



下班前的個資保衛戰！

最容易發生失誤的時刻，往往就在趕著收尾的「下班前三分鐘」。這堂課專為每天與文書、表單、數位群組奮戰的行政同仁設計。不談大理論，直接切入您每天都在用的辦公工具。

課程說明

個資保護聽起來很嚴肅，但其實不必神經緊繃。只要稍微改變一點數位習慣，就能把危機擋在門外。這門課設計給每天要處理表單、文件、群組訊息的行政同仁——語言輕鬆、步驟實用，讓您從此安心下班、不再半夜驚醒！



第一小時

**建立直覺！看懂身邊的資料
分類**

辦公室風水學與個資紅綠燈
分類法



第二小時

數位工具的安全使用手冊

LINE群組、雲端硬碟、釣魚信
件全攻略



第三小時

辦活動與招生的個資懶人包

報名表設計、數位大掃除、情
境模擬



下班前三分鐘，是最危險的時刻

您有沒有這樣的經驗？快下班了，急著把報名表 E-mail 出去，結果夾帶了錯誤的附件；或是匆匆忙忙把名單丟進 LINE 群組，才發現傳給了不相關的人。

根據資安研究，**超過六成的個資外洩事件** 並非來自駭客攻擊，而是來自內部人員在疲勞或倉促狀態下的操作失誤。行政同仁每天接觸大量個資，一個小習慣的疏漏，就可能造成當事人的重大損害，也讓學校面臨法律責任。



個資法第28條：非公務機關違反個資法，導致當事人損害，可處新台幣2萬至200萬元罰鍰。

建立直覺！

看懂身邊的資料分類，是做好個資保護的第一步。

什麼是「個人資料」？

個資保護法所稱的個人資料，是指「**可以直接或間接識別特定自然人的資訊**」。這個定義比您想像的廣泛得多。



直接識別型

姓名、身分證字號、護照號碼、生日、照片——這些資料單獨存在，就能直接指向某個人，屬於最需要嚴格保護的類別。



間接識別型

學號、手機號碼、電子郵件、IP位址——單獨看似沒什麼，但結合其他資訊就能鎖定到特定個人，同樣需要謹慎處理。



特種個資

醫療、病歷、心理輔導紀錄、宗教信仰、政治傾向、前科——這類資訊受到個資法特別保護，原則上**禁止蒐集**，除非有明確的法律依據。



辦公室常見誤解：「學生的班級、學號又不是秘密，貼公告沒關係。」
——但學號結合成績，就構成受保護的個資組合！ $1+1 >> 2$

蒐集個人資料前，必須做到的事

《個人資料保護法》第8條規定，蒐集個資前必須告知當事人特定事項。這不只是法律要求，也是讓對方安心配合的好方法。

1

說明蒐集目的

「我們蒐集您的資料，是為了辦理本次研習活動的報到與聯絡之用。」——必須具體說明，不能用「業務需要」這種模糊字眼含糊帶過。

2

說明利用範圍

資料會在哪個單位內使用？會不會分享給外部廠商？使用期間多久？這些都要明確告知當事人。

3

告知當事人的權利

當事人有權查詢、閱覽、補充、更正、停止蒐集或刪除自己的個資。表單上必須留下聯絡窗口，方便行使這些權利。

4

取得同意

非必要情形下，蒐集個資需取得當事人書面或可查驗的同意。電子表單可在送出前加入「我已閱讀並同意個資蒐集說明」的勾選框。

特地目的

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

基於這個特定目的，蒐集的個人資料有哪些？

⇒ 個人資料 姓名、電話、郵件 (?)、社群帳號 (?)、生日 (?)....



資料的紅綠燈分類法

● 紅燈 | 絕對機密

身分證字號、低收入戶證明、
心理輔導紀錄、醫療病歷

只在必要時使用，建議用完立即
銷毀。

● 黃燈 | 限閱資料

學號、成績單、聯絡電話、
宿舍門牌

控管閱覽權限，不隨意分享。

● 綠燈 | 可公開

校網公告、活動海報、辦公室電話
可自由分享。

紅燈資料：絕對機密，嚴格把關



身分識別核心資料

身分證字號、護照號碼、健保卡號——加密存放，不建議明文出現。



社會福利與弱勢資料

低收入戶、原住民身分、身心障礙手冊——單獨存放，不得與一般名冊合併。



心理健康與輔導紀錄

諮商紀錄、危機事件記錄——特種個資，原則上禁止蒐集，誤收須立即通報。

黃燈資料：限閱，不隨意分享

常見黃燈資料

- 學號(可直接查詢完整學籍資料)
- 成績與修課紀錄(涉及個人學習隱私)
- 宿舍房號與個人聯絡電話
- 家長姓名與聯絡方式(涉及第三人個資)
- 請假紀錄、缺曠課統計
- 校外實習單位與聯絡人(涉及個人職涯與去向資訊)

黃燈資料是行政業務中最常見的類型，也最容易因「習以為常」而降低警覺。單筆資料看似無害，但一旦組合起來就具有強烈識別力

例如**學號＋姓名＋宿舍房號** 三項並列，就足以精準定位到某位同學。

黃燈資料的建議處理方式



傳送前確認群組成員

只有業務需要的人才能看到，否則改用私訊，不在大群組廣播名冊。



電子郵件最小必要原則

只寄給真正需要的人，副本不隨意加人。



印完立刻取件

暫離座位時，將文件翻面或放入抽屜，避免旁人瀏覽。



共用電腦存加密資料夾

用完即刪，不留明文檔案在桌面。



公開場合謹慎開口

先環顧四周，確認無關人士不在場再討論。



外部索取先問授權依據

不因對方態度急迫就跳過確認步驟，先問清楚法律授權依據。

實體辦公室的「風水學」

個資外洩不只發生在數位世界。辦公室的實體環境，同樣是資安的重要防線。有時候，一個來辦事的學生、家長，甚至外包廠商，就能從您的桌面上讀到不該被看見的資訊。

- ❏ 「桌面淨空」不只是整潔習慣，更是個資保護的第一道防線。



桌面淨空運動：讓資料不外露

訪客在窗口等候時

桌面上若擺著其他學生的申請表、獎學金名冊或成績單，一眼就能被看見。建議在接待訪客時，養成習慣將當前處理的文件翻面或蓋上，並確保螢幕不正面朝向訪客。

離開座位前(含短暫離開)

