校園教職員資訊安全教育訓練

115學年度第1學期校園個人資料保護法宣導專題研習暨資通安全通識課程

從日常防護到課堂應用，成為守護校園的數位守門人

適用對象：全校教職員

課程時數：3 小時

主講者：楊雯珺

我們的資安政策

為加強電腦使用安全、維護資料機密及作業管制，以達到資訊之機密性、完整性與可用性，確保資料安全與正確性，進而提升作業效率，本校應制訂資通安全政策 。

講師介紹

課程講師｜楊雯珺 Janice Yang

學歷背景

澳洲中央昆士蘭大學行銷研究所、國立中山大學資訊工程與管理研究所、台北科技大學工業工程與管理系。

現職

漢昕科技股份有限公司 管理顧問，深耕資訊安全與品質管理領域，業界資歷達 20 年。

產業資歷

曾任財團法人電信技術中心稽核室管理師、品質小組工程師，歷任聯華電子、住華科技、益通光電等企業品保與稽核職務。

專業資格

ISO 27001、ISO 27701、ISO 9001、IATF 16949 等國際管理系統稽核資格，並具 IPMA C 級國際專案管理師、品質工程師等多項專業認證。



課程說明

今天的課程，希望帶給您這五件事

建立資安基本觀念
認識機密性、完整性、可用性三要素，理解資安是全體教職員的法定責任，不只是資訊組的事。

看穿詐騙與社交工程手法
學會辨識釣魚郵件、變臉詐騙、AI深偽詐騙等常見手法，養成「停、看、想」的防禦直覺。

養成日常防護好習慣
掌握密碼安全、實體防護等日常小習慣，並學會把生成式AI安全地用在教學與行政工作中。

學會保護學生資料
認識校園常見的敏感資料，了解傳統與AI時代下，該如何避免學生個資外洩。

熟悉事件通報流程
萬一真的踩到雷，知道第一時間該怎麼做、該找誰，把握黃金應變時間。

課程地圖

3 小時課程大綱

一 **為什麼資安跟我有關** CIA三要素、法定責任、常見詐騙手法

14:00~15:20

二 **日常工作中的小習慣** 密碼、實體防護、AI日常使用習慣

中場休息 *15:20~15:30*

三 **學生資料要怎麼保護** 敏感資料分級、安全傳輸、AI與資料保護

15:30~17:00

四 **遇到狀況怎麼辦** 黃金1小時、拔停報三步驟、通報窗口

破冰提問

開始之前，先想一想

在您心目中，「資訊安全」是誰的責任？

- 資訊組 / 資訊組長？
- 學校行政主管？
- 每一位教職員？
- 其實是我自己？

01

大綱一

為什麼資安跟我有關

認識資安三要素與法定責任，看懂校園常見的詐騙手法



大綱一

為什麼要保護資訊？資安三要素 CIA

機密性 Confidentiality

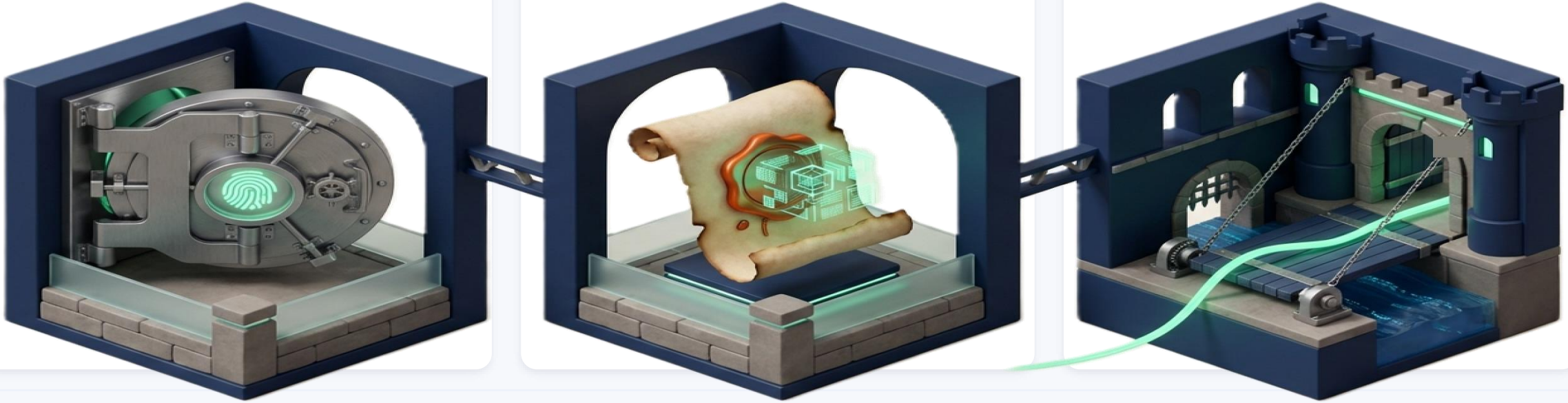
只有「對的人」能看到資料。例如：學生成績、家庭狀況只能授權人員查閱，不能任意外流。

