

那些年，我們不小心洩漏的個資

呂思瑩



課程大綱

1

原來這也是個資？

- 個資法定義與特種個資
- 核心法規義務與違規後果
- 破冰小測驗：哪些算個資？
- 三個真實校園案例解析

2

好心，居然辦壞事情

- 身分核實與電話詢問
- 榜單公告的馬賽克藝術
- Email 群發的 CC/BCC 地雷
- 紙本文件的流浪問題
- Google 表單的後遺症

3

急救與防護包

- 社交工程威脅識別
- 帳號借用的法律炸彈
- 未加密網路的風險
- 法律責任為何無法免除
- 外洩緊急應變 SOP

⊗  **個資法更新提醒：**114年11月11日已公布個資法修正版，主要新增：

- ①個人資料保護委員會(個資會)成立，統一監管機關；
- ②公務機關(含學校)須設「個資保護長」；
- ③外洩通報罰則強化，非公務機關未通報最高罰 20 萬元，可按次處罰。

原來這也是個資？

校園裡的 隱形地雷



法規定義

個資法第2條、第6條核心條文
解析



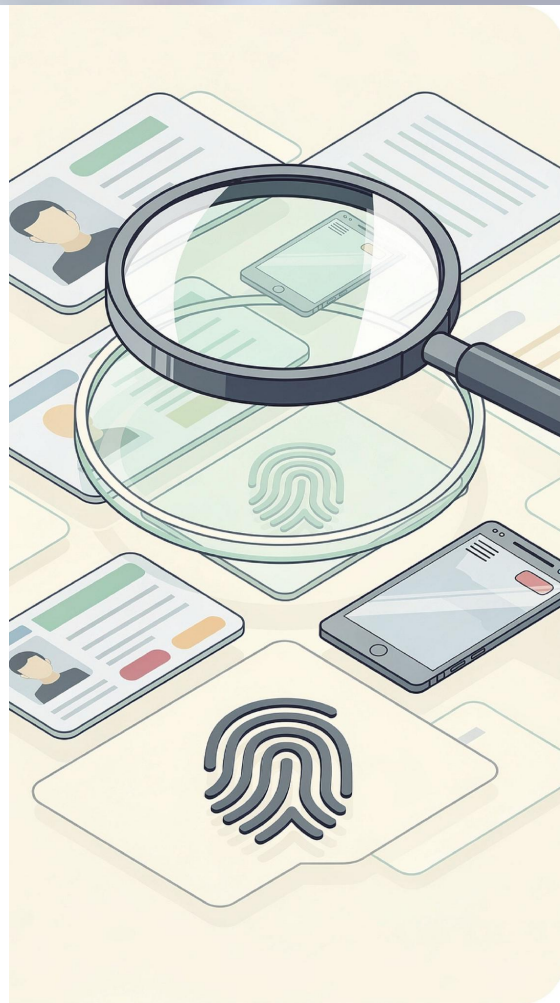
法定義務

蒐集三原則、當事人五大權利、通
報義務



案例解析

三個真實校園情境：成績單、社群媒體、筆電遺失



什麼是個人資料？

法律定義(個資法第 2 條)

指自然人之以下資料，以及其他得以直接或間接方式識別該個人之資料：

- 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

關鍵判斷原則

法律保護的核心不在於「資料類型」，而在於「識別可能性」：

- 只要「能直接或間接識別出特定個人」，就是個資，不限於姓名或身分證字號。

校園常見個資類型

- 學生成績、請假原因、家庭狀況
- 緊急聯絡人、健康聲明書
- 學生照片、學號

特種個資： 保護等級最高的敏感資料

個資法第 6 條特別列出以下六類「特種個資」，原則上**不得蒐集、處理或利用**，違反者法律責任更重。

病歷

醫療

基因

健康檢查

犯罪前科

性生活



學校應遵守的核心法規規定

蒐集三原則 (個資法第5條)

1. **尊重當事人權益**
——以誠實及信用方法為之
2. **不得逾越特定目的之必要範圍**
——只蒐集真正需要的資料
3. **與蒐集目的須有正當合理關聯**
——目的與資料類型必須相符