去茶水間、上廁所、開會——這些「幾分鐘的空檔」是資料外洩的高風險時段。養成習慣：離開前把文件收入抽屜，電腦按下「Windows + L」鎖定螢幕。

共用辦公室或開放式空間

若您的座位位於走道旁或開放式隔間，桌面資料更容易被路過的人看見。可以使用螢幕防窺片，並將重要文件放入有蓋的文件盒而非直接堆疊在桌上。

印表機與碎紙機：兩個最常被遺忘的地方

印表機的正确使用

文件印出後立即取走，不要讓它在印表機上等您。多功能事務機的「暫存列印」功能（到機器前才輸入密碼放行）是保護資料最好的方式。共用印表機最容易發生「忘記拿走」的情況，請養成「印完立刻去拿」的習慣。



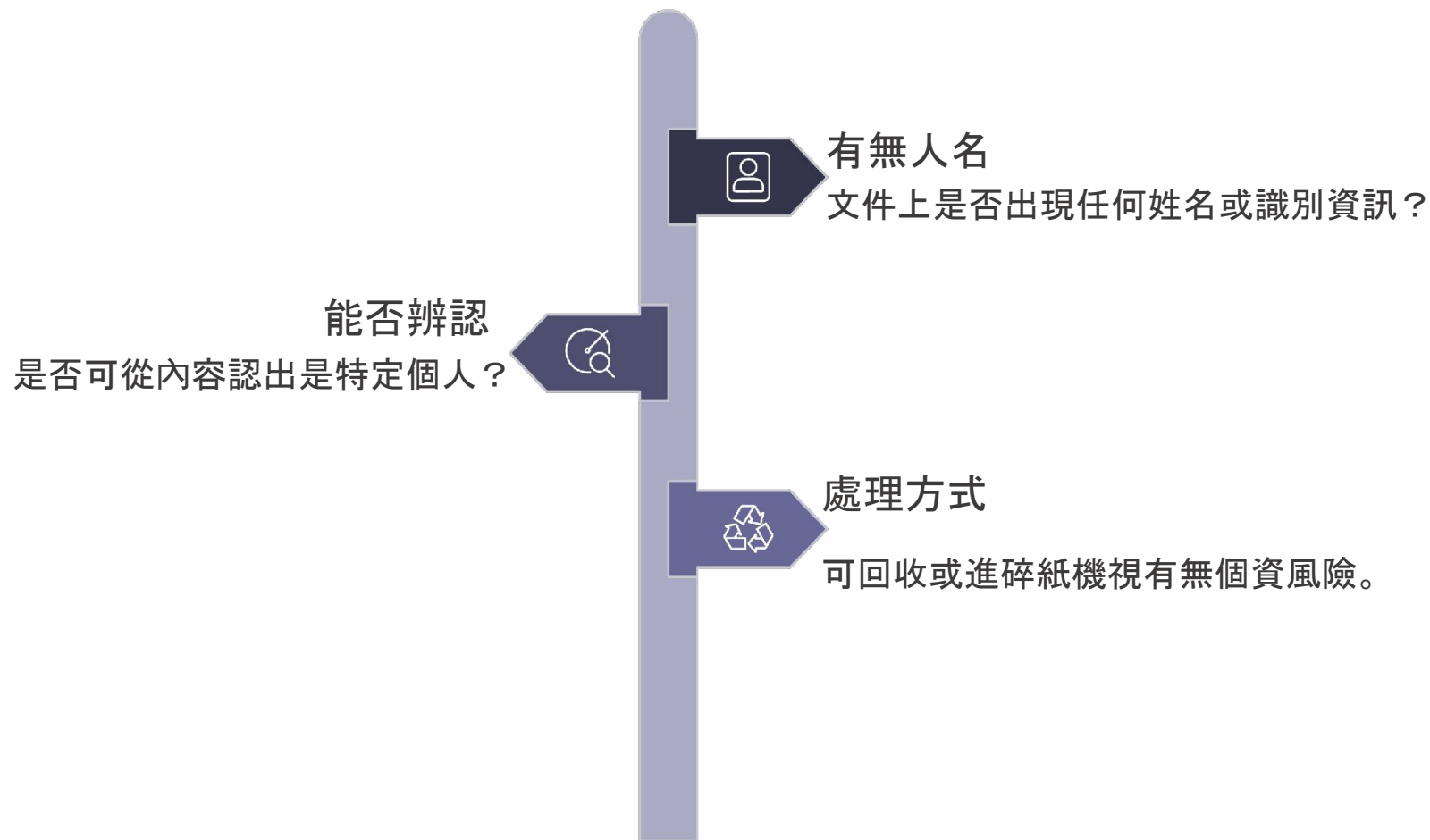
碎紙機的正确使用時機

含有個資的文件——包括印錯的版本、草稿、不需要的名單——必須過碎紙機，不可直接丟入回收箱或垃圾桶。碎紙等級建議使用「交叉碎紙」(Cross-cut)，而非直條碎紙，前者重組難度大幅提升。回收紙箱絕對不是個資文件的終點站！