完整性 Integrity

確保資料「沒被偷偷改過」。例如：成績登錄後不能被竄改，公文內容傳遞途中不能被竄改。

可用性 Availability

需要用的時候，系統「隨時能用」。例如：段考當天，成績系統、列印設備都必須正常運作。



大綱一

打破迷思：資安不只是資訊組的事

危險的迷思

- 「反正有防火牆和防毒軟體，資安交給資訊組就好」
- 「我只是老師 / 行政人員，駭客不會找上我」
- 「密碼設簡單一點方便記，反正不會被發現」

法規的現實

- 資通安全管理法明確規定，全體員工都有法定資安責任
- 若因個人疏失（如亂點信件、密碼外洩）導致資安事件，當事人須面臨懲戒
- 資安，是每一位同仁保護自己的法定護身符

台視新聞HD

7校學生個資遭駭客入侵



- 某校系統漏洞入侵主機
- 執行惡意程式
- 竊取該校帳號密碼
  以該組帳號密碼
  成功登入其他6所學校
  校務系統



嘉義市 27-31

校務系統遭"駭"！7所學校學生個資外洩

12:25:08

人工增雨 春雨雲系到 石門水庫燃放焰劑盼增降雨機率

核心比喻

學校就像一座城堡，
每一位教職員都是守城的衛兵



資訊組蓋起厚實的城牆（防火牆與防毒軟體），但再高再厚的城牆，也防不住一位主動幫陌生人開門的衛兵。

真正的最後一道防線，是您。

校園面臨的雙重夾擊：外部攻擊與內部疏失

外部攻擊 External

- 來源：國際駭客組織、勒索軟體集團
- 手法：系統漏洞攻擊、DDoS癱瘓服務
- 防禦主體：資訊組的防火牆與系統更新



內部疏失 Internal

- 來源：教職員自身操作不慎
- 手法：點擊釣魚郵件、使用弱密碼、隨身碟未掃毒
- 防禦主體：您 —— 真正的第一道防線



攻擊時間軸總覽

六起主要行動，橫跨美國、加拿大、台灣及全球關鍵基礎設施



颱風來襲，請做好防颱準備 !!

