# 中華大學

## 教育機構如何因應個資法及社交工程防範

講師：NII 產業發展協進會
吳昭儀資深經理

- 社交工程之防範
- 個資法的衝擊與因應

所謂「社交工程」，就是詐騙！

透過電子郵件等方式偽裝身份

誘騙您上勾受騙…

假冒的身份；友善、誘惑的內容…

# 電子郵件攻擊的陷阱

- 夾帶惡意程式執行檔
- 內文中的惡意網頁超連結
- Html郵件隱藏遠端下載

# Html郵件隱藏遠端下載

Html電子郵件可以在Html中撰寫程式語法，所以您只要瀏覽電子郵件，就觸發該程式執行

利用IE漏洞，不開啟附檔也會中毒！

- 2004年3月，Beagle.O電腦病毒使用IE漏洞攻擊，使用者在Outlook / Outlook Express環境下啟用信件預覽功能，信件中的script就會啟動，連結到惡意程式網站下載病毒程式

# 演練執行方式

統計各單位惡意郵件「開啟率」及「點閱率」

郵件主題分為政治、公務、健康養生、旅遊等類型，郵件內容包含連結網址或word附檔

偽冒公務、個人或公司行號等名義發送惡意郵件給演練對象

→當收件人開啟郵件或點閱郵件所附連結或檔案時即觸發紀錄！

除非您瞭解電子郵件附檔的來源、
您知道會收到該附檔，否則請勿開啟！

如果電子郵件來自不知名人士，
請勿因為好奇心隨意開啟郵件和附檔！

除了不要點擊連結與隨意開啟附檔外，

您應該曉得的安全防護還包括：

- 關閉自動下載圖片
- 關閉預覽視窗

不要自動回覆讀信回條

考慮設定以純文字格式讀取郵件

# 資安相關注意事項

## ❖使用者責任

使用者的態度，對於有效防止非法的使用者存取，以保障安全的工作非常重要。

目標：防止未經授權的使用者存取資訊與資訊處理設施，以及使其遭受破壞或竊盜。

- 通行碼的使用
- 無人看管的使用者設備
- 桌面淨空與螢幕淨空政策

# 資安相關注意事項

- 通行碼的使用-密碼管理
  - 定期更新密碼
  - 定期檢查密碼
  - 設定優質密碼
    - 避免使用重複數字/單位簡稱/詞語/生日
    - 數字字母符號穿插且不過於複雜
    - 避免重複使用密碼
  - 不告訴他人密碼或寫下密碼
  - 懷疑密碼外洩立即更新

# 資安相關注意事項

## ❖ 無人看管的使用者設備

使用者應確保無人看守的設備獲得適當保護。

安裝在公共區域的設備（如公用主機、印表機或伺服器），應有具體的保護：

- 在活動完成時應終止對話，結束畫面。
- 使用密碼保護的螢幕保護程式。
- 活動結束時登出系統或主機，再關閉電腦。
- PC或設備不用時，應使用密鑰鎖或其他安全控制措施，以防止他人非法使用。

# 資安相關注意事項

- 桌面淨空與螢幕淨空政策

  桌面淨空

  - 重要/機密文件不置於桌上
  - 重要/機密文件下班或離開辦公室前應鎖入安全空間

  螢幕淨空

  - 設定螢幕保護程式
  - 設定保護密碼
  - 離開座位或暫時不使用時鎖定螢幕

# 資安相關注意事項

- 電子郵件的安全
  - 安裝防毒軟體過濾郵件
  - 不隨意開啟郵件附檔
  - 防堵垃圾郵件
    - 絕對不回覆垃圾電子郵件訊息
    - 不購買垃圾電子郵件的廣告商品
    - 不轉寄串接式的電子郵件，(例如聲稱不轉寄給10 個人就會倒楣的電子郵件。)
    - 要寄送同一訊息給許多收件者時，可採用「密件副本」方式來進行
    - 刪除寄件者為空白的電子郵件
    - 使用垃圾電子郵件過濾軟體
  - 垃圾郵件過濾簡易設定
    - 在Web 郵件上設定過濾垃圾郵件寄件者
    - 利用常見關鍵字過濾郵件

# 資安相關注意事項

- 即時通訊軟體風險
  - 存在的風險
    - 病毒威脅
    - 垃圾訊息
    - 檔案交換
    - 洩密
    - 工作效率的影響
  - 常犯之錯誤
    - 盲目的檔案分享
    - 花費過多時間於私人聊天
    - 將個人帳號資訊以儲存密碼方式設定儲存
    - 任意將個人之連絡者清單給他人