⊗ 「這份文件有錯字，要重印一份。舊的丟回收就好。」——這是最常見的個資處理錯誤！印有個資的廢紙，一律送碎紙機。

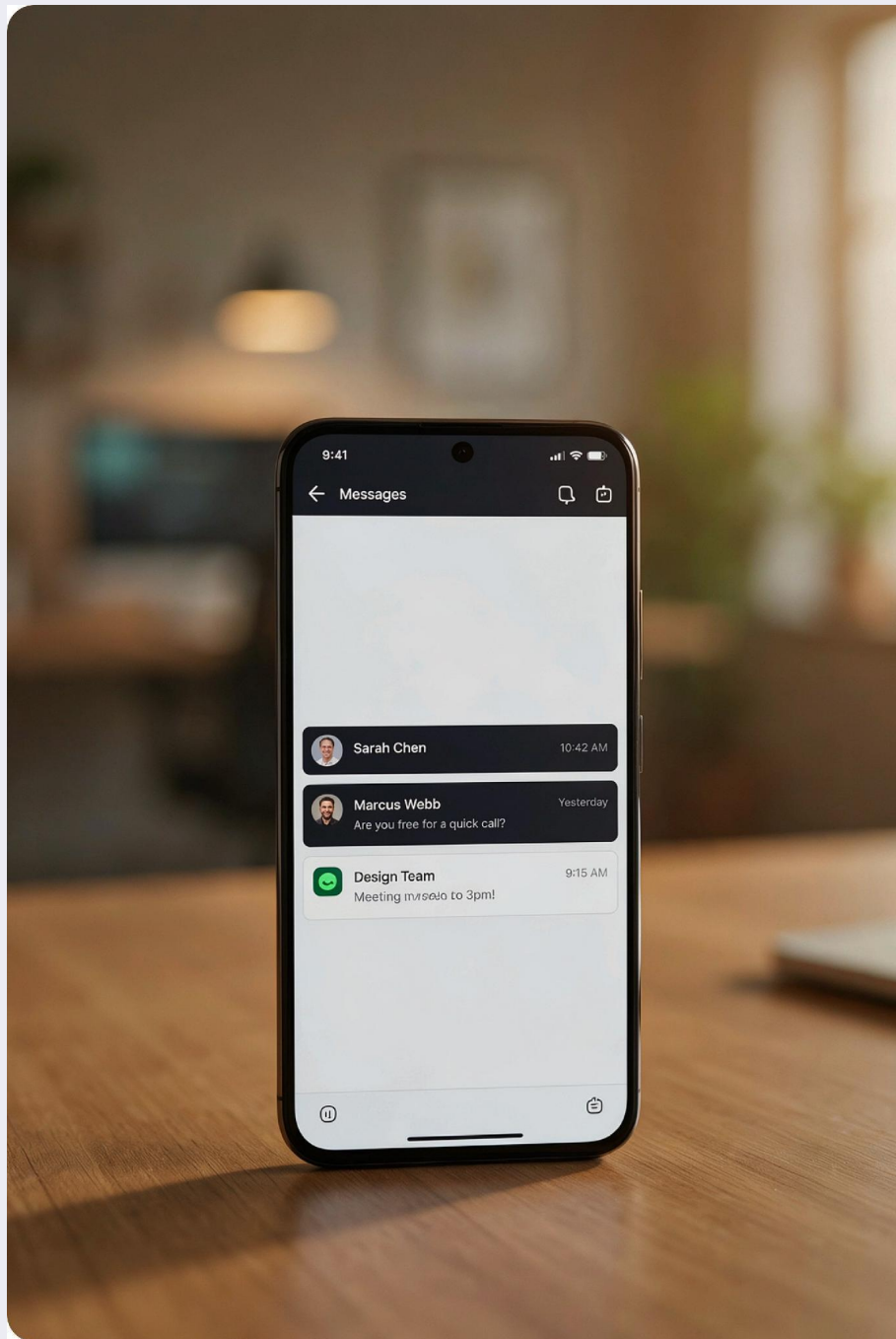
「這個可以丟回收嗎？」快速判斷三步驟

面對一張要丟棄的文件，不確定該進回收箱還是碎紙機，只要問自己這三個問題：



數位工具的安全使用手冊

LINE、雲端硬碟、電子郵件——您每天都在用的工具，也可能是個資外洩的入口。



LINE 公務群組的生存法則

LINE 是台灣職場溝通使用率最高的工具，公務群組裡傳出去的訊息，一旦送出就難以完全收回。

傳資料進群組前，先問自己兩件事

每次要把個資相關的內容貼到 LINE 群組之前，養成習慣停下來問自己這兩個問題。

❶ 這個群組裡的每一個人，都需要看到這份資料嗎？

群組往往隨著業務發展越加越多人，但清理的頻率卻很低。一個當初為了「辦活動」建的群組，可能至今還有已離職的同仁或已卸任的委員在裡面。**傳資料前，確認群組成員名單。**

❷ 這份資料用 LINE 傳，真的是最合適的方式嗎？

LINE 的訊息會在所有成員的手機上留下記錄，也可能被截圖轉傳。除了 LINE，沒有更適合的傳送方式了嗎？加密後採用電子郵件傳送？雲端硬碟開權限下載？

❏ 實用原則：LINE 適合傳「通知」，不適合傳「名單」。需要傳完整個資的情況，請改用有權限管控的管道。

截圖傳 LINE 可以嗎？

以下從幾個角度來思考截圖的合理性

截圖會複製原始資料的所有內容

如果您截圖的原始文件含有多個學生的個資，但您只想分享其中一筆，截圖仍會帶走整個畫面。務必在截圖前確認畫面中只有必要的資訊，或使用裁切工具後再傳出。

截圖一旦進入群組，就難以控管

任何群組成員都可以將截圖儲存到自己的手機相簿，再傳給其他人。即使您之後「收回」訊息，對方可能已經儲存了截圖。因此，凡是含有個資的截圖，請三思後再傳。

主管的「轉傳截圖」要特別小心

當主管轉傳一張截圖給您，請確認截圖中是否有附帶其他當事人的個資。若有，請不要再往下傳，並直接向主管確認處理方式。這不是不信任主管，而是正確的個資保護意識。

小心翻群與錯頻！最尷尬的個資事故

「翻群」是指在群組列表中不小心點到錯誤的群組就發出訊息；「錯頻」是指以為在私訊，結果發到了群組。這兩種錯誤看似小事，卻可能造成嚴重後果。

真實情境案例

- 把「弱勢學生名冊」傳進了全系學生群組
- 把「某生請假原因(含病情說明)」傳進了院辦群組
- 把對同事的私訊吐槽，發到了所有人都在的公務群組
- 把含有家長電話的聯絡清單，誤傳給家長本人的班級群