2023.05
Volt Typhoon
美國關鍵基礎設施

2023.08
Flax Typhoon
台灣 / 美國政府機構

2024.10
Salt Typhoon
全球電信業者

2024.12
Silk Typhoon
美國財政部

2025.07
SharePoint 攻擊
全球政府機關

2026.08
反制行動
8.8萬伺服器修復

外部攻擊 External



外部攻擊 External



內部疏失 Internal



內部疏失 Internal



一次疏忽的真實代價

當「城門」失守之後……

信任崩塌：家長與學生失去對學校的信任，校務服務停擺、公信力瞬間歸零。

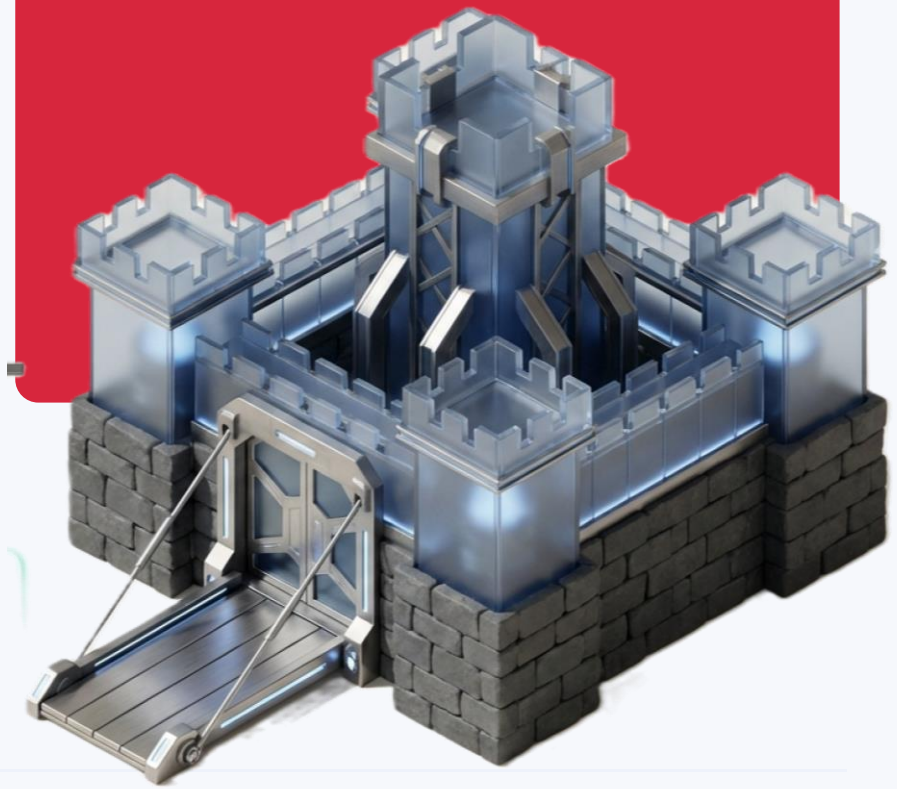
財務損失：系統重建費用、勒索軟體帶來的營運中斷損失難以估計。

法規懲處：依資通安全管理法，肇事人員將面臨行政懲戒，甚至因觸犯個人資料保護法背負刑事責任。

依法通報時限

1 小時

資通安全事件通報及應變辦法規定，知悉事件後必須於黃金1小時內完成通報。




TVBS新聞台 HD
中華航空
更多新聞在這裡
華航遭駭會員個資洩"賴清德.張忠謀.小S"受害
掌握新聞脈動 ▶ 訂閱TVBS NEWS頻道



核心觀念

社交工程不破解系統，只破解「人性」

就像詐騙集團假冒綁匪打電話騙贖金——沒有真的綁架，卻利用您的恐慌與急躁，讓您乖乖交出鑰匙。駭客也是如此，利用好奇、貪婪、恐懼或權威服從，讓您親手打開城門。

什麼是社交工程？不破解系統，只破解「人性」

技術破解（耗時費力）



社交工程（直指核心）



社交工程就像「詐騙集團假冒綁匪打電話騙贖金」，根本沒有綁架您的家人，利用「恐慌」和「急躁」，讓您乖乖把錢匯出去。駭客不花時間尋找系統漏洞，而是直接騙您交出進入系統的鑰匙。

- **貪婪（Greed）：** 限時優惠、免費贈品
- **恐懼（Fear）：** 帳號凍結、法律威脅
- **好奇（Curiosity）：** 八卦新聞、未公開異動
- **權威服從（Authority）：** 假冒長官的緊急指示