當事人五大權利 (個資法第3條)

學生與家長均可主張以下權利，且**不得預先拋棄或以特約限制**：

1. 查詢或請求閱覽
2. 請求製給複製本
3. 請求補充或更正
4. 請求停止蒐集、處理或利用
5. 請求刪除

外洩通報義務 (個資法第12條)

知悉個資被竊取、洩漏、竄改時，應**立即通知當事人** 並向主管機關申報。



不得隱匿

延遲通報本身即構成違法，情節嚴重者加重處罰。

違規後果一覽

餐廳生意太好，天天客滿，大家請老闆登記並依序通知、安排入座

⇒ 特定目的是 候位、通知

學校要讓學生使用選課系統選擇課程

⇒ 特定目的是 選課、聯繫、人數控管

違規後果一覽

刑事責任

個資法第 41-46 條

- 最重 **5 年**有期徒刑
- 罰金最高 **100 萬元**
- 「意圖營利」列為加重處罰條款

民事賠償

個資法第 28-31 條

- 每人每一事件：**500 元至 2 萬元**
- 同一事件賠償總額上限：**2 億元**
- 受害人不須證明實際損害即可求償

行政罰鍰

個資法第 25、47-50 條

- 一般情節：**2 萬至 50 萬元**
- 情節重大：最高 **1,500 萬元**
- 學校與負責人 **可併罰**，雙重處分

修法動態 (114 年 11 月 11 日公布)

- **新設「個人資料保護委員會(個資會)」**：統一監管所有公務機關與非公務機關，學校亦在管轄範圍 內
- **公務機關須設「個資保護長」**：由機關首長指派人員兼任，負責統籌推動個資保護事務(修正第 18 條)
- **外洩通報罰則強化(修正第 12 條)**：須採取即時應變措施、記錄事故影響、保存紀錄；非公務機關未依規通報者，罰鍰 2 萬至 20 萬元，可按次處罰

