香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

第十四屆聯合教育會議

教育界加強AI治理及防範個人資料外洩攻略

個人資料私隱專員
鍾麗玲女士

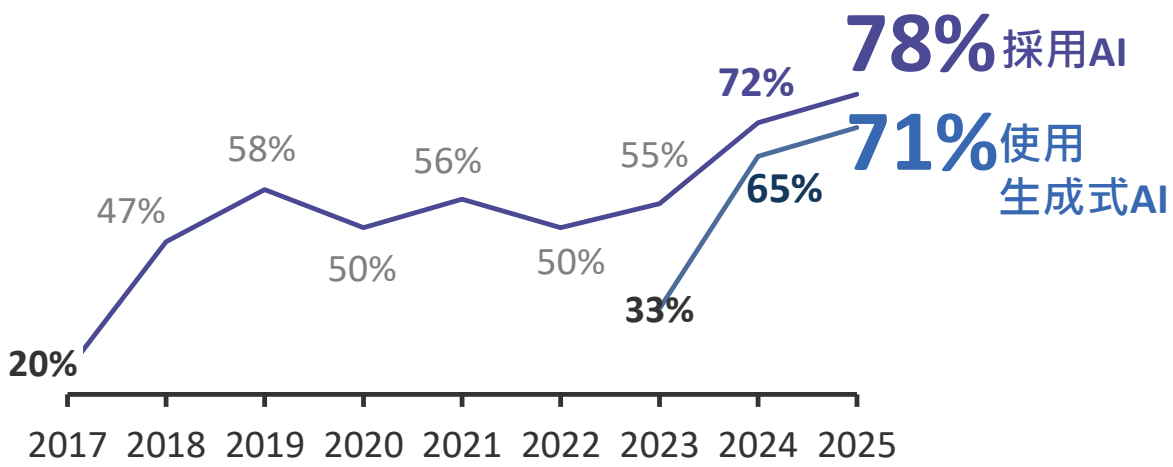
2025年12月12日

趨勢
機構正積極採用 AI；AI教育市場規模將會擴張

📈 全球機構AI（包括生成式AI）採用率於近年大幅上升

表示至少在一個商業功能上採用AI的受訪機構比例

全球企業， 2017-2025

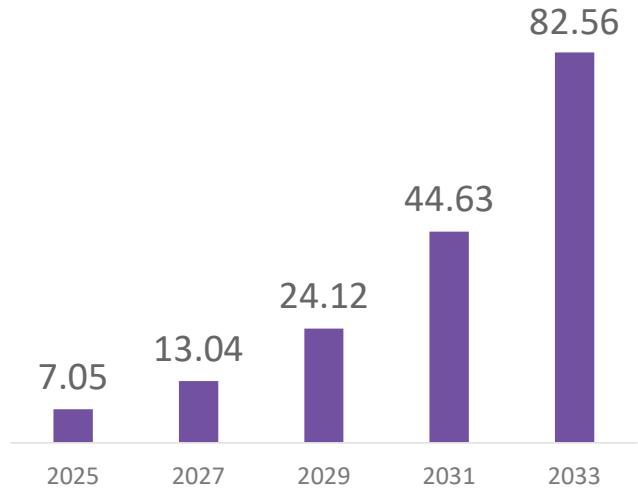


資料來源: McKinsey

🏛 有研究指AI教育市場規模將急速擴張

AI教育市場規模 (2025)