抓漏教學：釣魚郵件 5 大特徵

偽造寄件人網域

顯示名稱看似官方，但真實信箱卻是一串無關的亂碼或免費信箱。

不合邏輯的稱呼

用「親愛的用戶」而非您的真實姓名，暴露其廣撒網本質。

可疑的超連結

按鈕文字寫著官方字樣，但滑鼠懸停卻顯示非官方的奇怪網址。

虛假的急迫感

利用恐懼逼迫立即行動，如「24小時內未完成驗證將被停權」。

非慣用語法

出現機器翻譯語氣、簡體字或罕見用語，與平常溝通方式不符。

養成開信前檢查習慣

五點都檢查過一遍，就能避開絕大多數的釣魚陷阱。

大綱一

校園常見的釣魚情境

校務系統帳密到期通知

假冒教育局或校務系統，要求「立即

偽冒公文附件

冒充教育局或上級機關名義，寄送「

假冒家長或學生投訴信

製造情緒張力誘使教師點擊附件或連

免費教學資源 / 贈品

以「免費電子教材」「限時教具贈送



一封偽冒公文，如何演變成資安事件

STEP 1

誘餌釋放

駭客冒用機關名義，寄送「重要公文」信件，並貼心附上解壓縮密碼降低戒心。

STEP 2

內部上鉤

收件人為求時效，未經驗證即下載並解壓縮附件，開啟隱藏的執行檔。

STEP 3

端點淪陷

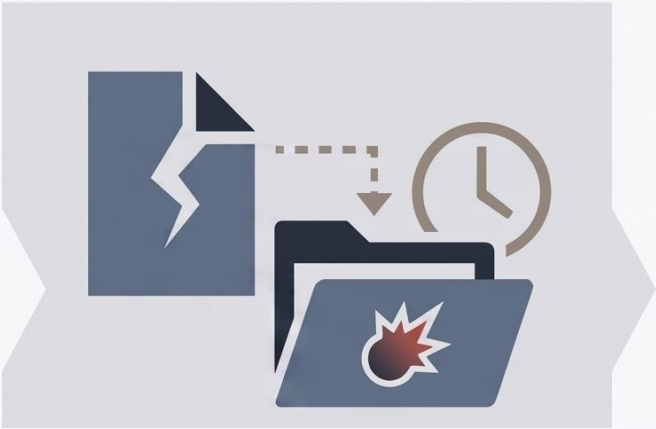
惡意程式植入後門，電腦瞬間成為駭客潛入校園網路的跳板。

STEP 4

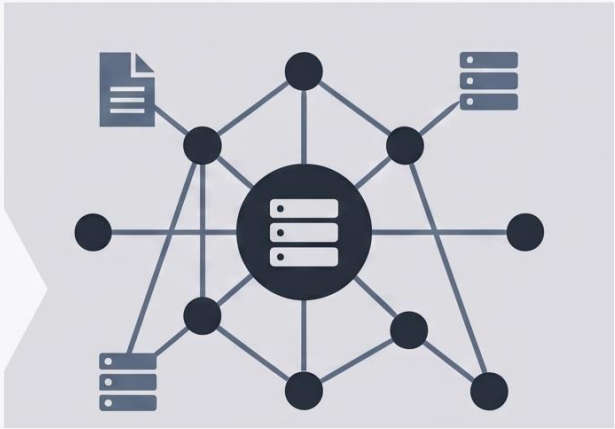
橫向擴散

駭客以此電腦為跳板，在校園內部網路橫向擴散，機敏資料外洩。









變臉詐騙與AI深偽詐騙



商業郵件詐騙 BEC

駭客長期潛伏、摸透內部溝通模式後，假冒校長、主管或會計人員，於下班前發出「更改匯款帳號」或「緊急調閱資料」指令。



AI 深偽視訊詐騙

運用深偽技術（Deepfake）合成聲音與影像，冒充長官在視訊會議中「本人下達指示」，誘使受害人依指示轉帳或提供機密。眼見不再為憑，遇到金流異動務必透過其他管道二次確認。


TVBS新聞台HD
更多新聞在這裡
你刷9830元...假銀行發mail詐騙 民眾:太逼真
TVBS NEWS
掌握新聞脈動 ▶ 訂閱TVBS NEWS頻道


CBC東森新聞HD
違法行為 請勿試法
絕對是詐騙啦
晚間新聞 詐騙猖獗抓不完!AI技術遭濫用 靠APP破解
CBC NEWS 下載APP精彩內容不錯過

社交工程威脅矩陣：認識攻擊媒介



攻擊型態	攻擊媒介	心理觸發點	防禦關鍵
釣魚郵件 Phishing	電子郵件	恐懼、貪婪	核對真實網域、不點擊
簡訊釣魚 Smishing	簡訊、LINE	好奇、急迫	不下載不明App、不給驗證碼
語音釣魚 Vishing	電話通話	恐懼、權威	掛斷電話、自行回撥官方客服
變臉詐騙 BEC/深偽	郵件、視訊會議	權威服從、信任	透過非原管道進行雙重驗證

防禦黃金法則：停、看、想

STEP 1



停 Stop

收到急迫、威脅或極度誘惑的訊息時，先停下點擊的手，深呼吸三秒鐘。

STEP 2



看 Look

檢查寄件者真實網址、滑鼠懸停確認連結走向、留意未說明的附件。

STEP 3



想 Think

這封信的語氣合理嗎？透過「不同管道」向對方確認，再決定是否放行。

只要做到「停、看、想」再點擊，社交工程對您就徹底失效。

情境演練

如果是您，會怎麼做？

您收到「校長」用 LINE 傳來的訊息：「我在開會不方便講電話，幫我買三張5000元禮券，發序號給我」，您會？

立刻去超商買，畢竟是校長交代

先回LINE問清楚為什麼

打電話或當面向校長本人求證

直接不理會，太奇怪了

資安是法律要求，更是您的護身符

- 法規強制、無人例外：資通安全管理法賦予每一位教職員法定義務
- 破除迷思、全員皆兵：資安不只是資訊組的責任，90% 的防禦取決於第一線人員
- 社交工程利用善意、好奇或恐懼來騙取資料，釣魚郵件五大特徵要牢記
- AI深偽技術讓「眼見為憑」不再可靠，金流異動務必二次確認
- 牢記「停、看、想」三字訣，就是最強的人體防火牆

