



順德聯誼總會鄭裕彤中學

Shun Tak Fraternal Association Cheng Yu Tung Secondary School

人工智能素養與守護學生網絡安全網上研討會

守護數位時代的師生安全，構建安全與創新並進的智慧校園

陳永德助理校長

08-10-2026

中學資訊素養與網絡安全教育的校本經驗分享

- 由「知道風險」走向「在真實情境中作出安全選擇」
- 從學生 / 教師的真實風險，到課程設計，再到課堂實踐



本次分享的三大核心焦點

1 師生常見資安安全陷阱



2 Cyber Security 課程融入



3 課堂實踐與經驗總結



本次分享的三大核心焦點

01 | 我們面對甚麼？

學生與教師最常遇到的網絡安全問題

不只講「駭客」，更聚焦日常使用中的判斷、習慣與責任。

02 | 怎樣教進課程？

把 Cyber Security 由「一次性宣傳」變成可持續的學習內容。

知識 × 技能 × 態度 × 情境。

03 | 課堂怎樣做？

分享校本資訊素養 / 數字教育課堂的設計思路。

讓學生由「答對」走向「做得到」。



1. 師生最常遇到的網絡安全問題



學生層面：四大常見數碼陷阱

1 社交工程 (Social Engineering)



師生最常遇到的 網絡安全問題

2 帳戶與身份 (Accounts & Identity)



教職員層面

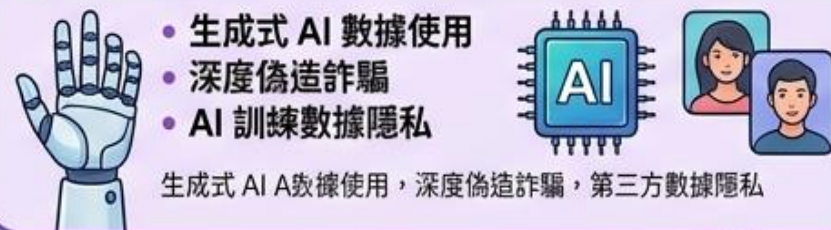


網絡安全 (Cybersecurity)

3 私隱與數據 (Privacy & Data)



4 AI 策隱與數據 (AI, Privacy & Data)



網絡安全建議：強密碼、多因素驗證、保持警惕、軟件更新

1. 師生最常遇到的網絡安全問題

■ 學生層面：四大常見數碼陷阱

社交工程

釣魚訊息
冒充老師 / 同學 / 平台
遊戲虛實詐騙
「立即處理」式壓力

帳戶與身份

弱密碼 / 重複密碼
帳戶共享
多重驗證與復原設定

私隱與數據

個人資料外洩
公開分享位置 / 相片
第三方 App 權限

內容與 AI

假資訊 / 深偽
AI 生成內容
版權、引用與數據倫理



1. 師生最常遇到的網絡安全問題

- 建議將資訊素養拆成四種可觀察的能力
- 「安全」的終點不是學生永遠不犯錯，而是犯錯後懂得及時止損與求助。

辨識

我能否察覺可疑訊息？

關鍵字：來源、語氣、連結、要求、情境

驗證

我會不會停一停，再查證？

關鍵字：第二來源、官方渠道、反向查證

保護

我知道如何降低暴露風險嗎？

關鍵字：密碼、MFA、權限、更新、備份

求助

遇到問題，我知道向誰求助嗎？

關鍵字：停止、保留證據、通報、復原





教師與校務層面：防禦漏洞與挑戰



1. 偽冒機構釣魚電郵



1. 偽冒機構釣魚電郵

2. 密碼管理與跨平台重用



2. 密碼管理與跨平台重用

3. 雲端學生資料管理失當



3. 雲端學生資料管理失當

1. 師生最常遇到的網絡安全問題

■ 教師與校務層面：防禦漏洞與挑戰



1. 偽冒機構釣魚電郵

詐騙者偽冒教育局或校務系統誘騙登入憑證。

2. 密碼管理與跨平台重用

個人帳號與學校公務電郵共用弱密碼風險。

3. 雲端學生資料管理失當

共享檔案權限設定過於寬鬆導致資料外洩。



2. 如何落實 Cyber Security 議題放到課程



如何落實 Cyber Security 議題放到課程：五步教學法

IMPLEMENTING CYBER SECURITY INTO THE CURRICULUM: A 5-STEP TEACHING FRAMEWORK

1 情境 (Context)

