校內規範加密**，且密碼應以**不同管道通知**。

雲端、系統與帳號

- **優先使用校方受管理帳號與核准雲端服務**，不以私人 Google Drive、私人 Email 或私人通訊軟體長期處理公務個資。
- 雲端資料夾**只授權特定帳號**，避免設定為「知道連結的任何人都可檢視／編輯」。
- **依職務授予最小權限**，區分檢視、下載、編輯、匯出與管理權限。
- 人員離職、調職、專案結束或學生畢業後，**應檢視並移除不再需要的存取權限**。
- 對個資資料庫、校務系統及重要雲端資料夾**啟用身分驗證、存取控制、加密傳輸、操作日誌與異常監控**。

紙本與實體文件

- 學生名冊、成績資料、補助申請、病假證明、診斷書、人事資料及研究文件應**妥善鎖存**。
- **列印後立即取件**，不讓文件長時間留在印表機、會議室、辦公桌或公共區域。
- 會議資料採**編號、回收**或依需要提供；**避免將完整敏感資料**作為一般**會議附件**。
- 到期或不再需要的紙本資料，依校內程序以**碎紙、集中銷毀或其他安全方式處理**，不可直接丟進一般垃圾或回收箱。

小心處理 就是最好的保護 | **遵守規範 保護自己也保護學生** | **多一分謹慎 少一分風險** | **確實落實 讓個資更安全**

高風險資料加強管理

這些資料一旦外洩，可能對學生、教職員或其家屬造成重大影響，
學校應採取更高強度的控管措施。

學校常見的高風險資料類型

學生健康與輔導資料

身心障礙與特教需求

診斷或病假證明

成績與獎懲

家長及緊急聯絡資訊

家庭經濟與獎助學金資料

人事薪資與考核資料

研究受試者資料

可連結到上述資料的
帳號與系統紀錄

建議的加強管理措施

1 限縮存取與授權管理

僅授權**業務必要人員**，
並依案件或職務給予適當權限。

2 使用受控系統妥善保存

使用**校方受控系統**保存，
避免散落於個人電腦、USB、
私人雲端或 Email 附件。

3 設定保存期限定期清理

依規定**設定保存期限**，
定期檢視並安全刪除不再需要的資料。

4 日誌監控與異常告警

針對大量匯出、異常下載、
非上班時段查詢及高權限帳號操作
建立**日誌與告警機制**。

5 檢視表單與歷史資料

定期確認現有表單是否**過度蒐集資料**，
並檢查歷史資料夾是否仍保留
不必要的副本。

高風險資料需要**更嚴謹的管理**，
才能保護學生、教職員及其家屬的隱私與安全，維持校園的信任與正常運作。

Email 寄送前檢查卡

收件人

- 是否寄給正確人員？
- 需不需要全部看到彼此地址？

附件

- 是不是最新版？
- 是否含不該寄出的欄位或工作底稿？

替代方式

- 可否改為權限控管連結
- 系統查詢或個別通知？

©2025, BCCS. All rights reserved.

雲端共用檢查卡

收件人	附件	替代方式
• 是否寄給正確人員？ • 需不需要全部看到彼此地址？	• 是不是最新版？ • 是否含不該寄出的欄位或工作底稿？	• 可否改為權限控管連結 • 系統查詢或個別通知？

BCCS 漢昕科技 - 離你最近的資安專家 -
©2025, BCCS. All rights reserved.

紙本管理檢查卡

列印後立即取

- 印表機旁不留資料

敏感文件上鎖

- 抽屜、櫃體與會議

  資料要有管制

依規定銷毀

- 不要當一般垃圾或

  資源回收直接丟棄

©2025, BCCS. All rights reserved.