這些到底算不算個資？（上）

判斷關鍵：不只身分證字號才算個資 —— 只要「能直接或間接識別出特定個人」，就受個資法保護。



學生車牌



Line 頭貼

這些到底算不算個資？（上）

判斷關鍵：不只身分證字號才算個資 —— 只要「能直接或間接識別出特定個人」，就受個資法保護。

✓ 學生車牌——算！

車牌號碼可透過監理系統反查車主身分，屬於「間接識別個人」的資料，受個資法保護。

即使只是停車場管理或接送紀錄，記下車牌就等於記下個資。收集車牌需有明確的蒐集目的，且須告知當事人。

✓ Line 頭貼——算！

頭貼含有個人影像，屬於「特徵」類個資；若頭貼清晰可辨識本人，更具直接識別性。

截圖或轉傳頭貼均可能構成個資的非法利用 —— 即使是在工作群組中分享，也須注意。

這些到底算不算個資？（下）

個資保護義務不因當事人畢業、離職或資料曾公開而消失。



生病請假理由



畢業校友公司分機

這些到底算不算個資？（下）

個資保護義務不因當事人畢業、離職或資料曾公開而消失。



生病請假理由——算！且屬特種個資

病因屬於**健康資訊（特種個資）**，保護等級最高，不得隨意揭露或留存。

請假單不應放在辦公桌上——連辦公室同事也不應知悉學生的病情。收到請假單後應立即鎖入有鎖抽屜。



畢業校友公司分機——算！

分機號碼結合姓名或部門，可連結至特定個人，仍屬個資範疇。

個資保護義務不因當事人畢業或離職而消失，校方仍須依規定妥善保存或依期限銷毀相關資料。



常見迷思：「當事人已經畢業了，這些資料沒關係吧？」

——錯。個資的蒐集目的消失後，應依規定期限銷毀，不得無限期保存。

為什麼我們該在意？

個資保護的核心是人的**尊嚴與安全**，法律責任只是最後的防線。理解為何重要，才能真正落實保護。



對學生的影響

個資外洩可能導致騷擾、詐騙，甚至人身安全風險。學生的健康狀況、家庭背景、成績資訊一旦外洩，可能成為霸凌、歧視的依據，造成難以挽回的心理傷害。



對學校的影響

損害機構信譽，面臨主管機關調查與裁罰。一起個資事件足以引發媒體關注、家長聯署、主管機關介入，對學校公信力造成長期損害。



對個人的影響

個人可能承擔行政或刑事責任。**「奉命行事」不能免責**——法律要求的是每位接觸個資的人員都盡到保護義務，長官的指示不能作為違法的擋箭牌。



案例一：成績單群發事件

真實情境模擬



案例狀況

某國中行政人員以 Email 寄送期末成績單，誤將全班 30 名學生的成績以「副本(CC)」群發給所有家長。每位家長都看到其他孩子的成績，校方遭家長聯署投訴並移送個資保護主管機關調查。



問題核心

操作者不了解 CC 與 BCC 的功能差異，且寄出前未經第二人確認。**一個操作失誤，影響 30 個家庭**，30 位學生的成績資料同時暴露在其他家長面前。

- CC(副本)= 所有收件人互看彼此信箱與內容
- BCC(密件副本)= 各自收信、互不知情



建議改善

- 群發含個資的信件一律改用 **BCC**
- 建立「寄出前雙人確認」機制，由同事覆核收件清單與附件內容後再送出
- 考慮採用學校官方通知系統，避免以個人信箱群發

案例二：社群媒體貼文事件

真實情境模擬



案例狀況

某高中教師將學生優秀作文拍照上傳 Facebook 公開表揚，未遮蔽學生姓名與班級。遭家長以違反個資法向學校檢舉，教師須接受懲處並公開道歉。



問題核心

以「表揚美意」為由，忽略當事人的**知情同意權**。公開平台的觸及範圍遠超課堂，風險遠高於預期：

- Facebook 貼文可能被轉發、截圖，控制範圍幾乎為零
- 即使出於好意，未經同意的揭露仍構成個資法違規
- 「學生的作文是好事」不等於「可以公開學生身分」



建議改善

- 張貼學生作品前須取得**本人與家長書面同意**
- 若無同意，須遮蔽姓名、班級等所有可識別資訊後才可公開
- 建議採用學校官方公告管道（告示欄、校內系統），控制觸及範圍

案例三：筆電遭竊事件

真實情境模擬



案例狀況

某大學行政人員將含有全系學生健康聲明書的資料夾存入私人筆電帶回家加班，筆電於通勤途中遭竊。**逾200名學生個資(含病史、緊急聯絡人)**面臨外洩風險，校方須逐一通知當事人並向主管機關申報。



問題核心

- 公務個資存於 **未加密的私人設備**，一旦設備遺失即無任何防護
- 「帶回家加班」的習慣讓個資 脫離學校的安全管控範圍
- 健康聲明書屬特種個資，保護義務更高，卻以最不安全的方式儲存



建議改善

- 個資文件 **僅存於學校核可的加密設備或雲端系統**
- 如需遠端作業，應使用學校VPN 連線，禁止複製至私人裝置
- 筆電、USB 隨身碟等設備存有個資時，務必啟用全碟加密

新聞報導的校園個資事件

事件一：7 所高中校務系統遭駭（2024 年 3 月）

駭客透過亞昕資訊系統漏洞入侵 7 所高中，竊取逾 2 萬筆學生個資（含身分證號、家長手機、住址），並在美國暗網 BreachForums 公開販售。教育部依個資法第 12 條啟動通報程序，逐一通知受害學生。

關鍵教訓：第三方廠商的系統漏洞，學校仍須承擔通報義務；個資一旦外洩，無法收回。

來源：中央社 2024.03.30

事件二：桃園國小校長洩漏性平案件個資（2024 年 5 月）

某國小校長為澄清外界質疑，在全校教師週會公開洩漏學生性平案件資訊，導致學生遭社區排擠、逃家、自傷，衍生兩起校安事件。監察院糾正桃園市教育局，校長被處罰鍰 3.5 萬元並記申誡，並重新評估適任性。