# 個人資料保護-課程大綱

- 個人資料保護法基本認知與重要條文說明
- 校園情境案例
- 個人資料保護及安全原則

# 個人資料保護法

- 電腦處理個人資料保護法
  - 84年8月11日制定公布。
- 個人資料保護法
  - 99年5月26日由總統府正式公布修正之全文，施行日期由行政院定之。

# 個資法架構

第一章　總則

第二章
公務機關對個人資料之蒐集、處理及利用

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

第五章 罰則

第六章 附則

# 何謂個人資料 ？

自然人的
- 姓名
- 出生年月日
- 身分證號碼
- 護照號碼
- 特徵
- 指紋
- 婚姻
- 家庭
- 教育
- 職業
- 病歷
- 聯絡方式
- 財務情況
- 社會活動

一般資料

特種資料
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

其他資料
- 得以直接或間接方式識別該個人之資料

# 個人資料之定義

❖根據個資法第 2 條，個人資料包括

- 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。

- 新法將個人資料的判斷標準為「得以直接或間接方式識別該個人之資料」，即便未指名道姓，只要揭露，即足以識別為某一特定人之資料，都在個資法保護的範疇內。

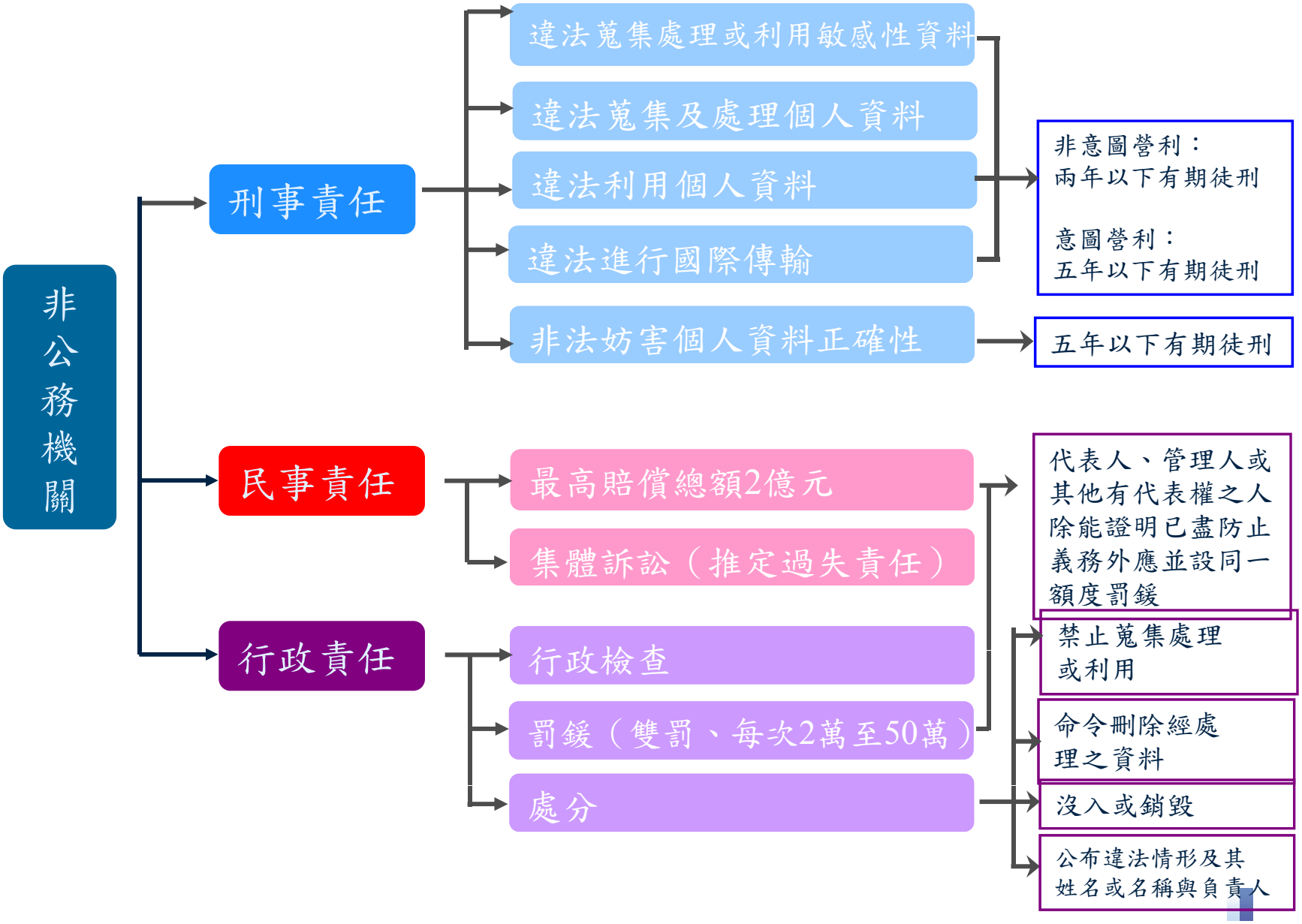
# 個人資料之定義（續）

- 特種個人資料，包括醫療、基因、性生活、健康檢查、犯罪前科
  - 特種個人資料除個資法第 6 條所定情形外，不得蒐集、處理或利用。
  - 性生活包括性取向。

# 個人資料保護法修正重點

5. 調整賠償義務及罰則：
   - 民事賠償：新台幣2千萬元→2億元
   - 刑事處罰：新台幣5萬元→100萬元
     有期徒刑：3年以下→5年以下
     意圖營利犯罪者，非告訴乃論
   - 行政處罰：新台幣10萬元→50萬元
   - 主管機關並得為下列處分：
     - 禁止蒐集、處理或利用個人資料。
     - 命令刪除經處理之個人資料檔案。
     - 沒入或命銷燬違法蒐集之個人資料。
     - 公布違法情形及其姓名或名稱與負責人。