引入現實生活中的案例，建立學習動機



引入現實生活中的案例，建立學習動機

例如：網絡釣魚攻擊

2 概念 (Concepts)

教授核心原則、定義和理論



3 操作 (Operation)

實際演練、模擬或使用工具



4 反思 (Reflection)

討論、總結、評估學習成果



5 遷移 (Transfer)

將所學應用到新的或實際的情境中



2. 如何落實 Cyber Security 議題放到課程

- 課堂模式可分拆為 5 小步：



2. 如何落實 Cyber Security 議題放到課程

課程設計原則

- 少講「危險清單」，多設計「需要作判斷的任務」
- 每次課堂只聚焦 1-2 個安全行為，形成累積式學習
- 把 Cyber Security 與資訊素養、AI 素養、媒體素養連結



2. 如何落實 Cyber Security 議題放到課程

- 可融入不同科目的 Cyber Security，在原有課程中嵌入

資訊科技

帳戶安全、網絡威脅、資料保護、AI 與網絡安全

中文 / 英文

釣魚訊息語言分析、假資訊、來源與論證

公民 / 公經社

數位公民、私隱、網絡欺凌、平台責任

數學 / STEM

機率與風險、密碼強度、資料與演算法

班主任 / 德育

數位足跡、求助流程、網絡禮儀與責任



3. 本校資訊素養與數字教育課堂分享

- 從理論教學到體驗式學習：實際課堂設計與推行經驗



3. 本校資訊素養與數字教育課堂分享

名稱
📁 A 正確使用電子設備教學
📁 B 筆記摘錄教學
📁 C 人工智能導論課程
📁 D 校本文書處理軟件 - 演示軟件
📁 E 校本文書處理軟件 - 文書處理軟件
📁 F 校本文書處理軟件 - 試算表
📁 G 校本Microbit - 遊戲開發
📁 H 認識電腦系統結構

名稱
📁 A 優化筆記全攻略
📁 B 人工智能的局限與倫理
📁 C 數碼時代的挑戰與責任
📁 D 校本沉浸式互動世界
📁 E 互聯網的結構
📁 F AI漫畫家養成計畫 (中史科 x 電腦科跨...
📄 desktop.ini

名稱
📁 A 校本人工智能教材：人工智能與機器學...
📁 B 創意 App 製造機
📁 C 初創 AI 互動遊戲
📁 D AI 歌曲創作
📁 E 「穿梭順德 - 時光旅人」專題
📁 F 人工智能與Python

人工智能導論課程 01

初探AI - 它到底是什麼？怎麼工作？

學習目標



態度 (A)

- 建立對AI科技的批判性思維
- 養成負責任的AI使用態度
- 形成正確的資訊倫理觀念

AI的主要限制



會犯錯 (產生「幻覺」)