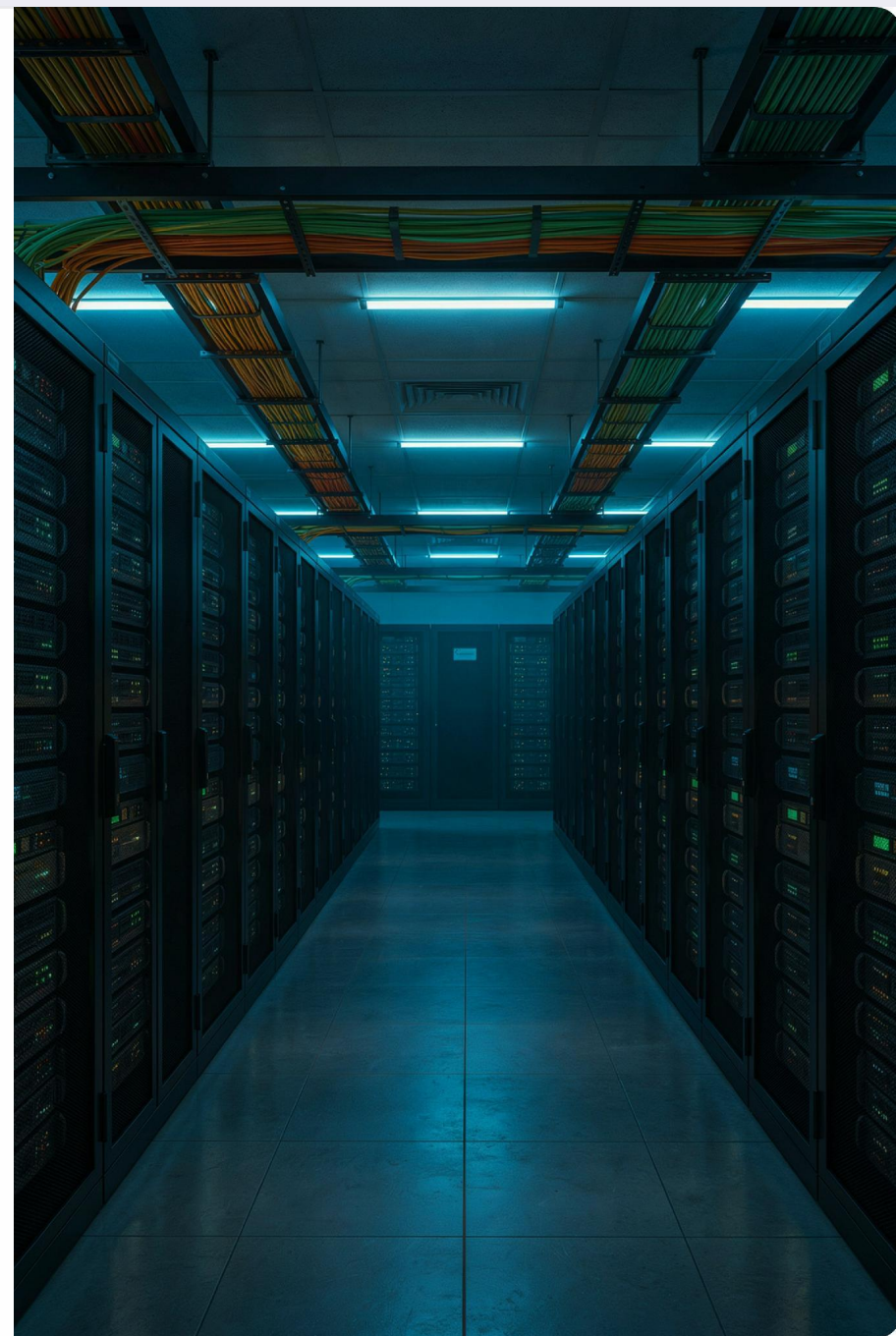
預防翻群的三個習慣

- **傳送前確認群組名稱**——養成「看清楚再按送出」的習慣
- **幫公務群組設置特殊標誌**——在群組名稱加上「公務」或換一個明顯的群組圖示
- **重要個資改用電子郵件**——郵件有收件人欄位可以再次確認，比 LINE 更安全

一旦發現傳錯，立刻收回訊息(LINE有短時間內可收回的功能)，並主動向主管報告、說明情況。

雲端硬碟與隨身碟的排雷術

Google 雲端硬碟、OneDrive、隨身碟——這些工具讓檔案分享變得前所未有的方便。但「方便」和「安全」之間，往往有一道很薄的界線，稍不注意就會踩雷。



雲端硬碟的權限設定：最常犯的三個錯誤

→ **✗ 錯誤一：**把分享連結設成「知道連結的人都能開啟」

這等於把文件放在網路上公開。任何人只要拿到這個連結（包括被截圖轉傳的連結），都能直接開啟文件。含有個資的文件，請務必改為「限指定人員」才能存取，並且只邀請有業務需求的人。

→ **✗ 錯誤二：**把所有人的權限都設成「可以編輯」

如果只是讓對方查看，請設成「檢視者」即可。「可以編輯」代表對方可以刪除、修改甚至覆蓋檔案內容。對多數接收者而言，「僅限檢視」就已足夠，不必多給不必要的編輯權。

→ **✗ 錯誤三：**活動結束後沒有收回或清除存取權限

一份三年前辦活動用的報名資料，至今可能還在雲端硬碟上被數十個人共享存取。定期清理雲端文件的共享名單，是「數位大掃除」的重要一環。個資不再需要時，應及時刪除或限縮存取。

檔案傳來傳去，到底哪個版本才是對的？

「最新版_final_v2_確認版_這個才對.xlsx」——相信這種檔名您不陌生。版本混亂不只讓人頭痛，更可能造成個資管理上的漏洞：舊版本裡可能有已被要求刪除的個資，散落在各人的電腦和信箱裡。

01

使用雲端協作，告別版本地獄

Google 試算表或 Microsoft 365 的 Excel Online 支援多人同時編輯，自動記錄版本歷史，再也不需要「傳來傳去」這個動作。一份文件，一個連結，所有人看到的都是最新版。

02

建立統一的命名規則

若仍需要以檔案方式傳遞，請在檔名中加入日期（格式建議：YYYYMMDD），例如「20250612_活動報名名冊.xlsx」。這樣可以輕鬆辨識版本先後，也方便日後清理舊版。

03

舊版本要主動刪除

確認新版本無誤後，主動通知相關人員刪除舊版，並自行清除信箱中的舊版附件。舊版文件中的個資，和新版一樣具有法律責任，請不要讓它們在角落默默存在。

實作教學：幫 Excel / PDF 加上密碼

這是最簡單、也最直接有效的個資保護動作之一。只要一分鐘，就能確保文件在傳輸過程中即使被截獲，對方也無法直接窺。以下是操作步驟：

Excel 加密步驟

1. 開啟您要加密的 Excel 檔案
2. 點選上方選單「檔案」
3. 選擇「資訊」→「保護活頁簿」
4. 點選「以密碼加密」
5. 輸入密碼並確認（建議8位以上，混合英數）
6. 儲存後，下次開啟就需要密碼

PDF 加密步驟(Adobe / 內建功能)

1. 在 Word 或 Excel 選擇「另存為 PDF」
2. 點選「更多選項」或「選項」按鈕
3. 找到「使用密碼加密文件」選項
4. 設定開啟密碼
5. 密碼請另行用電話或其他管道告知收件人