# 非公務機關（私立學校）之法律責任



# 校務行政相關的個人資料

- 學生學籍資料
- 學生申請補助資料
- 學生清寒家庭身分
- 學生成績資料
- 學生獎懲及違規紀錄
- 學生家庭狀況
- 保健室病歷紀錄
- 學生家長或緊急連絡人聯絡方式
- 教職員健康檢查資料
- 教職員人事資料
- 教職員出缺勤紀錄
- 教職員通訊錄
- 畢業校友資料
- 畢業紀念冊
- 圖書館借還書記錄

案例：新生訓練是否為恰當時機讓學生知道學校可能利用其個人資料的狀況，學校也可一併在新生訓練或註冊時取得其同意授權？

No!

除非學校使用個人資料有可能超過教育行政之特定目的，否則是不需要學生額外授權的。

但因為新法增加了「告知」的義務，因此在學生入學時應立刻履行告知義務，詳述學校使用個人資料之範圍用途等。

More

如果學校對於學生的個人資料有逾越特定目的之利用，應及早告知學生並取得其「書面同意」。

案例：學生畢業後是否仍可寄發活動通知? 或應該在學生畢業前先取得其同意授權？歷屆畢業生個人資料應如何管理才符合個資法?

Yes!

學校使用校友個人資料還須符合「教育行政」之特定目的，若超過特定目的則不能使用，可能需要在畢業前取得學生授權。

More

一般人並不會反對辦校友活動會超過特定目的，但學校應與教育部、法務部溝通，確保學校能繼續使用校友資料。

此外，學校應建立控管機制避免校友資料外洩。

## 案例：學校是否可寄發與銀行合作發行的校園認同卡相關資料給校友?

No!

學校當初蒐集校友個人資料之特定目的為教育或訓練行政，或學生資料管理。學校寄發認同卡相關資料給校友，構成利用校友個人資料之行為，似已逾越上述特定目的，除非取得校友之書面同意，否則不得為之。

案例：畢業紀念冊上的學生資料是否屬於個人資料？
圖書館中陳列的歷屆畢業紀念冊是否應該管理？

Yes!

畢業紀念冊上的學生資料是屬於個人資料。

More

過去畢業紀念冊的收集與公開並非違法行為，但因為現在有越來越多的販賣個人資料或詐騙個人資料之行為，所以學校應改變個人資料之保管方式，就能加以控管限制閱覽畢業紀念冊的人員。

案例：老師擔心學生最近可能因閱讀某些讀物而造成行為偏差，所以向圖書館調閱學生的借書紀錄，請問圖書館是否可以提供？

借書紀錄含學生姓名、社會活動或其他得以識別學生之資料，此屬於個人資料之範疇。

No !