02

大綱二

日常工作中的小習慣

密碼、設備、AI 工具，養成日常防護的直覺反應



大綱二

日常資安好習慣，四件事就夠



驗明正身

收到匯款或索取個資的信件，務必檢查寄件者「完整地址」，不要只看顯示名稱。



拒絕誘餌

不點擊來路不明的連結，不隨意開啟壓縮檔（.rar、.zip）或執行檔（.exe）。



上好門鎖

離開座位務必鎖定螢幕（Win+L），密碼設定足夠強度，並開啟多因子驗證。



通報異常

遇到疑似攻擊或不尋常要求，第一時間通報資訊人員 / 學校資安窗口，絕不隱瞞。

隨堂互動

一起想想看

回想一下校園日常，您覺得最容易讓「城門」失守的小習慣是什麼？

密碼寫在螢幕便利貼上？

撿到 USB 直接插電腦？

公私帳號密碼全部相同？

看到免費資源秒點擊？

駭客破解密碼，比您想的還要「自動化」



字典攻擊 Dictionary Attack

程式在一秒內自動測試數萬個常見單字、連號與生日組合，簡單密碼幾乎秒破。



撞庫攻擊 Credential Stuffing

駭客拿其他網站外洩的帳號密碼，自動化去「撞」您在校務系統的帳號——公私密碼相同者首當其衝。

資安地雷榜：您中了幾個糟糕的密碼習慣？

弱密碼

只用生日或「123456」，在字典攻擊面前形同虛設，幾乎秒被破解。

萬年不換

密碼從未更新，或離職人員帳號仍保留，成為長期潛在破口。

一碼走天下

公私帳號共用同一組密碼，只要一處外洩，就等於全線淪陷。



生日當密碼好記 卻是駭客最易破解數字

午間新聞

強制長度與定期更換，是國家級的防護要求

依據《資通安全責任等級分級辦法》附表十（資通系統防護基準）



強制長度與複雜度

系統必須強制最低密碼**複雜度**（含文字、數字、符號）與**長度**

對抗自動化暴力破解。密碼長度每增加一碼，駭客破解的數學難度呈「指數型上升」。

強制定期更換與歷程

強制密碼**效期限制**，且變更時不得與前3次相同

設下「停損點」。確保即使密碼在不知情下外洩，駭客手中的「通行證」也會過期失效

密碼想好了，然後呢？<u>絕對不要貼在螢幕上</u>！

最強的數位防護，往往敗給最脆弱的實體習慣

❌ 絕對禁止



貼在螢幕邊框、寫在桌上的筆記本、
存成未加密的 **Word / Excel** 檔。

✅ 安全作法



使用單位核可的「密碼管理工具（**Password Manager**）」、開啟系統內建的安全儲存庫，
或是**把密碼短語牢牢記在腦海中**。

警報響起！突然收到驗證碼？

收到未授權的驗證碼，代表密碼已外洩，駭客正在嘗試登入！



絕對不按「同意」

防範 MFA 疲勞攻擊，也絕對不要把驗證碼報給任何人（即使對方宣稱是 IT 單位）。

立刻更改密碼

這通警報證明您的第一道防線（密碼）已經破裂了！

立刻通報

聯繫校內的資安人員或 IT 部門，啟動資安應變機制。

告別難記亂碼：學會設定「密碼短語」

密碼不一定要是痛苦的亂碼，「長度」比「複雜度」更具防護力！

傳統複雜密碼（不推薦）

例如 P@ssw0rd!，看似複雜但長度短，現代設備可能只需幾分鐘就能暴力破解，而且難記易忘。

密碼短語 Passphrase（推薦）

例如 RedFox-Ice-Run-88，將多個毫無關聯的詞彙串連，好記、畫面感強，長度夠長讓破解成本大幅提高。

告別難記亂碼！學會設定高強度「密碼短語 (Passphrase)」

密碼不一定要是痛苦的亂碼，「長度」比「複雜度」更具防護力！

傳統複雜密碼：

P@s$wOrd!



- 難記、易忘。
- 看似複雜，但長度太短，現代顯示卡只需幾秒到幾分鐘就能暴力破解。

密碼短語(Passphrase)：

RedFox-Ice-Run-88



- 將多個毫無關聯的詞彙串連。
- 好記、畫面感強。因為長度比較長，駭客破解需要耗費許多時間。

多因素驗證 MFA：保險箱除了鑰匙，還要核對指紋

STEP 1



第一道鎖

您知道的（Something you know）：輸入帳號密碼。

STEP 2



第二道防線

您擁有的 / 您本身的：手機動態驗證碼（OTP）或指紋、臉部辨識。

STEP 3



授權放行

雙重核對身分成功，才能開啟核心系統，即使密碼外洩，駭客仍無法登入。

校務系統、遠端連線等核心系統，務必開啟多因子驗證。

多因素認證（MFA）：保險箱除了要鑰匙，還要核對指紋

密碼只是第一道鎖。**MFA 加入了第二道防線**，確保即使密碼外洩，駭客也無法登入

第一道鎖
(您知道的Something you know)



輸入密碼。

第二道防線
(您擁有的 / 您與生俱來的
Something you have / are)



系統要求手機動態驗證碼(OTP)
或生物辨識(指紋 / 臉部)。

授權放行
(Access Granted)