關鍵教訓：「澄清誤解」的善意，不能成為洩漏個資的理由；性平案件資訊屬最高保密等級。

來源：中央社 2024.05.17

校園日常的 5 大「好心辦壞事」情境

1

身分核實

電話查詢學生資料

2

榜單公告

該遮與不必遮的邊界

3

Email 群發

CC 與 BCC 的致命差異

4

紙本文件

請假單與健康聲明的流浪

5

線上表單

Google 表單的可怕後遺症

老師，我是小明的媽媽，他成績怎樣？



日常場景

電話鈴響，對方自稱是某學生家長，語氣親切地詢問孩子本學期成績、出缺席狀況，甚至要求提供導師聯絡方式。你無法確認對方身分，但對方說得頭頭是道。



風險核心

電話、Line 訊息、當面詢問均**無法核實身分**——冒充家長索取資料的詐騙案例真實存在。一旦提供，即構成個資違法利用，**「我以為是真的家長」不能免責**。

延伸情境

外系教授、實習單位主管、媒體記者來電要求提供學生資料，同樣不得直接給予，須走**正式申請程序**。



安全做法

- 請對方透過學校官方系統（家長帳號）自行查詢
- 若需當面確認，請出示證件並由**學生本人在場同意**
- 任何電話查詢學生資料的要求，一律婉拒並說明正式管道



委婉話術

「為保護您孩子的個人資料安全，我們需要先透過系統核實身分，請問您方便登入家長平台嗎？」



這句話不是拒絕家長，而是保護學生——也是保護你自己。

榜單與得獎名單的「馬賽克」藝術

期末獎學金榜單、得獎公告 —— 哪些欄位 **必須遮蔽**，哪些可以公開？邊界比你想像的更清楚。

要遮蔽的資訊

- 身分證字號(含末幾碼)
- 出生年月日
- 聯絡方式(電話、信箱)
- 銀行帳號(含末幾碼)
- 不必要的班級座號
- 家庭狀況說明

不必遮蔽的資訊

- 姓名(公告目的明確、當事人知情且與得獎直接相關時)
- 得獎項目、獎學金額

常見錯誤

錯誤 1: 只遮名字卻保留學號 —— 學號可透過學校系統反查出個人，遮了等於沒遮。

錯誤 2: 將含有完整個資的榜單截圖傳入 Line 群組 —— 傳出去即無法控制擴散範圍，且群組成員均成為個資的「接收者」。

安全做法

公告前由 **主管逐欄確認** 哪些欄位屬必要資訊，其餘一律遮蔽或刪除後再公告。

全校大放送的 Email 災難

CC vs BCC 一秒搞懂

CC(副本) = 所有人互看信箱, 彼此知道誰收到了這封信

BCC(密件副本) = 各自收信、互不知情, 保護每位收件人隱私

✖ 群發通知一律用 BCC。

附件地雷

寄出前確認附件是否為正確版本、是否含有非必要欄位(如身分證字號、薪資、病史)。

兩個常見災難場景

場景 A: 行政人員寄送全校教職員通知, 用 CC 一次加入 200 個信箱, 所有人都看到彼此的 Email, 其中包含兼任教師、約聘人員的私人信箱。

場景 B: 將含有學生名單的 Excel 附件誤寄給全班家長, 附件內還有其他班級的資料; 或主旨直接寫「○○同學輔導追蹤名單」, 光看主旨就洩漏敏感資訊。



發信前 SOP(四步驟)