委外作業的風險

將個資交由廠商或合作單位處理時，可能因其管理不足而造成外洩、濫用或被再次轉交。
學校不會因為資料交由廠商處理，就免除自身管理責任。

常見的委外對象

- **活動廠商**（報名、活動管理）
- **系統維護商**（校務系統、資訊設備）
- **雲端服務商**（雲端儲存、SaaS）
- **問卷平台**（調查、滿意度問卷）
- **研究合作機構**（研究資料、受試者資料）
- **其他委外單位**（設計、印刷、物流等）

可能的風險

- **資料遭外洩**
  廠商資安防護不足或遭駭客入侵
- **內部人員濫用**
  未經授權查閱、下載或轉交他人
- **再委外或轉交**
  未經同意將資料轉交其他廠商
- **管理不當**
  權限過大、保存過久、未安全刪除
- **事件通報延遲**
  發生外洩後未即時通知學校

契約或管理要求應包含

資料用途	只能用於約定的業務目的，不得作其他用途
可存取範圍	僅限業務必要人員，採最小權限
安全措施	要求具備適當的技術與管理安全措施
再委外限制	未經同意不得再委外或轉交其他單位
事件通報	發生資安事件應立即通報學校
保存期限	約定保存期間，屆期應刪除或返還資料
返還與刪除	合約終止後，完整返還或安全刪除所有資料

加強管理，降低委外風險

1. **事前評估**
   確認廠商資安能力與過往紀錄
2. **簽訂契約**
   明確規範資料使用及安全要求
3. **持續監督**
   定期稽核、檢視資安措施執行情形
4. **合約終止**
   確認資料返還或安全刪除

AGENDA

05. AI 與新風險

◘ AI 的個資風險

©2025, BCCS. All rights reserved.

中央社
國際焦點
韓國
韓金融資安警報 萬人個資外洩AI疑幫凶

AI 時代的核心觀念

在使用生成式 AI 時，請記住：您輸入的內容，可能成為外部工具處理的資料

1 提示詞也是資料傳送

把學生姓名、成績、家長聯絡方式貼進對話框，
本質上就是**把資料送入外部工具處理。**

即使只是「問問題」或「請 AI 幫忙整理」，
只要包含**可識別的個人資料**，就屬於**資料傳送**。

2 上傳檔案更敏感

PDF、Excel、診斷書、會議紀錄若原封不動上傳，
風險通常比單純問答更高。

文件中可能包含大量個人資料、敏感資料
與其他可連結資訊，**上傳前務必去除不必要內容或避免上傳。**

AI的風險來源

- 提示詞：直接貼入可識別內容
- 上傳附件：原始資料檔未去識別化
- 串接外掛：AI 可讀取 Email、雲端、資料庫
- AI Agent權限：授權過大，可能越權讀取或誤寄

©2025, BCCS. All rights reserved.