雙重核對身分，
成功開啟核心系統。

重點回顧：把您的密碼當成「牙刷」！

日常生活的必需物品，就是數位防護的最佳指導原則

絕對不共用

就算感情再好，您也不會跟別人共用牙刷。

➜ **嚴禁共用帳號密碼。**

刷毛夠強韌

刷毛要夠長夠韌，才刷得乾淨。

➜ **使用高強度且好記的「密碼短語(Passphrase)」。**



定期要更換

刷毛用久了會分岔失效，必須定期換新。

➜ 遵守法規要求，**定期更新密碼。**

搭配漱口水加倍防護

單靠刷牙不夠，加上漱口水更安全。

➜ **核心系統務必開啟 MFA 多因素認證。**



記住這句話

把密碼當成您的牙刷——絕對不共用、要定期更換

刷毛要夠強韌（高強度密碼短語）；單靠刷牙不夠、加上漱口水更安全（核心系統開啟MFA）；這是日常生活的必需物品，也是數位防護的最佳指導原則。

校園實體資安常見盲點

螢幕便利貼密碼

密碼貼在螢幕邊框，來訪者一眼可見。

未拔出的隨身碟

離開座位隨身碟仍插在電腦上。

印表機留機密公文

列印後未即時取件，內容任人瀏覽。

尾隨進入辦公室

好心幫忙開門，未核對訪客身分。

淨空桌面、螢幕鎖定：不只是愛乾淨



淨空桌面 Clear Desk

離開座位時，機敏文件（成績單、輔導紀錄等）必須收妥上鎖，不能大剌剌攤在桌上任人瀏覽。



螢幕鎖定 Screen Lock

離開座位的第一反射動作：Windows 按 Win+L，Mac 按 Ctrl+Cmd+Q。不鎖螢幕等於敞開大門歡迎訪客。



拒絕尾隨 Tailgating

核對身分、拒絕不明人士尾隨進入辦公室或機房，是專業而非冷漠的表現。


選前敏感毒駭
TVBS新聞台 HD
TVBS
惡作劇?駭客?議員收可疑USB 藏木馬病毒



大綱二 · AI使用習慣　先搞懂定義

生成式AI，是根據海量資料「重組」出新內容的工具

生成式AI（Generative AI）透過機器學習大型語言模型，依據使用者輸入的提示（Prompt），生成文字、圖片、音樂或影片等作品。它擅長重組既有資料，但不具備真正的理解與判斷力。

生成式AI能為教學做什麼？

對話

即時問答與討論

翻譯

跨語言內容轉換

摘要

長文重點整理

創作

文本圖像生成

分析

資料歸納比較

問答

引導式思考

修辭

文句潤飾修改

語意比較

找出相關概念

教師可以怎麼用AI？三階段應用模式

STEP 1



課前準備

產生課程計畫、製作教學素材、補充教學內容、設計分組學習、建置評量規準。

STEP 2



教學與評量

產出學習範例、精進提問能力、創新多元作品、促進素養學習、多元評量回饋。

STEP 3



滾動式修正

課程修正與調整、教學改進與交流、驗證創新教學模式，持續優化教學歷程。

資料參考：高雄市高級中等以下學校生成式AI工具教學應用參考指引

六步驟提示語架構法，讓AI產出更貼近需求

角色、目標、規則為必填；結構範例、限制條件、實施方式可視需求填入

① 角色（必填）+ ② 目標（必填）

例：「我是國小教師。我要創作一份臺南古蹟參觀教案。」明確指定角色程度，讓AI產出貼近學生程度的內容。

③ 規則（必填）+ ④ 結構範例

例：「活動時間08:00~12:30，要包含課程表；內容需含學習目標、先備知識、評量方式五大項。」

⑤ 限制條件 + ⑥ 實施方式

例：「議題融入需包含SDGs指標；需以表格方式呈現。」條件越具體，AI產出的內容越可用。

學生可以怎麼用AI？三步驟法＋四大使用時機



規劃學習目標與歷程

釐清陌生主題的背景與架構，擬訂學習起點與步驟。



選擇策略

釐清想法、建議學習策略、模擬角色促進思考。



評量與回饋

修正文章、獲得回饋、產出開放性問題進行練習。



調整學習

依回饋調整學習策略，分析成果並持續改進。

好習慣不是規定，是保護自己的直覺反應

- 驗明正身、拒絕誘餌、上好門鎖、通報異常，四件事天天做
- 密碼像牙刷：善用密碼短語、不共用、核心系統開啟MFA
- 淨空桌面、螢幕鎖定，不明USB就像撿到的二手牙刷絕不能插
- 使用AI前先想好角色、目標、規則，讓AI產出更貼近教學需求
- AI是教師與學生的學習夥伴，但仍須經過人為檢視與把關



中場休息

休息 10 分鐘，接下來是本次課程的重點單元！

接下來：大綱三　學生資料要怎麼保護

03

大綱三

學生資料要怎麼保護

從紙本到雲端，從傳統外洩到AI時代的新風險



大綱三

什麼是校園情境中的敏感個資？

學生成績與學習歷程

成績單、學習歷程檔案屬高度敏感資料。

健康與輔導紀錄

健康檢查、身心狀況、輔導諮商紀錄。

家庭與聯絡資訊

家長聯絡方式、家庭經濟與監護狀況。

身分與證號資料

身分證字號、學號、教職員個資。

認識資料分級：先分清楚您手上的資料屬於哪一級



公開

官網新聞稿等一般性資訊，外洩對校務無實質影響。



內部

內部行政表單，僅限校內同仁存取。



機密

學生個資、財務報表，外洩將導致嚴重衝擊與究責。



極機密

涉及重大機密事項，外洩將產生災難性打擊。

日常辦公的資料外洩地雷

常見的手滑悲劇

- 大量寄送信件誤用「副本CC」而非「密件副本BCC」，聯絡方式全數曝光
- 公務檔案傳錯家長群組或私人群組，無法收回
- 機密文件用LINE或個人雲端空間傳送，形同明信片公開傳遞

安全的作法

- 大量寄送一律使用密件副本（BCC），保護收件人隱私
- 傳送前多看一眼收件人與附件，公務用公務信箱
- 機密檔案加密傳輸，密碼透過其他管道分開提供


CTV NEWS
CTV NEWS
CTV NEWS
CTV NEWS
CTV NEWS
CTV NEWS
CTV 中視新聞
民政及人文課
屏東
25-34
中視新聞 YouTube
頻道異動
中嘉系統 中視新聞台(HD)統一定頻115頻道