知識有截止日期



有偏見



不懂常識

判斷所生成的結果是否正確？



「我們如何判斷AI生成的結果是否正確？」



內容來源可信嗎？



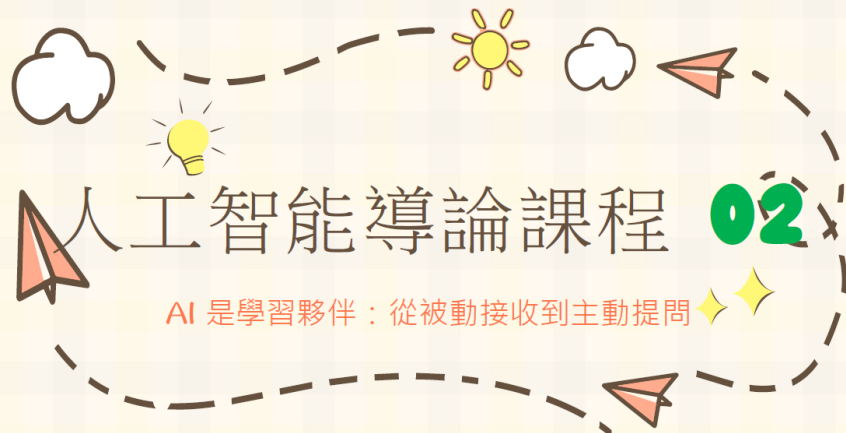
有沒有邏輯矛盾？



時效性如何？



存在偏見嗎？



人工智能導論課程 02

AI 是學習夥伴：從被動接收到主動提問

學習目標

-  緊記使用 AI 教自己做功課的 3 大核心原則
-  培養學術誠信、資訊素養
-  必須用常識、課本知識或可靠來源交叉驗證

關鍵問題

- 作業不會做時，你會直接搜尋答案還是問AI？
- 直接抄襲AI生成的作文，算善用科技還是作弊？



使用 AI 教自己做功課的 3 大核心原則

1. AI 是起點，不是終點
2. 你必須擁有最基本的了解
3. 永遠保持批判與驗證

人工智能的局限與倫理 01

中二級 電腦科

LIMITATIONS & ETHICS OF AI

態度 (A)

- 核心實踐指南
- 負責任使用：分享前務必查證事實，不散佈未經證實的謠言與恐懼。
- 不盲目轉發：拒絕當標題黨，點進去內文看清楚，思考動機後再分享。
- 尊重版權與資訊來源：轉載時明確標註原作者與出處，不任意重製或改作。



LIMITATIONS & ETHICS OF AI

知識 (K)

- Fact Check (事實查核) 的基本方法：面對 AI 時代的資訊爆炸，自主查核是防止被誤導的關鍵技能。
- 多方驗證：至少交叉比對三個獨立、權威的信源，避免單一來源偏誤。
- 溯源追查：尋找原始文獻、官方聲明或研究報告，而非二手二手傳播。
- 反向搜尋：利用 Google 進行圖片或影片反向檢索，確認是否為舊圖新用或深偽變造。
- 查核工具：善用第三方事實查核機構（如：台灣事實查核中心、MyGoPen、Cofacts 真的假的）。

LIMITATIONS & ETHICS OF AI

任務 3

- 請老師現在於 AI 平台中輸入「試生成以順德聯誼總會鄭裕彤中學為中心的寶琳區的地圖」

- 資料正確嗎？
- 有沒有時差？
- 有沒有 AI 幻覺？



As

人工智能的局限與倫理 02

中二級 電腦科

LIMITATIONS & ETHICS OF AI

⚠ 任務一

- 討論如何可以避免騙案落在自己身上？
- 科技幫手？
- 自己警覺？
- 可行方法？



LIMITATIONS & ETHICS OF AI

學習目標

- 讓學生識別 AI 的多層次局限
- 讓學生能掌握應對AI詐騙的「Fact Check」驗證技能
- 釐清生成式AI的版權爭議與法律責任
- 恪守校內AI使用守則，實踐負責任的應用