圖書館保存借書紀錄之目的為「學生資料管理」，並不具評估學生行為偏差與否之目的。

老師向圖書館調閱學生借書紀錄，固然可認為是學校內部「教育或訓練行政」目的，但仍應於該目的之必要範圍內為之，並應尊重當事人權益。

如有證據可合理懷疑某學生偏差行為與閱讀有相當關聯，老師為進一步確認而向圖書館調閱學生借書紀錄，或可被認為符合「教育或訓練行政」目的之必要範圍。若老師在無任何證據情況下，全面調取學生借書紀錄，恐被認為逾越「教育或訓練行政」目的之必要範圍，因而違反個資法的規定。

案例：若當事人尚未成年，請問個人資料蒐集需要取得當事人或監護人同意嗎？

Yes!

民法規定，滿20歲為成年。未成年人包括：

1) 未滿7歲者，為無行為能力人：應由法定代理人代為意思表示，並代受意思表示。
2) 滿7歲以上者，為限制行為能力人：其為意思表示及受意思表示，原則上應得法定代理人之允許。

依民法規定，未成年人為書面同意，應由法定代理人代為書面同意，或得到法定代理人之允許。

More

民法規定，已經結婚之未成年人，有行為能力。
換言之，已經結婚之未成年人，可以自行為書面同意，並無法定代理人代為書面同意或允許之問題。

案例：學校公布欄上公告曠課學生名單（學生姓名、學號）有違反個資法嗎?

No!

有關獎懲應符合學校辦理教育行政之目的，公布並不違反個資法，但須注意公布學生名單時，應僅揭露必要之個資。

案例：若當事人自行公開其特種個人資料，是否可以蒐集與傳播?

No!

已公開的特種個資雖然可以蒐集，但蒐集及利用仍須依個資法之特定目的範圍，也不能任意傳播。

案例：2008年承攬國中基測電腦閱卷、計分的業者因販售學生個人資料給補教業牟利，檢方將主要負責人共3名依背信罪及違反電腦處理個人資料保護法聲押。業者販賣給補習班的個資以光碟存放，每份售價23或35萬元，價格依地區有所不同。

Q. 蒐集與利用個資的相關業務是委外給廠商執行，若個資有外洩漏事件，應該由委外廠商負責。不是嗎?

根據個資法第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。因此，雖然是外包公司洩漏個資，但是國中基測的負責單位也須負責任的。

那我要如何控制別人的公司不會外洩這些個人資料呢?

委外廠商篩選須謹慎，特別是委外蒐集與處理個資的廠商；建議應該對委外廠商的個人資料安全管理有相當的要求與管控，並應在契約條款轉嫁相關的風險。

# 個人資料保護基本原則

*以下原則摘要整理自教育部100年度提升校園資訊安全服務計畫「教育機構個人資料保護工作事項」*

1. 機關學校應設置並指定「個資保護聯絡窗口」，作為機關學校間個資業務協調聯繫之對口、機關學校本身個資安全事件通報之對口，以及重大個資外洩事件之民眾聯繫單一窗口。
2. 機關學校應將「個資保護聯絡窗口」之聯繫方式（如：電話、email）置於單位網站，以便利民眾提出申訴與救濟。
3. 機關學校單位管理之網站或網頁內容，於確有必要公布個人資料時，需經所屬單位主管核准，且依相關法律及規範處理，始得公布。

# 個人資料保護基本原則（續）

4. 個人資料檔案應定期備份，並防止個人資料被竊取、竄改、毀損、滅失或洩露。
5. 個人資料輸入、輸出、存取、更新、更正或註銷等處理行為，宜釐定使用範圍及調閱或存取權限。
6. 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身份之登入通行碼，且不得與他人共用並定期更新。
7. 含有個人資料之紙本報表或檔案存取之申請、讀取、列印、使用、存檔、轉交及銷毀等處理及利用行為，宜建立相關之授權、監督及行為記錄機制。
8. 內部傳遞或與其他機關交換個人資料時，應選擇可靠且具備保密機制之傳遞方式，例如在紙本文件封袋加上彌封、使用破壞性信封袋；或對電子資料檔案加密，並對轉交或傳輸行為加以記錄流向備查。

# 個人資料保護小提醒

- 除非組織允許，不將包含個人資料的公務資料帶回家處理
- 職員的個資也受到法律的保護
- 不在電話裡隨意透露自己或他人的個人資料
- 非信任之網站，勿隨意留下個人資料
- 不點選來路不明的超連結網址
- 不委託他人代辦信用卡

簡報完畢，敬請指教