案例：把成績貼給 AI 寫輔導建議

運用 AI 快速生成學生輔導建議雖然方便，但也可能造成個資外洩風險！

1 便利點

可以節省時間，快速產出個別化的輔導建議與文字內容。

- 快速分析學生學習狀況
- 協助撰寫輔導建議
- 節省文字撰寫時間
- 提供不同角度的建議參考

2 風險點

把包含學生姓名與成績的名單輸入 AI，可能造成以下風險：

個資外洩風險

學生姓名、學號、成績等個資可能被外部工具處理或留存。

資料用途不明

無法確定輸入的資料會如何被使用、是否用於模型訓練。

涉及大量敏感資料

成績可能揭露學生的學習弱點，若與其他資料比對，可能進一步識別特定學生。

難以完全刪除

送出的資料可能已被暫存、備份或留存在第三方系統中，難以保證完全刪除。

3 建議作法

若需要使用 AI 輔助撰寫輔導建議，請採取以下做法：

去識別化資料

先移除或以代碼取代學生姓名、學號等可識別資訊。

僅提供必要資訊

只提供分析所需的重點資料，避免整份成績名單直接上傳。

使用學校核准的 AI 工具

依學校資訊安全規範，使用經評估並核准的工具或環境。

人工審閱與修正

AI 產出的內容僅供參考，需由老師專業判斷並檢視後再使用。

避免輸入其他敏感資訊

不輸入家長聯絡方式、健康資料、輔導紀錄等其他個資。

案例：上傳學生申請文件請 AI 摘要

將學生的申請文件（如獎助學金、特殊教育、就學貸款等）上傳給 AI 進行摘要，
雖然能快速整理重點，但也存在個資外洩風險。

1 便利點

可以快速整理申請文件的重點，
節省閱讀時間，協助撰寫核辦意見。

- 快速整理大量文件
- 提取重點與關鍵資訊
- 協助撰寫核辦意見
- 節省人工閱讀與整理時間

2 風險點

若直接上傳未去識別化的申請文件，
可能造成以下風險：

個資外洩
文件包含學生姓名、身分證號、家庭狀況、健康或特殊需求等敏感資料，可能被外部工具處理或留存。

資料用途不明
無法確定上傳後的資料會如何被使用、是否用於模型訓練，或留存在服務端。

敏感資料暴露
可能包含家庭經濟、身心障礙、診斷證明、醫療資訊等高度敏感資料。

影響學生權益
資料若外洩，可能造成學生被標籤化、歧視或被不當使用，影響其權益與隱私。

3 建議作法

若需要使用 AI 協助摘要，請採取以下做法：

先去識別化
移除或遮蔽姓名、身分證號、地址、電話、具辨識性的細節。

僅提供必要資訊
只保留與申請目的相關的內容，避免整份原始文件上傳。

使用學校核准的 AI 工具
依校內資安規範，使用經評估並核准的 AI 工具或環境。

人工審閱與修正
AI 產出的摘要僅供參考，需由承辦人確認正確性與適當性。

避免上傳完整原始檔
不直接上傳包含個資與敏感資料的 PDF、Excel、診斷書等原始檔案。

案例：AI Agent 串接雲端與 E-mail

1 設計情境

自動讀取 Google Drive 產生回覆
AI Agent 連結雲端硬碟，
自動讀取學生相關文件並產生回覆。

自動寄送 Email
AI Agent 根據內容自動撰寫並寄送
Email 給學生或家長。

聊天機器人查詢學生進度
透過對話方式；查詢學生的修課、
出缺席或申請進度等資訊。

2 可能風險

讀到非必要資料夾、下載敏感文件
可能讀取到包含學生個資、
成績、診斷書等敏感檔案。

誤寄附件、寄給錯誤收件人
自動寄信時可能附上不當檔案
或寄送到錯誤對象。

身分驗證不足，造成越權查詢
若權限設定不當，可能查詢到
不屬於本人學生的資料，並留下操作紀錄。

3 控制重點

限縮資料夾與檔案類型權限
僅開放必要資料夾，限制可讀取
的檔案類型與內容範圍。

高風險寄送保留人工覆核
重要郵件、含附件或外部收件人，
須經人工確認後才寄送。

查詢前驗證身分並記錄操作
要求身分驗證、依權限查詢，
並保留完整操作紀錄以便稽核。

使用AI前的五秒快速檢查

在輸入、上傳或授權之前，先停下來 5 秒鐘，確認以下 5 個問題！

1 這些資料可以輸入嗎？

- 是否包含學生姓名、學號、身分證字號？
- 是否包含成績、健康、家庭、輔導等敏感資訊？
- 是否能先去識別化或使用代碼？

2 附件或檔案可以上傳嗎？

- 檔案是否包含大量個人資料？
- 是否有不必要的欄位或敏感內容？
- 是否能先刪除或遮蔽個資後再上傳？