LIMITATIONS & ETHICS OF AI



香港真實案例：耳聽未必為憑

- 騙徒AI扮聲設呃錢陷阱
- <https://www.youtube.com/watch?v=cNLoyr6hicc>



LIMITATIONS & ETHICS OF AI

科技輔助工具

- 國家反詐中心 App：官方應用程式已上線「AI 鑑真查驗」功能，支持上傳可疑語音、影片進行 AI 溯源甄別。



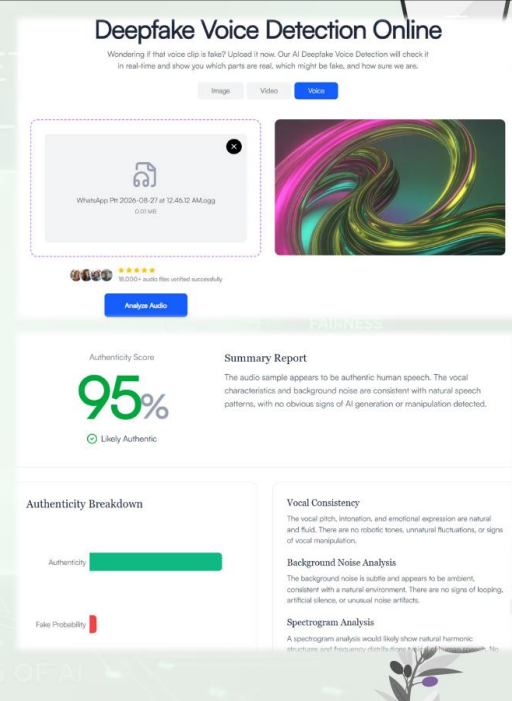
香港 Deepfake 詐騙

- <https://news.now.com/home/local/player?newsId=588936>
- 不要把「影片很真」當成「事情真的發生」。
- 遇到投資、轉帳、身份要求時
- 必須使用獨立渠道核實。



任務二

- 嘗試透過科技輔助工具，分析兩段錄音的真偽
- <https://undetected.ai/ai-voice-detector>
- 分析：人工智能的局限與倫理 02 錄音 A 和 B



校內 AI 使用守則

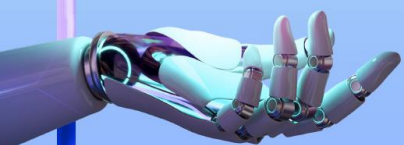
- 學生手冊 P.15-16

生成式人工智能可接受使用政策	
本校認識到生成式人工智能 (Generative AI) 如 ChatGPT、DeepSeek 等工具，在教育領域的潛力與挑戰。本校持開放及積極的態度，鼓勵學生探索及善用此類工具以輔助學習，並培養資訊素養及創新思維。與此同時，本校堅守學術誠信的核心價值，所有學生提交的課業及評估，皆應真實反映其個人學識與努力。本政策旨在為學生及家長提供清晰指引，確保在善用科技的同時，不違背學術誠信的原則。 1 使用原則： - 學術誠信：學生必須對自己的學習成果負責，誠實地呈現自己的思想與創作，抄襲或由他人 (包括 AI) 代筆是絕不容許的。 - 批判性思維：學生應批判地評估 AI 生成的資訊，學習核實其準確性、偏見和時效性，而非全盤接收。 - 負責任使用：學生在使用 AI 工具時，必須遵守版權法，並保護個人及他人的私隱，不得輸入敏感或機密資料。同時，嚴禁利用 AI 進行惡作劇、欺凌、騷擾或損害他人聲譽的行為。 - 創新探索：鼓勵學生將 AI 工具融入學習中，作為提升效率、激發創意及深化理解的輔助。 2 建議的應用方式： - 腦力激盪：針對一個主題，尋找不同的切入點、觀點或關鍵詞。 - 資料搜集：快速了解一個陌生課題的商業知識或基本概念，但必須透過可靠來源核實。 - 學習輔助：總結冗長或艱深文本的要點、解釋複雜的科學概念、數學原理或歷史事件。 - 語言潤飾：檢查文法、拼寫錯誤，或改進句子結構，以提升文章的可讀性。 - 編程輔助：理解代碼邏輯、修訂或學習新的編程語法。	
3 禁止的應用方式： - 直接抄襲：將 AI 生成的文字、圖像或代碼，直接複製並當作自己的原創作品提交。 - 代寫功課：輸入功課題目，要求 AI 為你完成整份或大部分的功課。 - 未經許可的評估中使用：在測驗、考試或老師明確禁止使用 AI 的課業中，擅自使用相關工具。 - 偽造資訊：使用 AI 偽造數據、引文或參考資料。 - 侵犯私隱：輸入任何個人、同學、老師或家庭的敏感或私人資料。 - 創作或散播虛假內容：利用 AI 製作虛假資訊、不實圖像或聲音，用作惡作劇、欺凌、騷擾，或損害他人聲譽。 4 註明使用 AI 方式： - 若老師允許在課業中使用 AI，學生必須在提交時清晰註明，並在功課的末尾或指定位置加入聲明。此聲明應包括：[DeepSeek、豆包] 輔助完成以下部分： 1. [用 DeepSeek 為專題報告尋找初步資料及圖表] 2. [用 DeepSeek 檢查英文作文的文法及拼寫錯誤] 3. [用 豆包 生成插圖] - 高中學生須注意：若在完成香港中學文憑考試後課業過程中曾使用人工智能工具，必須與其他參考資料一樣，清楚註明出處。學生可參考「香港中學文憑考試校本評核簡介」小冊子中關於引用及註明資料出處的示例 (https://www.hkeaa.edu.hk/tc/sba/) (以考評局最新公佈之指引為準) 5 違反政策的後果： - 任何違反本政策的行為，將被視為學術不誠實。 - 學校將根據現行的校本紀律處分程序處理，可能的處分包括：該份課業給予零分、紀律處分。 - 科技日新月異，本政策將會每年檢討一次，並根據最新發展作出修訂。	