1. 收件人是否正確?(姓名、信箱逐一核對)
2. 附件內容是否已去除多餘個資?
3. 主旨是否洩漏敏感資訊?
4. 請同事覆核後再按送出

學生請假單與健康聲明書的流浪記

1 請假單堆在辦公桌角落

上面寫著「因憂鬱症就醫」、「家人住院需陪同」等敏感原因，路過的同事、學生、家長都可能看到。這些是**最高等級的特種個資**，應收到即鎖入有鎖抽屜。

2 健康聲明書翻面當廢紙使用

含有學生病史的那面就這樣在辦公室流傳；或直接丟入一般回收桶，清潔人員整理時一覽無遺。**禁止翻面再用或丟回收桶**——唯一正確做法是碎紙機銷毀。

3 紙本文件放在公用印表機旁等待取件

成績單、輔導紀錄表被其他人誤拿或看見。列印含個資的文件應**立即取件**，不得離開印表機後才去拿。

❏ 關鍵心態：「這只是一張廢紙」——但對當事人來說，那是他最私密的**健康或家庭資訊**。

紙本個資的處理，與數位個資一樣重要。

好方便的Google表單 好可怕的後遺症

三個常見的災難場景

場景 A: 用個人 Google 帳號建立報名表，收集學生姓名、電話、身分證字號、飲食禁忌(含宗教或健康因素) **活動結束後表單繼續開著，一年後仍有 300 筆資料躺在雲端。**

場景 B: 表單設定為「任何人可檢視回應」，學生填完後點選查看先前的回應，看到所有人的個資；或表單連結被轉傳到校外群組。

場景 C: 用 Line 群組直接請家長回覆孩子的健康狀況，訊息在群組中對所有成員公開可見。



活動後必做清單

1. 關閉表單接受新回應
2. 下載回應備份至學校核可的加密系統
3. 刪除表單中的所有回應
4. 確認表單權限設定為「僅限特定人員」

建立制度

- 每次活動結束後**X天內**完成個資清理，並由主管確認
- 禁止以個人帳號建立含敏感個資的表單
- 含特種個資(健康、宗教)的蒐集，應使用學校官方系統

不小心踩雷了怎麼辦？

急救與防護包



社交工程

駭客不攻系統，攻人心 —— 辨識與防範偽裝攻擊



帳號借用

「幫個忙」背後的法律炸彈 —— 責任隨帳號轉移



未加密網路

咖啡廳改成績的代價 —— 公共 Wi-Fi 的致命風險



法律責任

「我不是故意的」為何不能免責 —— 台灣法規的主動義務

社交工程

什麼是社交工程？

攻擊者偽裝成可信任的人(IT人員、主管、廠商)，透過電話、Email 或 Line 誘騙你提供帳號密碼、點擊惡意連結，或開啟含有病毒的附件。

校園常見三大手法

- 「我是資訊組，系統要維護，請提供您的帳號密碼」——**正規 IT 人員絕不會這樣要求**
- 偽造學校公文 Email，要求點擊連結「更新個人資料」
- 假冒教育部或主管機關來電，要求提供學生名冊

⚖️ 法規責任

即使是被騙所導致的個資外洩，學校仍須依個資法第12條通報，且可能因「未採取適當安全維護措施」承擔行政責任。

❌ 「我被騙了」不能免責——法律要求的是預防措施，而非事後解釋。

✅ 防範原則

- 任何索取帳密的要求，一律要確認再確認
- 可疑 Email 不點連結、不開附件
- 可先電話核實寄件人身分再行動



帳號借用——幫個忙背後的法律炸彈

日常場景

- 教授請助教用**自己的帳號**登入系統代為輸入成績
- 行政人員請工讀生用**主管帳號**查詢學生資料
- 同事出差請你用**他的帳號**處理公文

為什麼不行？

- 系統操作紀錄會顯示「帳號擁有者」的名字，一旦出錯或外洩**法律責任由帳號擁有者承擔**
- 助教以教授帳號登入成績系統，若資料遭竄改或外洩，教授無法主張「不是我操作的」
- 帳號借用本身即違反**資通安全管理法**對存取控制的要求——資安法要求防止「未經授權之存取」



正確做法

需要他人代為操作，應申請「**授權帳號**」或「**代理權限**」，透過正式程序留下可追溯的操作紀錄；任何人不得以他人帳號登入系統。

帳號就像印章，借出去的那一刻，責任也跟著借出去了。

申請代理權限的步驟

1. 向系統管理員提出書面申請
2. 說明代理期間、代理範圍
3. 由主管核准後開通限時授權
4. 代理期結束後立即撤銷權限

未加密網路——咖啡廳改成績的代價

日常場景

- 在咖啡廳、捷運站、機場使用免費公共 Wi-Fi 登入學校系統處理學生資料
- 在家使用未設密碼的鄰居 Wi-Fi 上傳成績單
- 出差時連接飯店 Wi-Fi 存取學生個資