密碼請勿與加密文件用同一封郵件傳送！這樣等於沒加密。請用電話或另一封信告知密碼。

隨身碟：方便背後的風險

隨身碟輕巧方便，但在個資保護上是高風險設備。它可能遺失、被借走後忘記要回、插入不安全的電腦感染病毒。以下是使用隨身碟的安全建議：



公務與私人隨身碟分開

公務資料請使用專屬的公務隨身碟，不要和個人影音、私人文件混放在同一支。萬一遺失，至少可以限縮風險範圍。



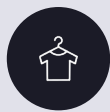
考慮使用加密隨身碟

市面上有支援硬體加密的隨身碟，插入後需輸入 PIN 碼才能存取。若您的業務需要經常攜帶個資外出，這類設備 值得投資。



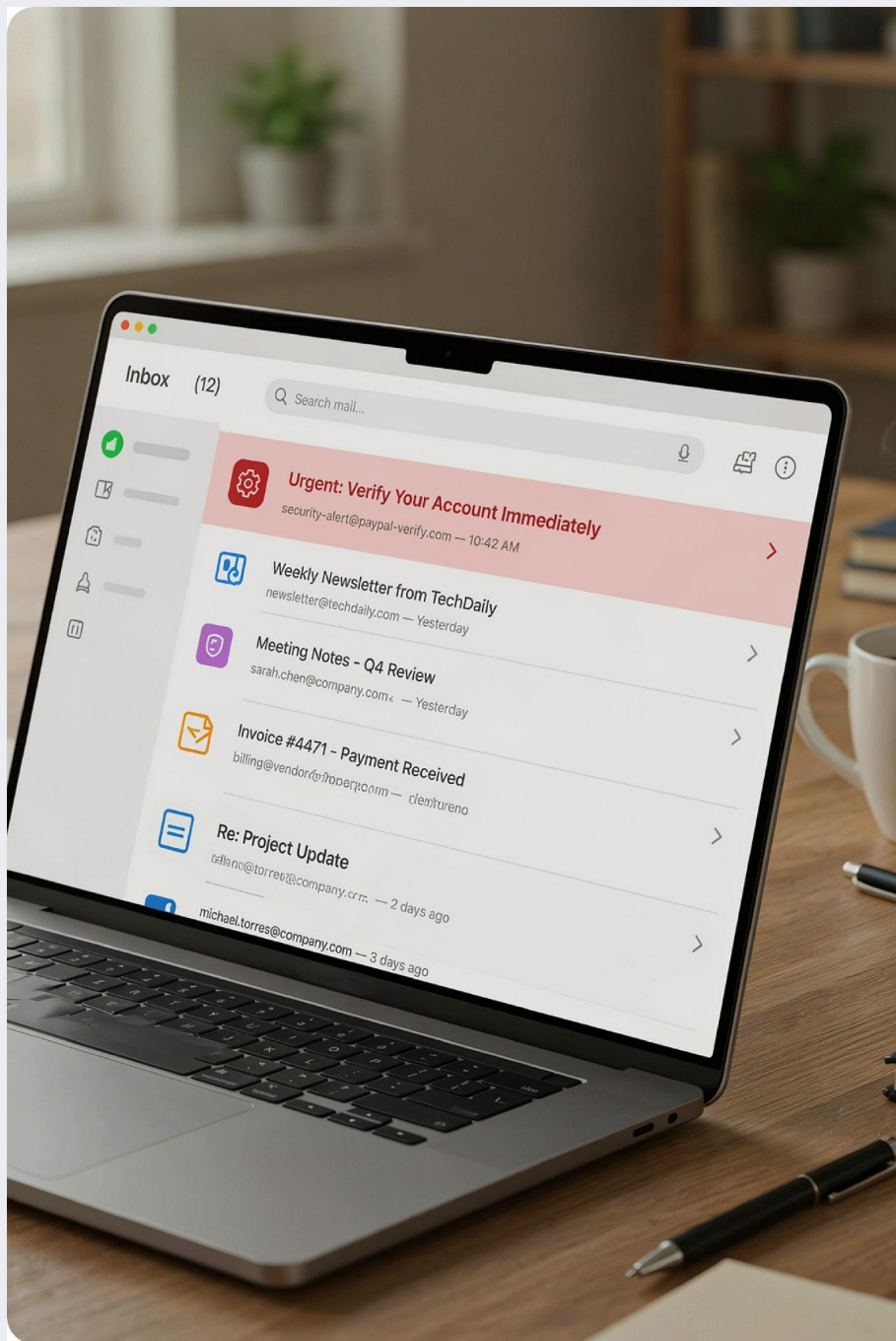
業務結束後清除資料

活動結束、學期結束後，請清除隨身碟中不再需要的個資檔案。「刪除」後記得清空資源回收筒，或使用安全刪除工具確保資料無法復原。



遺失時立即通報

如果含有個資的隨身碟遺失，請立即向主管及資訊安全單位通報，啟動應變程序。延遲通報只會讓後果更嚴重。



釣魚信件大破解

電子郵件是台灣機關最常遭受的資安攻擊管道之一。釣魚信件的设计越来越精緻，有時連資深的行政人員都會上當。認識釣魚信件的樣貌，是最重要的防禦動作。

最常見的三種釣魚信件劇本

釣魚信件通常利用「緊迫感」或「權威感」來促使您在沒有思考的狀況下點下去。認識劇本，就能識破騙局。

1

帳號緊急通知型

「您的校務信箱容量已滿，請立即點此連結驗證，否則帳號將在24小時內停用。」——這是最常見的釣魚手法，利用緊迫感讓您不假思索地點入假登入頁面並輸入密碼。**學校的 IT 部門不會用這種方式通知您。**

2

長官緊急委託型

「我是校長，現在在開會無法打電話，請你幫我去買 5 張 3000 元的 Google Play 點數，購買後把序號傳給我，費用之後核銷。」——這類信件假冒高層，利用下屬對上級的信任。**任何要求您購買點數的請求，100% 是詐騙。**

3

合作廠商假冒型

偽裝成您熟悉的廠商、銀行或政府機關，信件內容要求更新資料、確認訂單或查看附件。這類郵件通常模仿官方格式，乍看很像真的。**請從官方網站或您手中已有的聯絡方式另行確認，不要直接點信中的連結。**