AI教學應用六大風險，一定要跟學生一起討論

正確性

AI生成內容絕對正確嗎？我們如何判斷、查核？

可溯源性

訓練資料是否涵蓋不同國家與背景的觀點？

事實性

如何辨識深偽內容，覺察以假亂真的資訊？

生成性

如何因應機密資料管理與隱私保護問題？

思辨性

如何提升自我資訊辨識及批判思考能力？

風險性

使用數位工具與生成式AI時，如何避免風險？

AI可能產生偏誤與文化侷限的內容

案例：旅遊行程規劃

若資料庫缺乏當地氣候、地理、文化資料，AI可能綜合各種網路遊記，產出不順路、非當季，甚至虛構景點的行程。

案例：文化偏見

要求AI生成「新娘」圖片，可能只產出穿白紗的西方臉孔女性，而非考量使用者當地文化習俗的多元樣貌。

教學提醒

引導學生結合自身經驗與批判性思維檢視AI產出的結果，而不是全盤接受。

AI可能編造內容、也可能被深偽技術濫用



AI幻覺（Hallucination）

AI可能一本正經地編造不存在的引用來源、數據或事件。教師與學生都應養成「多方查證」的習慣，不可盡信AI的產出。



深偽技術 Deepfake

能修改臉部與聲音的深度仿造技術，可能製造看似真實的假影片、假新聞。觀看網路內容時，應留意是否為深偽技術合成，並判斷可能的動機。

絕對禁止：這些內容不能輸入給公開AI工具

學生個人資料

姓名、學號、成績、健康與輔導紀錄

學校機密公文

未公開之會議紀錄、行政決議

未公開消息

人事異動、尚未公告之校務決策

帳號密碼等憑證

任何登入資訊、金鑰、驗證碼

記住這句話

把學生資料餵給公開AI工具，就像在夜市用擴音器廣播機密

未經授權的公開AI工具，會將輸入內容作為未來訓練資料的一部分。您為了偷懶輸入的學生個資，下一秒可能就成為別人提問時得到的答案，而且無法收回、刪除。

學生作業使用生成式AI的四種規範模式

模式	說明
模式一	由學生自行完成撰寫，再交由生成式AI進行修改
模式二	由生成式AI產生架構後，再由學生完成內容撰寫
模式三	由學生擬訂架構後，再由生成式AI產生內容並修改
模式四	不得使用生成式AI

資料參考：教育部「高級中等學校學生學習評量及學習歷程檔案使用生成式人工智慧注意事項」。教師應於課程開始、作業或評量實施前，明確向學生說明採用哪一種模式。

使用AI，一定要「揭露」與「引註」

教師揭露原則

若使用生成式AI產出教案等課程內容，應於教材適當標註「引用自生成式AI工具」等文字。

學生引註原則

學生使用AI輔助作業或報告時，應依課程規範於備註處註明AI工具名稱、版本，並保留提問與對話歷程作為佐證。

對生成內容負責

無論教師或學生，都應對採用的AI生成內容負責，審視其正確性後才能使用。

AI生成內容偵測工具，只能作為初步參考

真實測試：GPTZero 也會誤判

舉例一：一段「非AI生成」的文字經GPTZero檢測，判定80%機率為人創作——判斷正確。

舉例二：一段「確實由AI生成」的文字，GPTZero卻判定74%機率為人創作——判斷錯誤。

偵測工具本身也是AI，準確度存在誤差。教師應謹慎使用判定結果，並參酌學生平時表現綜合判斷，避免僅憑偵測結果指控學生違規。

偵測工具準確度

僅供參考

建議搭配自我揭露引註機制（AI名稱、版本、Prompt紀錄），比單靠偵測工具更能對生成內容負責。

判斷AI使用品質的評量規準（簡化版）

評量項目	良好 Good	待改進 Need Improvement
正確性	內容經查核完全正確，有可靠來源支持	答案仍有錯誤，找不到相關資訊支持
無偏見歧視	內容沒有偏見與歧視，用語禮貌	內容出現偏見與歧視，用語有待改善
符合學習目標	內容與學習主題高度相關	內容與學習主題相關性不足
批判與創意思考	經過思辨且具創新價值	內容以AI生成為主，未經檢視
保護個人資訊	完全保護個資，避免外洩敏感資訊	知道重要性，但無法完全做到

資料參考：教育部中小學數位教學指引3.0版，表5「應用生成式AI判斷生成內容品質的評量規準」

大綱三・AI與資料保護・班級共識

班級／校園AI使用公約，怎麼一起訂？

和學生一起討論：「如果可以使用生成式AI，會有什麼好處？又有什麼風險？」

人為什麼需要學習？AI能取代這件事嗎？

使用AI時，我們共同遵守的規範有哪些？

AI生成內容如何查核？由誰負責把關？

這些風險若不解決，會帶來什麼影響？

案例：陸製App的資料外洩風險



害國家資通安全產品
及使用。

學生資料的保護，傳統與AI雙管齊下

- 認清手上資料的分級，機密資料妥善存放與銷毀，傳輸多一分小心
- 牢記AI六大風險：正確性、可溯源性、事實性、生成性、思辨性、風險性
- 絕對禁止將學生個資、機密公文輸入公開AI工具
- 使用AI務必揭露引註，並對生成內容負責；偵測工具僅供參考
- 陸製AI工具不得用於公務，教學應用仍須遵守資安法規紅線