校本人工智能教材

人工智能與機器學習 01

中三級電腦科



第四部份：人工智能素養



安全、守法與正確使用

安全第一

保護個人帳號密碼。不隨意在不明 AI 平台輸入敏感隱私數據。

遵守法律

明白 AI 生成內容的版權歸屬，不利用 AI 進行欺詐或傳播謠言。

正確使用

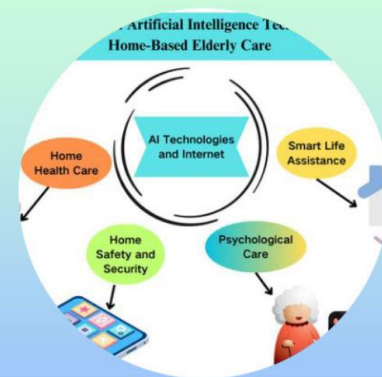
AI 是輔助工具而非替代品，不應依賴它完成所有思考，避免學術不端。

同理心與科技良知

「同理心」是讓 AI 變溫暖的關鍵。

思考一下：如何利用圖像識別技術，幫助視障人士辨認過馬路的紅綠燈？或幫助長者管理藥物？

科技不應只為方便，更應為了改善生活。



3. 本校資訊素養與數字教育課堂分享

- 課堂實踐：沉浸式模擬演練與工作坊



模擬攻防挑戰賽

學生分組扮演檢測員，找出模擬 社交媒體 / 郵件中的10個安全漏洞。

時事新聞案例拆解

引入近期真實校園或社會資安事件進行批判性小組討論。

互動式安全評估問答

運用即時課堂平台進行定性測驗，即時檢視學習成效。

三個帶得走的訊息

- 把網絡安全教育由「提醒」變成「能力」

01 | 安全教育要真實

用學生每天遇到的訊息、平台、AI 和帳戶情境教學。

越貼近生活，越容易遷移。

02 | 安全教育要可實踐

不要只問「你懂不懂」，要讓學生做判斷、找證據、作選擇、處理錯誤。

03 | 安全教育要成文化

學生會忘記規則，但可以養成習慣。

全校共同語言 + 清晰求助流程 + 持續演練。



謝謝！

- 守護數位時代，最重要的不只是「避免出事」
- 而是讓師生有能力在面對未知時，作出更安全、更負責任的選擇。