⚠ 風險核心

未加密的公共Wi-Fi, 同一網路上的任何人都可能**攔截你的傳輸內容**, 包含帳號密碼、學生個資、系統操作紀錄。公共場所的 Wi-Fi 多是開放網域, 是駭客竊取資料的最佳管道。

⚖ 法規責任

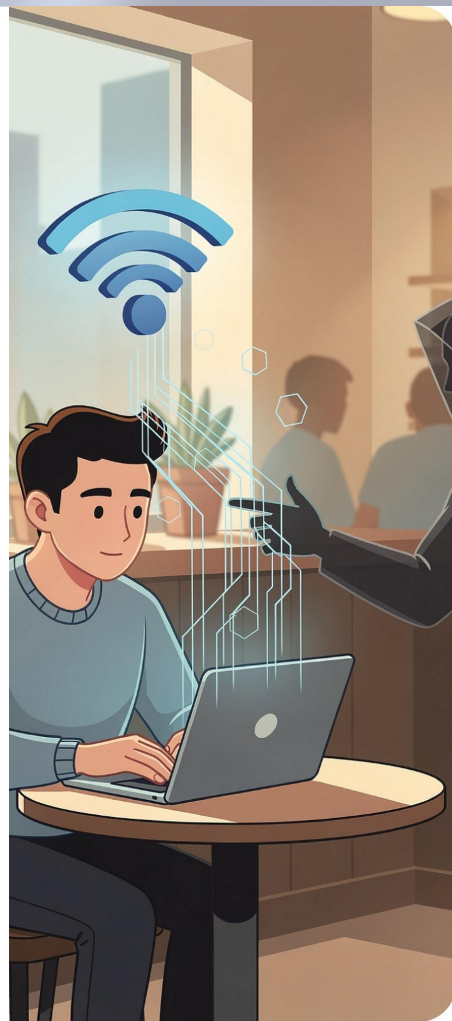
個資法要求機關應採取「適當安全維護措施」, 在不安全網路環境下處理個資, 即屬未盡安全維護義務, 導致外洩時不得以「不知道有風險」為由免責。

安全三原則

- **禁止**: 在公共 Wi-Fi 下登入學校系統或處理個資
- **必要時**: 使用學校核可的 VPN 建立加密連線後再操作。連到有「https」的網站, 或透過 VPN(虛擬私人網路)來建立安全連線。
- **最安全**: 使用手機行動網路(4G/5G)熱點, 避開公共 Wi-Fi



如何判斷網址是否安全? 確認瀏覽器網址列顯示「https://」, 有鎖頭圖示即為加密連線。



「我不是故意的」 ——為何台灣法規不讓你免責？

台灣法律對個資保護採取**主動義務**架構，不是「沒有惡意就沒有責任」，而是「**未盡防護義務就有責任**」。

個資法第 5 條：安全維護是主動義務

蒐集、處理、利用個資，應「依誠實及信用方法」並採取適當安全措施。法律要求的是**主動預防**，而非「出事後才補救」——未採取防護措施本身就是違法。

個資法第 12 條：外洩即須通報，不得隱匿

無論外洩原因是社交工程、帳號借用或網路攔截，一旦知悉即須通報當事人與主管機關。**「我是被騙的」不影響通報義務**，延遲通報本身即另構成違法。

資通安全管理法第 28 條：人員個人須受懲戒懲處

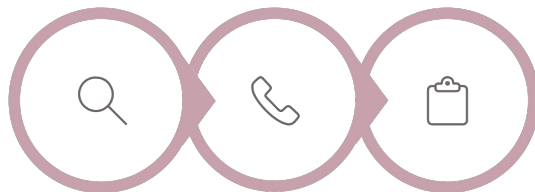
公務機關所屬人員（含教職員、行政人員）未依規定辦理資安事項，應按情節輕重予以**懲戒或懲處**，責任落在個人身上，不因「長官指示」或「不知情」而免除。