一眼看穿釣魚信件的五個檢查點

您不需要成為資安專家，只要養成這五個快速檢查的習慣，就能過濾掉大多數的釣魚攻擊：

01

看寄件人的完整 Email 地址

顯示名稱可以偽造(例如顯示「IT 客服中心」)，但 Email 位址通常藏著破綻。把滑鼠移到寄件人名稱上，看看真實的位址是否為官方網域(例如 ntu.edu.tw)，還是一串奇怪的字母。

02

看連結的真實網址

把滑鼠停在信中的連結上(不要點!)，查看瀏覽器底部或浮現的真實 URL。如果顯示的網址和信件描述的來源不一致，就不要點。

03

感覺到「很緊急」就先停下來

釣魚信件的设计目的就是讓您不思考就行動。任何要求您「立即操作」的信件，都值得多花30秒確認真偽。緊急感是操控您的工具。

04

附件先別開，特別是 Office 文件

含有惡意程式的附件通常偽裝成 Word、Excel 或 PDF。如果您沒有預期收到這個附件，或寄件人不確定，請先聯絡寄件人用其他方式確認。

05

有疑問就通報，不要自己扛

如果您不確定一封信是否安全，轉寄給學校的資訊安全單位請求協助。通報一封假警報比誤點一封真釣魚信的代價小得多。

CLICKFIX 攻擊：最新的社交工程手法

近年出現一種新型態的釣魚攻擊手法，稱為「CLICKFIX」。它不是傳統的「點連結被導向假網站」，而是更狡猾的操作誘導方式。

CLICKFIX 的運作方式

攻擊者會讓您造訪一個看起來正常的頁面，頁面上出現一個錯誤訊息，例如「文件無法正常顯示，請按照以下步驟修復」。接著，頁面會要求您：

1. 按下 Win + R 開啟「執行」視窗
2. 貼上一段指令（由頁面提供，甚至自動複製到剪貼簿）
3. 按下 Enter 執行

這段指令通常會在背景下載惡意程式，竊取帳號密碼或植入遠端控制程序。

如何預防 CLICKFIX 攻擊

- **任何網頁要求您在電腦上執行指令** —— 直接關閉，這是 100% 的攻擊行為
- 不要從網頁複製貼上任何您看不懂的程式碼到「執行」或「命令提示字元」
- 如果真的遇到軟體問題，聯絡學校資訊服務台，由專業人員協助
- 定期更新作業系統與防毒軟體，降低被已知漏洞攻擊的風險



記住：任何網頁都沒有理由要求您在自己的電腦上手動輸入指令。

個資懶人包

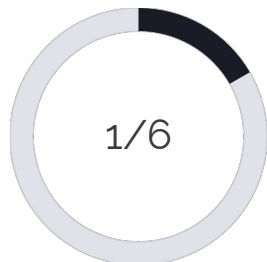
辦活動、招生、日常行政——讓個資保護成為工作流程的一部分，而不是額外的負擔。



活動報名表怎麼做才安全？

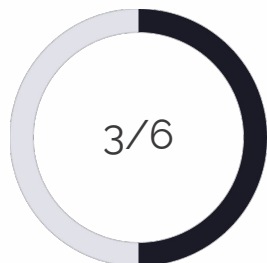
辦研習、辦講座、辦營隊.....每次活動都要做報名表，每次報名表都會蒐集個資。這是行政工作中接觸個資最密集の場合之一，也是最需要預先設計好個資保護機制的時候。

