文件名稱	生成式人工智慧安全使用指引	機密等級	公開	版次	1.0

中山醫學大學

生成式人工智慧平台安全使用指引

1 目的

生成式人工智慧(AI)已廣泛應用於教學、研究、學習及行政工作；然而，使用過程亦可能涉及個人資料、機密資訊、智慧財產權、資訊正確性及資通安全等風險。為確保本校資訊資產、個人資料之機密性、完整性及可用性，特訂定本指引提供生成式人工智慧安全使用規範，提醒本校人員於使用時，應留意資通安全、個人資料保護及使用者責任，進而保障本校人員之權益。

2 適用範圍：本校人員、委外廠商提供服務之人員。

3 使用原則：

3.1 合法使用：應遵循相關法令及本校資通安全管理政策、個人資料保護管理政策與相關規範。

3.2 平台選擇：優先使用學校提供之平台（如 Microsoft Copilot）

3.3 資料保護：

3.3.1使用者應知悉輸入或上傳至生成式人工智慧平台之資料，可能被平台蒐集、儲存、處理或利用，並有遭未經授權之第三方存取、利用或揭露之風險。

3.3.2輸入或上傳至生成式人工智慧平台的資料，應以公開資料或經妥善去識別化且無法藉由其他資料重新識別特定個人之資料為限。

3.3.3不得將本校「限閱」以上等級之資料，以及其他未經授權公開之資料，輸入或上傳至生成式人工智慧平台，包括但不限於：

3.3.3.1 未公開之研究資料及實驗數據

3.3.3.2 財務、採購及人事資料

3.3.3.3 學生紀錄、成績及輔導資料

3.3.3.4 個人資料及醫療資訊

3.3.3.5 未公開之公務或內部資訊

3.3.3.6 帳號、密碼、API Key 及其他驗證資訊

3.3.3.7 受契約、法令或其他規範限制之資料

3.3.4前項所稱輸入或上傳之資料包括以提示詞、文字、文件、圖片、影像、聲音、程式碼或其他形式之內容，將資料提供與生成式人工智慧平台。

3.4 發布或分享前應審核：

生成式人工智慧平台產生的內容可能不正確、具誤導性、過時或包含虛構(AI 幻覺)、無法查證或帶有偏見之資訊，亦可能包含受著作財產權保護之內容。使用者不得完全依賴人工智慧產出，應於採用、發布、分享前自行查證、審核及修正，並對最終發布的內容負責。

3.5 程式及系統開發

3.5.1使用生成式人工智慧平台輔助系統開發時，仍應遵循本校資通安全管理制度(ISMS)遵循安全系統發展生命週期。

3.5.2未經核准，不得將未公開之原始碼、系統架構、設定檔、錯誤日誌、弱點資訊、測試資料、帳號權限、API Key 或其他機敏資訊，輸入或上傳至生成式人工智慧平台。

3.5.3生成式人工智慧產生之程式碼僅得作為開發參考。開發人員應進行人工審查、功能測試及安全性檢測，確認程式碼之正確性、安全性及適用性，並對最終採用之程式碼負責。

3.5.4採用生成式人工智慧建議之程式套件、函式庫、API 或其他第三方元件前，應確認其真實性、來源、版本、安全性、維護狀態及授權條款，不得直接安裝或引用未經確認之元件。

3.5.5生成式人工智慧產生之程式碼、指令、設定或其他內容，不得未經人工確認、測試及變更程序，直接於正式環境執行或部署。

3.5.6開發或導入連接本校資通系統、處理本校資料，或可自主執行操作之人工智慧應用前，應辦理必要之需求及風險評估，並確認其資料

存取範圍、權限設定、紀錄保存、人工監督及異常處理機制。

3.6 通報：當有跡象顯示可能有個資外洩、機密資料誤傳或資安事件發生時，應停止相關操作、保留必要紀錄，並儘速通知相關窗口。

3.6.1資安事件：

圖書資訊處網路通訊組（緊急應變暨技術支援組）

電子郵件信箱：cs1515@csmu.edu.tw、

聯絡電話：04-36097295。

3.6.2個資外洩事件：

個資保護申訴窗口（秘書室林小姐）

電子郵件信箱：cs1021@csmu.edu.tw

聯絡電話：04-24730022# 11021。

4 相關文件

4.1 人工智慧基本法

4.2 行政院及所屬機關（構）使用生成式 AI 參考指引

4.3 數位發展部《公部門人工智慧應用參考手冊》

4.4 中山醫學大學生成式 AI 於教學研究的學術誠信指引

資安暨個資重要宣導

安全使用生成式AI

守護校園資安與個資安全

使用 AI 工具前，請先確認您輸入的內容是否安全！

✓ 可以做的事	✗ 不可以做的事
盡量使用學校提供的AI平台 如：Microsoft Copilot	**不得輸入含有個資之提示詞、檔案** 如：姓名、學號、身分證、成績、照片、聯絡方式等，足以識別個人之資訊
輸入公開、去識別化的資料 如：公開的網頁內容、新聞、法規 公開的學術文獻、教材、研究摘要 匿名化 / 去識別化的統計數據 一般知識、概念、語言翻譯	**不得輸入機密或敏感資訊、醫療資訊** 如：未公開的研究資料、實驗數據、人事、財務、採購機密資料、內部文件、密碼、API Key、帳號資訊、病人姓名、病歷號、檢驗結果、影像等
驗證AI回覆的正確性 AI可能會有錯誤，請自行查證與判斷	**不得上傳機密或受保護之檔案** 如：合約、考卷、個資檔案、研究數據、公務資料等
善用AI提升學習與工作效率 如：資料整理、程式輔助、問題構思等	
遵守學校資安與個資保護規定 共同維護校園個人資料保護與資通安全	**不得利用AI從事不當或違法行為** 如：製作不實資訊、侵害他人權益等

⚠ 為什麼不能輸入或上傳含有個資或機密的資料？

資料可能被儲存、分析或用於模型訓練，致個資外洩、機密洩漏、違反法規，對個人與學校造成嚴重損害！

- 資料可能離開安全控制範圍
- 可能造成資料外洩與權益損害
- 可能違反個資法與相關法規
- 違規將可能面臨行政與法律責任

使用 AI 的小提醒

使用前： 確認資料是否合適、平台是否經核准 → **使用中：** 留意AI 回覆準確性 → **使用後：** 妥善保存與管理產出內容 → **尋求支援：** 如有疑問可洽詢圖書資訊處

延伸閱讀：

https://blog.trendmicro.com.tw/?p=92027 【與 AI 聊天也會被詐騙？7 招避免個資外洩 + ChatGPT 等隱私設定指南】

https://www.cw.com.tw/article/5137232 【把照片上傳到ChatGPT安全嗎？】