資通安全管理法第 33 條：資安事件涉及個資，雙法並行

資安事件若同時造成個資外洩，**須同時適用個資法與資通安全管理法**，兩套法律責任疊加，罰則加重。

萬一真的外洩了，第一時間該怎麼做？

不要自己偷偷解決！私下處理只會讓情況更糟，並加重個人責任。延遲通報本身即另構成違法。



確認範圍 立即通報 配合調查

步驟一：

確認外洩範圍

- 哪些資料外洩？(類型、數量)
- 影響哪些當事人？(學生、教職員)
- 外洩原因為何？(設備遺失、誤寄、駭客入侵)
- 外洩時間點為何？

步驟二：

立即通報主管與窗口

- 聯繫學校個資保護窗口或資訊安全負責人
- 不得自行決定是否通報，應由主管判斷後續處理
- 依個資法第 12 條，知悉後應**立即**通知當事人

步驟三：

配合調查並記錄

- 保留所有相關操作紀錄、通訊記錄
- 配合主管機關調查，如實說明經過
- 記錄處理過程，作為後續改善依據

3個護身符



螢幕上鎖快捷鍵

Windows: Win + L

Mac: Ctrl + Command + Q

離座前按一下，三秒保平安。即使只是去倒水，也養成上鎖的習慣——辦公室內部人員也可能是洩漏風險。



密碼不寫在便利貼

使用密碼管理工具，或設定好記又安全的通行密語。

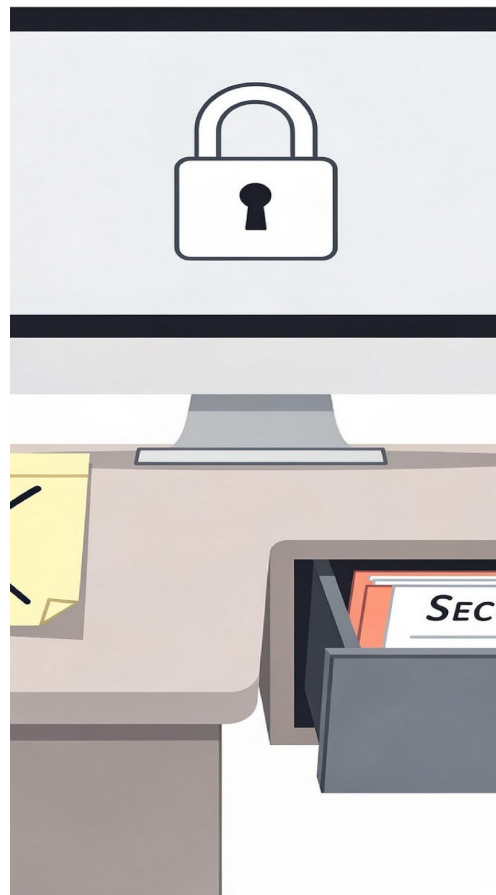
不要使用姓名、生日、電話號碼作為密碼，也不要多個帳號共用同一組密碼。



離開座位收好文件

含個資的紙本文件**不留桌面**，鎖入抽屜或歸檔。

含個資的電子檔案不存於桌面或未加密的隨身碟，存至學校核可的加密系統或有權限管控的資料夾。



QA 時間

今天的 3 個關鍵字

識別

保護

通報



有任何疑問，現在提出來
一起討論！

參考法規與資料來源

個人資料保護法－全國法規資料庫

<https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021>

個人資料保護法§48
相關法條－全國法規資料庫

<https://law.moj.gov.tw/LawClass/LawSingleRela.aspx?FLNO=48&PCODE=I0050021&ty=L>

如何適用個資法－個人資料保護委員會

[下載 PDF 文件](#)

資通安全管理法（修正日期：民國 114 年 09 月 24 日）

[下載 PDF 文件](#)

桃園國小校長洩漏性平案個資釀校安事件（2024年5月）

[中央社報導（2024.05.17）](#)

7所高中校務系統遭駭、學生個資暗網販售事件（2024年3月）

[中央社報導（2024.03.30）](#)

感謝出席！

期待未來再次相會，共同守護校園個資安全。