十億美金， 2025-2033

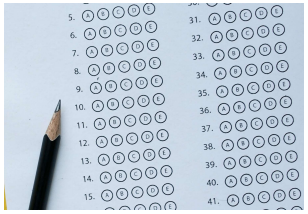


資料來源: Precedence research

用例1 - 教學輔助

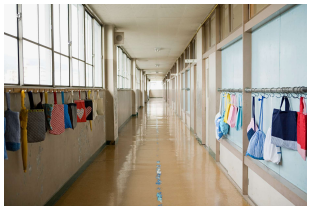
🏛 使用AI輔助教學的例子

生成教學資源



- 簡化複雜科學文獻，以配合學生程度
- 教案設計（輸入教學主題和時間限制以輸出教案）、簡報設計
- 草擬功課題目
- 模擬真實的語言環境，提高學生語言應用能力

支援行政工作



- 安排課程時間表、回答學生常見問題
- 持續管理政府公告和指引

資料來源: 教育局; PC Market；香港教育城； BusinessFocus

用例2 -評估學習情況

🏛 使用AI評估學生學習情況的例子

Quantity	Diversity	Originality	Total Mark
9	5	4	18
8	5	2	15
7	4	2	13

高效地評閱學生答案

- 進行初步評級並提出具體意見
- 例如：快速評改作文提供具體修改建議和指導

查看學生進度和分析強弱

- 系統提供學生強弱的評估報告，例如分析學生算術步驟有否出錯
- 因應學生錯誤之處，即時讓AI系統生成題目，讓學生加強操練

資料來源: 教育局；香港01

用例3 – 個人化學習

使用AI以提供學生個人化學習體驗的例子

學生生成式AI平台

- AI平台生成練習題，提供評估工具，學生從錯誤中分析不足之處
- 老師預設指令引導學生思考，而非直接提供答案
- 有小學使用平台後，學生英文寫作明顯進步；學生讚如私人補習老師

資料來源: 香港01

AI教學風波
美大學教授用生成式AI製作教材，引起學生不滿

事件發展

學生發現教授的教材有異
- 文字教材中出現疑似AI指令
- 圖片中人物肢體異常

質疑學校雙重標準
- 禁止學生使用，教授卻自行使用
- 指高昂學費是為接受真人教學，要求退款

校方處理
- 駁回退款
- **事件促使校方制定AI使用政策，要求註明使用AI並審核內容準確性**

資料來源: 新浪網

AI的私隱和道德風險例子

知情 / 訂明同意

要注意學生或家長就學生的個人資料會由AI處理方面，是否知情 / 有否給予訂明同意

資料使用目的

平台或會持續收集有關學生互動、表現甚至行為的數據，要注意當中個人資料有否被用於非收集用途的「新目的」

資料外洩

教師可能在家長或學生不知情的情況下，將學生的個人資料輸入AI；這些資料可能被儲存在不安全的系統、或用於訓練AI系統，使相關資料在其他用戶的對話中出現

資料收集過量

AI傾向於收集和保留盡可能多的數據，有機會涉及過量收集個人資料

數據安全

平台或存有大量有關學生的資料，包括其學習進度、錄音、含個人資料的AI對話，容易成為黑客目標

黑盒難題

AI使用者無法得知AI系統的內部運作邏輯，包括AI以甚麼準則評核學生的答案

公署的指引

公署因應AI的發展發布了不同指引

機構

（ 2021年8月 ）

（ 2024年6月 ）

（ 2025年3月 ）

公眾

（ 2023年9月 ）

《僱員使用生成式AI的指引清單》

🎯 目的

協助機構制定僱員在工作時使用生成式AI的內部政策或指引，以及遵從《私隱條例》有關處理個人資料的相關規定

✨ 特色

以清單形式呈現

作為良好的行事方式、機構可以制定與其價值觀及使命一致的內部政策或指引

僱員使用生成式AI的政策或指引的建議內容

01 範圍

02 保障個人資料私隱

03 合法及合乎道德的使用及預防偏見

04 數據安全

05 違反政策或指引

01 僱員使用生成式AI的政策或指引的建議內容 – 範圍

方面	內容
獲准使用的工具	**清晰訂明准許使用的生成式AI工具及應用程式**, 例如： • 公眾可用的AI工具或應用程式 • 內部開發的AI工具或應用程式
獲准許的用途	**清晰指明僱員可以使用生成式AI工具處理甚麼工作或活動**，例如： • 起草 • 總結資訊 • 生成文本、音頻及 / 或視像內容
政策適用性	訂明政策是否適用於**整個機構**；**指定部門**；**指定職級**；及 / 或**指定僱員**