一份好的個資蒐集同意聲明，必須包含哪些要素？



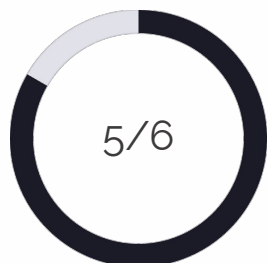
蒐集機關名稱

明確標示是哪個學校、哪個單位在蒐集資料。



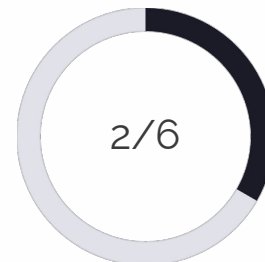
資料類別

列出將蒐集哪些類型的個資，例如姓名、單位、電子郵件。



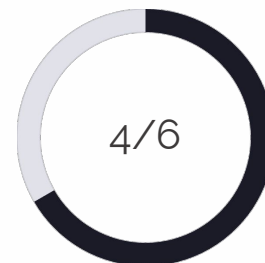
當事人的權利

告知當事人可以查詢、閱覽、更正、刪除個資，並提供聯絡窗口。



蒐集目的

具體說明為何需要這些資料，例如「辦理本次研習活動之報到、聯絡及出席記錄」。



利用期間、地區、對象及方式

說明資料將使用多久、在哪裡使用、給誰使用、如何使用。



不提供的後果

說明若當事人不提供資料，對其權益有何影響（例如無法完成報名）。

個資蒐集同意聲明【範例】

以下提供一份適用於**一般活動報名**的個資同意聲明範本，可直接複製貼入您的表單。建議放在表單的「最後一題」之前，並設置勾選框。

【個人資料蒐集告知事項】

本校〔辦理單位名稱〕依個人資料保護法第8條規定，告知以下事項：

一、蒐集目的：辦理本次活動（〔活動名稱〕）之報名、報到、聯絡通知及相關行政作業。

二、蒐集資料類別：姓名、服務單位/院系所、職稱/身分、聯絡電話、電子郵件信箱。

三、資料利用期間與範圍：本活動辦理期間，限本校〔辦理單位〕使用，不對外提供第三方。

四、您的權利：您得依法行使查詢、閱覽、複製、更正、補充、停止蒐集或刪除個人資料之權利 請洽：〔聯絡人姓名〕，電話：〔聯絡電話〕。

五、不提供之後果：如不提供以上資料，將無法完成活動報名。

☐ 我已閱讀並同意上述個資蒐集告知事項。（必填）

☑ 這份範本已涵蓋個資法第8條要求的所有必要告知項目！

只問需要的事就好！最小蒐集原則

個資保護的核心原則之一，叫做「**最小蒐集原則**」

——只蒐集達成目的所必要的最少個資。蒐集越少，保管的責任越小，外洩的風險也越低。

過度蒐集的範例

辦一場演講，報名表卻要求填寫：姓名、學號、身分證字號、出生年月日、手機、市話、系所、年級、緊急聯絡人

……

辦活動真的需要身分證字號嗎？需要緊急聯絡人嗎？
多問一個欄位，就多一份保管責任。

精準蒐集的範例

同樣的演講，精簡後只需要：姓名、單位 / 系所、電子郵件（用於發送確認信與活動通知）。

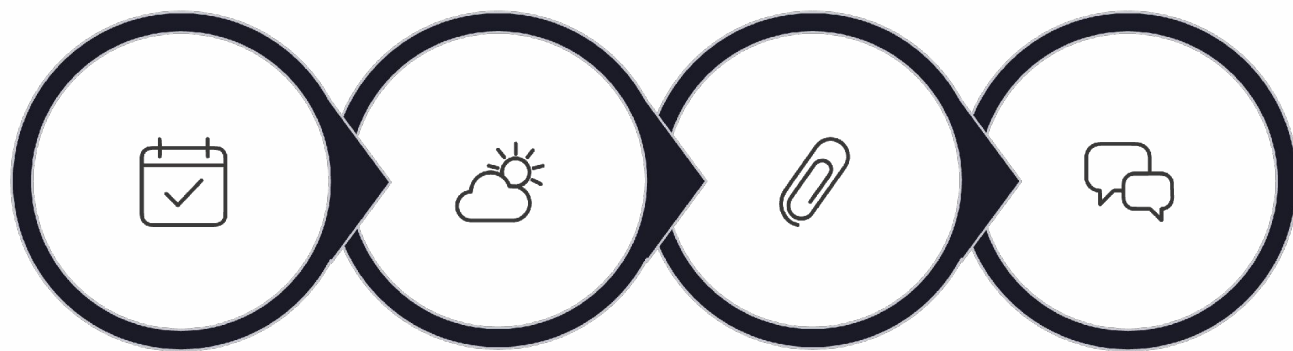
如果需要統計出席人數，可以在活動當天現場確認，而不是在報名表上多設欄位。

蒐集前先問：「不問這個，活動辦不成嗎？」

一個實用的自我檢查問題：「**我能跟當事人說清楚為什麼要蒐集嗎？**」如果答不上來，就不要問。

活動結束後的「數位大掃除」

活動辦完了，名冊還在雲端硬碟上、信箱裡、隨身碟裡、群組訊息裡這些「活動後的殘留個資」是最容易被忽略的風險。個資的保管責任，從蒐集那一刻就開始，但在您主動清理之前不會自動結束。