04

大綱四

遇到狀況怎麼辦

每一位您，都是校園最關鍵的數位消防員



大綱四

什麼情況算是「資安事件」？

系統異常

滑鼠自動亂飄、螢幕異常閃動或當機。

檔案異常

檔案打不開或副檔名被改變，疑似遭加密。

帳密異常

密碼沒打錯卻登不進去，或出現不明時段的登入紀錄。

誤點釣魚信件

收到假冒單位的信件，且不小心點了連結或輸入帳密。

誤傳機密資料

不小心把機密公文或個資傳到外部或錯誤的群組。

插入不明USB

插了來路不明或撿到的隨身碟到公務電腦。



心理建設

掩蓋火苗，
只會燒掉整間辦公室

我們都是人，人都會犯錯。打翻燭火不可怕，馬上喊救命，大家一起滅火就沒事了。請將「遇到資安事件」比喻為「辦公室角落起火了」——第一時間按下警報器，而不是自己拿報紙偷偷把火包起來藏好。

延誤通報 vs. 迅速通報，代價天差地遠

隱瞞不報

- 行動：紙包不住火，假裝沒看到
- 結果：機密外洩、系統全面癱瘓，甚至波及其他單位
- 法規後果：依資通安全管理法第28條，知情不報等同幫兇，面臨行政懲處

迅速通報

- 行動：發現異常，立刻按下警報器
- 結果：災情迅速控制，校園資料保全
- 法規結果：您保護了學校，迅速通報甚至可能依規定減輕責任或獲得肯定

真實案例：隱瞞資安事件的代價



出的慘痛代價。

第一時間自救三步驟：拔、停、報

STEP 1



拔 Disconnect

立刻拔除網路線或關閉Wi-Fi，物理隔離，不讓問題擴散到其他同事的電腦。

STEP 2



停 Preserve

絕對不要關機或重新開機！保持現狀，保留鑑識人員追蹤軌跡所需的證據。

STEP 3



報 Report

立刻透過學校通報管道，聯繫資訊組 / 資安窗口，說明狀況並請求協助。

黃金1小時：依資通安全事件通報及應變辦法，知悉事件後必須於1小時內完成通報。

大綱四

通報時，請說清楚「人事時地物」

人

這是誰的電腦？登入的是哪個帳號？

事

發生了什麼異常狀況？做了什麼操作？

時

大約什麼時候發生 / 發現的？

地

設備位置在哪裡？部門或財產編號？

物

有沒有異常畫面，例如釣魚信件或勒索訊息？

加分技巧

用手機拍下異常畫面，是最完美的保留現場方式。

迅速通報是英雄，隱瞞不報是災難

- 資安事件不是電影情節，日常的「怪怪的」異常都值得通報
- 隱瞞才是最大的傷害，火苗要在燒大之前及早撲滅
- 法規要求：知悉事件後1小時內完成通報
- 自救三步驟：拔網路、停操作（不關機）、報資訊組
- 通報時說清楚人事時地物，附上照片證據更完整；資安不是資訊組一個人的事，同事間互相提醒也是防護的一環

四大綱，四個帶得走的關鍵字

大綱一　為什麼資安跟我有關

資安是全體教職員的法定責任，社交工程「停、看、想」就能破解。

大綱二　日常工作中的小習慣

密碼像牙刷、螢幕要上鎖，AI也要用對方法，好習慣天天做。

大綱三　學生資料要怎麼保護

認清資料分級、傳輸多一分小心；學生個資絕不輸入公開AI工具。

大綱四　遇到狀況怎麼辦

黃金1小時，拔、停、報，迅速通報就是保護自己與學校。



謝謝大家，你們就是校園最堅強的防線

再厲害的駭客，也怕您第一時間按下警報器；再新穎的AI工具，也需要您把關使用的分寸。守護校園資安，從您我的每一次點擊開始。

Q & A

交流與討論

關於資安防護或生成式AI的使用，您還有什麼想提出來討論的？

帳號密碼管理的疑問？

AI使用範圍怎麼拿捏？

遇到疑似詐騙該怎麼辦？

歡迎自由提問，一起討論！

參考資料

延伸閱讀與法規依據

教育部中小學數位教學指引 3.0 版

第肆篇：應用生成式AI輔助教學之說明（113年）

中小學使用生成式人工智慧注意事項

教師、行政人員及家長版 / 學生版｜教育部113.07.01臺教資(三)字第1132702614號函

高級中等學校學生學習評量及學習歷程檔案使用生成式人工智慧注意事項

教育部113.12.13臺教授國部字第1135406551號函

資通安全管理法、個人資料保護法

全國法規資料庫 law.moj.gov.tw