3 會串接其他系統或外掛嗎？

- 是否會讀取我的E-mail、雲端硬碟、資料庫或其他系統？
- 是否只授權必要範圍？
- 是否清楚資料會被如何處理與留存？

4 AI 會替我執行動作嗎？

- 是否可能自動寄信、建立檔案或修改資料？
- 是否已設定最小權限？
- 是否需要保留人工確認機制？

5 結果可以直接使用嗎？

- 內容是否正確、完整？
- 是否可能包含錯誤、偏見或不當資訊？
- 是否需要人工審閱與修正後再使用？

停下來檢查 5 秒鐘，資料更安全、工作更安心！

AI 可考慮做與不宜做

可考慮做

- 去識別化文本摘要
- 行政文案草稿
- 公開資料整理與翻譯

不宜做

- 貼入完整成績、輔導、健康資料
- 上傳含身分證與地址的原始文件
- 讓 Agent 無限制讀寫校務資料

©2025, BCCS. All rights reserved.

AGENDA

06.事件通報

- 疑似個資事件發生時怎麼做

©2025, BCCS. All rights reserved.

個資侵害事故通報

- 依私立專科以上學校及私人學術研究機構個人資料檔案安全維護實施辦法規定，在發生個資被竊取、洩漏、竄改或其他侵害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」(如右)，迅速處理以保護當事人之權益。

機密等級：□機密 □敏感 □一般　　文件編號：OCU-4-043　　版本：1

日　　期：　　年　　月　　日　　紀錄編號：

僑光科技大學

個人資料侵害事故通報與紀錄表

非公務機關名稱 通報機關	通報時間：　　年　　月　　日　　時　　分 通報人：　　簽名（核 章） 職稱： 電話： E-mail： 地址：	
事故發現時間		
事故發生種類	□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） □一般個資_____筆 □特種個資_____筆
發生原因及事故摘要		
損害狀況		
個資侵害可能結果		
擬採取之因應措施		
擬採通知當事人之時間及方式		
是否於發現個資外洩後72小時通報	□是　　□否，理由：	

©2025, BCCS. All rights reserved.

哪些情況算疑似個資事件

- Email 誤寄、CC / BCC 設定錯誤、附件寄錯或寄給錯誤對象
- 雲端資料夾、表單或檔案連結設定為公開，或被不應存取者下載
- 學生名冊、成績、健康、輔導、住宿、家長聯絡、人事或研究資料遺失、遭竊、被不當公開或轉傳
- 帳號遭盜用、惡意程式、勒索軟體、系統入侵或資料庫異常匯出
- 個人電腦、手機、USB、紙本文件遺失或遭竊
- 委外廠商、雲端服務、問卷平台、研究合作單位或 AI 工具疑似不當存取、使用或外流資料
- 內部人員未經授權查詢、下載、截圖、列印、轉寄或分享資料

©2025, BCCS. All rights reserved.

當發生個資事件的時候~~~

保持鎮定

不要自行處理

立即通報

保留證據

配合處置

©2025, BCCS. All rights reserved.

個資侵害事故的處理與通報

- 依“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8條要求：
  1. 立即控制損害。
  2. 查明原因及影響。
  3. 適當通知當事人。
  4. 研議改善措施。
  5. 自發現事故起72小時內，填具「個人資料侵害事故通報與紀錄表」通報教育部。
  6. 未能於72小時通報者，應附理由。
  7. 處理結束後一個月內，將處理方式及結果報教育部備查。
- 這裡的72小時是「自發現事故起算」，不是等到調查完成或確認有人利用才開始。

©2025, BCCS. All rights reserved.

個資事件處理四步驟

1. 停止持續擴散

   先撤下公開連結、停止寄送、暫停可疑帳號，但不要任意刪除紀錄

2. 立即依流程通報

   通知主管、個資窗口、資訊或資安單位

3. 保留證據

   保留信件、截圖、時間點、收件人、檔案名稱與連結

4. 配合統一處置

   由權責單位評估、通知、補救與對外說明

©2025, BCCS. All rights reserved.