確認保存期限

清理雲端分享

刪除附件

通知群組清理

建議在活動結束後的**兩週內**完成數位大掃除。

若業務需要保留部分資料，請移至有權限管控的正式存檔資料夾，並記錄保存原因與預計刪除時間。

定期清理信箱與雲端空間的好處

很多人的信箱裡，躺著五年前辦活動的報名名冊、三年前某位同學的請假說明、兩年前某個案件的診斷書附件.....這些資料不是在保護，而是在積累風險。



降低外洩風險

存放的個資越少，一旦帳號被盜或設備遺失，外洩的資料量就越少。「不留沒必要的資料」本身就是一種保護。



符合法規要求

個資法要求個資在達成蒐集目的後應主動刪除。若因接受稽核或查詢而被發現仍留存大量過期個資，可能面臨法律責任。

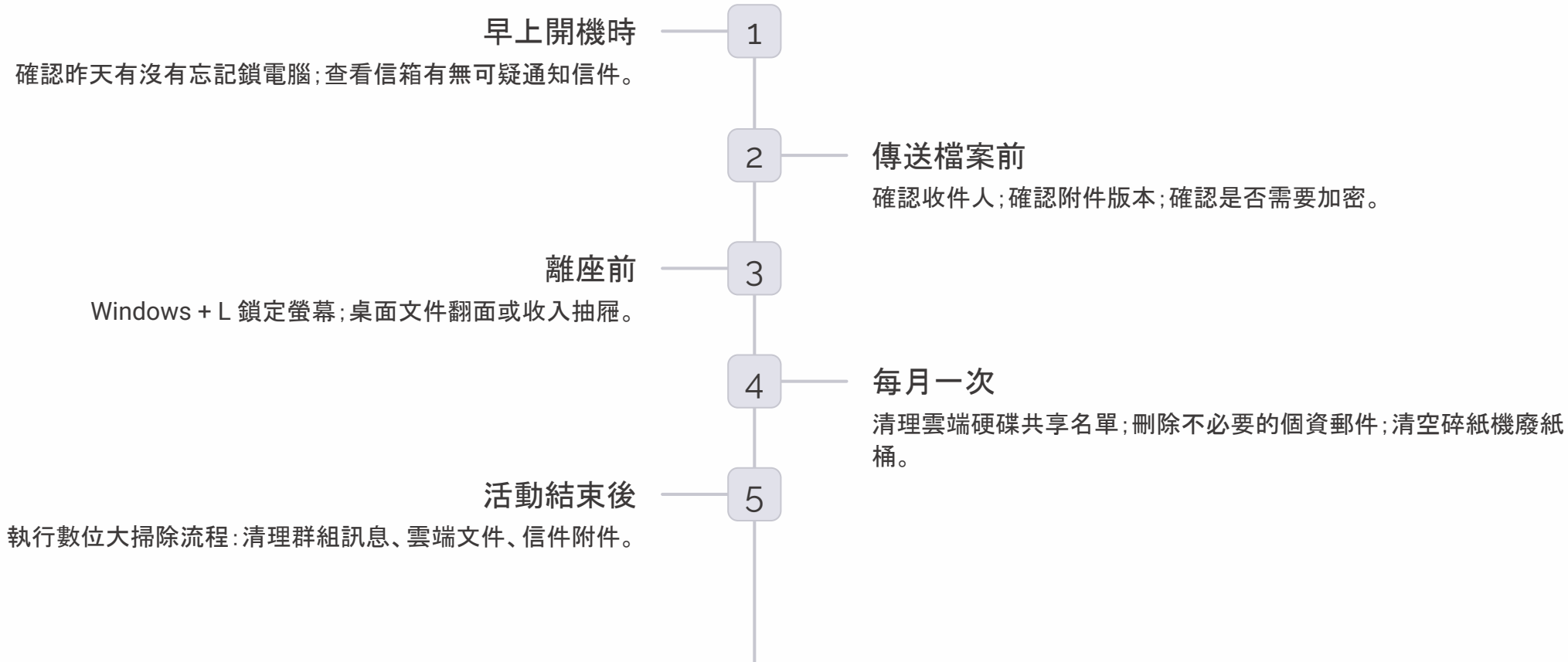


提升工作效率

信箱整潔、雲端有條理，找資料更快、不容易誤寄舊附件，也減少「這個版本對不對？」的困惑。整潔的數位環境就是高效工作的基礎。

建立個資保護的日常小習慣

個資保護最有效的方式，是讓它變成您的「反射動作」，而不是每次都要刻意思考。



萬一發生個資事故，該怎麼辦？

即使做了所有防護措施，意外還是有可能發生。發生個資事故時，最重要的是**不要隱瞞、立即通報**。



第一步：立即停止擴大

發現個資可能外洩，立即停止相關操作，例如撤回已傳出的訊息、關閉已公開的文件連結，防止更多人接觸到外洩的資料。



第二步：向主管通報

不論事件大小，立即告知直屬主管。隱瞞不會讓事情消失，只會讓情況更複雜。通報時說明：發生了什麼、涉及哪些個資、影響範圍有多大。



第三步：通知資訊安全或法務單位

由學校的專業單位接手評估事件嚴重性，決定是否需要通知當事人或主管機關（個資法第12條規定，若可能對當事人造成損害，需主動通知）。



第四步：記錄與檢討

完整記錄事件經過與應對過程，並進行內部檢討，找出是哪個環節的習慣需要調整，避免下次再發生同樣的問題。

情境模擬小遊戲(1/2)

以下提供幾個情境題，請舉起「 可以」或「 不行」作答。

情境一

您在辦公室印了一份含有20位學生學號和成績的名冊，印完後發現有一欄打錯了，需要重印。舊的那份，可以直接丟回收紙箱嗎？

情境二

主任在 LINE 公務群組傳來一份 Excel 附件，裡面是本學期全系同學的緊急聯絡人電話，請大家存到手機裡備用。您應該直接存嗎？

情境三

您收到一封信，主旨是「您的 Microsoft 帳號已被異常登入，請點此連結立即驗證」。寄件人顯示為「Microsoft 安全中心」。您應該點入連結嗎？

情境四

您在設計一份研習活動報名表，想知道報名者的個人偏好，於是加入了一題：「請問您的宗教信仰？」（非必填）。這樣可以嗎？

情境模擬小遊戲(1/2)

以下提供幾個情境題，請舉起「 可以」或「 不行」作答。

情境一

您在辦公室印了一份含有20位學生學號和成績的名冊，印完後發現有一欄打錯了，需要重印。舊的那份，可以直接丟回收紙箱嗎？

答案： 不建議。

含有學號與成績的文件屬於黃燈個資，廢紙建議使用碎紙機攪碎。

情境二

主任在 LINE 公務群組傳來一份 Excel 附件，裡面是本學期全系同學的緊急聯絡人電話，請大家存到手機裡備用。您應該直接存嗎？

答案： 不建議。

緊急聯絡人電話屬於黃燈個資，不應以 LINE 群組方式傳輸，也不應儲存在私人手機。應請主任改以有權限管控的雲端文件取代。

情境三

您收到一封信，主旨是「您的 Microsoft 帳號已被異常登入，請點此連結立即驗證」。寄件人顯示為「Microsoft 安全中心」。您應該點入連結嗎？

答案： 不行。

這是典型的釣魚信件。請直接到 Microsoft 官方網站登入確認，不要點信中的連結。

情境四

您在設計一份研習活動報名表，想知道報名者的個人偏好，於是加入了一題：「請問您的宗教信仰？」（非必填）。這樣可以嗎？

答案： 不建議。

宗教信仰屬於個資法第6條的特種個資，原則上禁止蒐集。即使設為非必填，也不應出現在報名表上。

更多情境模擬題(2/2)

以下提供幾個情境題，請舉起「 可以」或「 不行」作答。

情境五

您要寄一份含有學生個資的加密 Excel 給外部廠商，決定把文件和密碼一起附在同一封信中，這樣對方比較方便開啟。可以嗎？

情境六

活動結束三個月後，報名的 Google 表單仍然開著，任何有連結的人都能查看所有報名者的資料。這樣沒關係嗎？

情境七

一位家長打電話來詢問，說要確認孩子的選課情況，並提供了學生的姓名和生日。您可以直接告知嗎？

情境八

您離開辦公室去開一個小時的會議，桌上有一份正在處理中的獎學金申請文件(含學生身分證字號)。可以就這樣放著嗎？

更多情境模擬題(2/2)

以下提供幾個情境題，請舉起「 可以」或「 不行」作答。

情境五

您要寄一份含有學生個資的加密 Excel 給外部廠商，決定把文件和密碼一起附在同一封信中，這樣對方比較方便開啟。可以嗎？

答案： 不行。

文件和密碼必須用不同管道傳送。如果都在同一封信，一旦信件被攔截，加密形同虛設。密碼請改用電話通知或另一封信傳送。

情境六

活動結束三個月後，報名的 Google 表單仍然開著，任何有連結的人都能查看所有報名者的資料。這樣沒關係嗎？

答案： 不行。

活動結束後應立即關閉報名表單，並將回應資料限制存取權限。長期開放的表單是個資外洩的潛在漏洞。

情境七

一位家長打電話來詢問，說要確認孩子的選課情況，並提供了學生的姓名和生日。您可以直接告知嗎？

答案： 不建議。

學籍資料屬於當事人(學生)的個資，即使是父母，也需要有當事人授權或學校規定的驗證程序，不能僅憑口頭告知的姓名生日就提供。請依校內標準作業程序處理。

情境八

您離開辦公室去開一個小時的會議，桌上有一份正在處理中的獎學金申請文件(含學生身分證字號)。可以就這樣放著嗎？

答案： 不行。

離開座位超過幾分鐘，就應該將含有個資的文件收入抽屜或翻面放置，避免路過或來辦公室洽公的人員看見。

課程重點回顧

紅綠燈分類

學會用「紅燈/黃燈/綠燈」快速判斷資料的敏感程度，讓每一個處理動作都有依據，不再憑感覺。

數位工具安全

LINE傳資料前先問兩個問題；雲端檔案設好權限；收到可疑信件先停下來；加密文件和密碼分開傳。

懶人包實作

報名表要附個資同意聲明；只問必要資訊；活動結束後做數位大掃除；發現事故立即通報不隱瞞。

 個資保護不是額外的工作負擔，而是讓您工作得更安心的好習慣。

感謝您今天的參與。

個資保護不是一個讓人焦慮的大工程
只要建立好習慣，從下班前確認電腦已鎖定、桌面已淨空開始，您就已經是一位負責任的個資守門人！