進行個資事件通報時至少提供哪些資訊？

資訊項目	說明
事件時間	何時發現、何時發生、是否仍持續
資料類型	學生名冊、成績、健康、照片、家長聯絡等
可能範圍	可能涉及多少人、哪些單位或收件者
系統或媒介	Email、雲端、LINE、紙本、AI 工具、USB 等
已做措施	已停止哪些動作、是否已撤權或下架

©2025, BCCS. All rights reserved.

AGENDA

07. 課後測驗

- 20分鐘課後測驗時間~~~

  請各位同仁把握時間

AGENDA

滿意度調查~~

- 請掃碼做滿意度調查~~謝謝

©2025, BCCS. All rights reserved.

BCCS 漢昕科技

- 離 你 最 近 的 資 安 專 家 -

Thank you

FOR YOUR ATTENTION

Get in touch:

雲安維運　聯防設備　風險檢測　顧問諮詢　資安學苑

©2025, BCCS. All rights reserved.

考前抱佛腳~~1

1. 最符合「個人資料」的判斷原則：只要資料可直接或間接辨識特定個人，就可能是個人資料
2. 教師將全班學生姓名、學號與成績投影在教室螢幕上，主要可能產生何種問題？未經必要評估而公開學生個資
3. 行政人員要寄送活動通知給多位家長，但家長彼此不需要知道其他人的 Email，較適當的作法是？將所有 Email 填入「密件副本 BCC」欄位
4. 何者最符合「最少蒐集」原則？只蒐集完成特定業務所必要的資料

©2025, BCCS. All rights reserved.

考前抱佛腳~~2

5. 系辦人員將學生完整名冊放在 Google Drive，並設為「知道連結的人都可檢視」，主要風險為何？可能讓未經授權者取得或下載學生資料
6. 下列哪一項最適合透過班級 LINE 群組公開？不涉及個人身分的活動時間與地點
7. 教師需要請同學補交作業，較不適當的處理方式是？在群組中公布未交作業學生姓名與學號
8. 將含有學生資料的 Excel 檔放入 USB 前，較適當的作法是？評估是否必要，並採取加密與妥善保管措施

©2025, BCCS. All rights reserved.

考前抱佛腳~~3

9. 使用生成式 AI 協助整理資料前，最重要的優先作法為何？先確認資料是否含可識別個資，並去識別化或移除非必要欄位
10. 下列哪一項最不適合直接輸入未經核准的外部生成式 AI 工具？含姓名、學號與完整成績的學生 Excel 檔
11. AI Agent 與一般生成式 AI 相比，何者是需要特別注意的風險？AI Agent 可能串接 Email、雲端或系統並自動執行動作
12. 若要讓 AI Agent 協助處理校務工作，最合適的權限設計原則為何？依工作需要給予最小必要權限，並保留操作紀錄

©2025, BCCS. All rights reserved.

考前抱佛腳~~4

13. 發現 Email 誤寄含有學生個資的附件時，第一個正確原則為何？先停止擴散並立即通報主管與校內窗口
14. 發生疑似個資外洩時，下列何者不適當？為避免被追查而刪除系統紀錄
15. 為何個資外洩時需要保留證據？便於確認事件範圍、調查原因與採取補救措施
16. 下列哪一種資料通常需要較高強度的保護措施？學生健康、輔導或特教需求資料

©2025, BCCS. All rights reserved.

考前抱佛腳~~5

17. 個資事故中，「通知當事人」的主要目的為何？讓當事人能知道事件情況並採取保護措施
18. 委外廠商協助維護校務系統時，學校較適當的管理作法為何？以契約或管理要求規範用途、權限、保密、通報與刪除機制
19. 下列何者最能降低誤寄個資附件的風險？寄送前核對收件人、CC / BCC、附件內容與檔案版本
20. 下列何者最符合個資保護的核心做法？只蒐集必要資料、限制必要人員使用，並在不需要時妥善刪除或銷毀

©2025, BCCS. All rights reserved.