02 僱員使用生成式AI的政策或指引的建議內容 – 保障個人資料私隱

獲准輸入的資訊種類及數量

提供清晰指示，說明：

✓ **可輸入至生成式AI工具的資訊種類及數量**

✕ **禁止輸入的資訊種類**

輸出資訊的獲准許用途

提供清晰指示，說明生成式AI工具所生成的資訊（包括個人資料）的**獲准許用途**，以及僱員應否、何時及如何在進一步使用這些個人資料前將其匿名化

輸出資訊的獲准許儲存方式

要求僱員根據機構的**資訊管理政策**儲存資訊和**資料保留政策**刪除生成式AI工具所生成的資訊

遵從其他相關內部政策

確保**使用生成式AI的政策與機構的其他相關內部政策一致**

03 僱員使用生成式AI的政策或指引的建議內容 – 合法及合乎道德的使用及預防偏見

違法行為

僱員不能為進行非法或有害的活動使用生成式AI工具

強調僱員有責任擔當審查員

準確度及核實

強調僱員需要**核實AI所提供的資訊**

預防偏見及歧視

提醒僱員AI生成的結果可能帶有**偏見及歧視**

訂明**更正及報告機制**

加上水印 / 標籤

說明應**何時及如何**在AI生成結果上**加上水印或標籤**

04 僱員使用生成式AI的政策或指引的建議內容 – 數據安全

獲准許裝置

訂明准許僱員可用**哪些裝置**來**取用生成式AI工具**

保安設定

要求僱員保持**嚴格的保安設定**

獲准許使用者

訂明**可以使用**生成式AI工具的**僱員**

AI事故及資料外洩事故應變

要求僱員根據機構的**AI事故應變計劃報告AI事故**

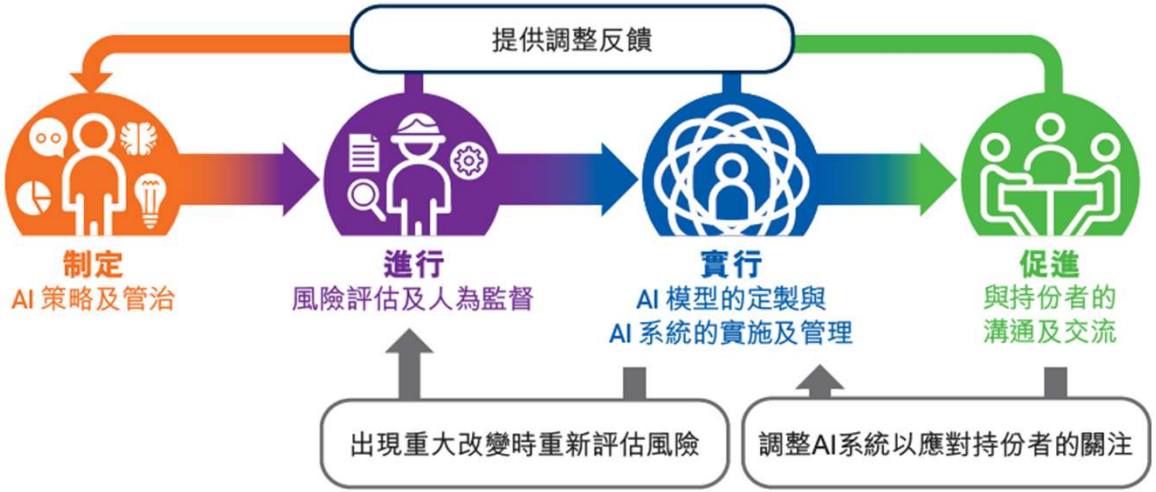
用戶憑證

要求使用**獨特且高強度的密碼**及**多重認證**

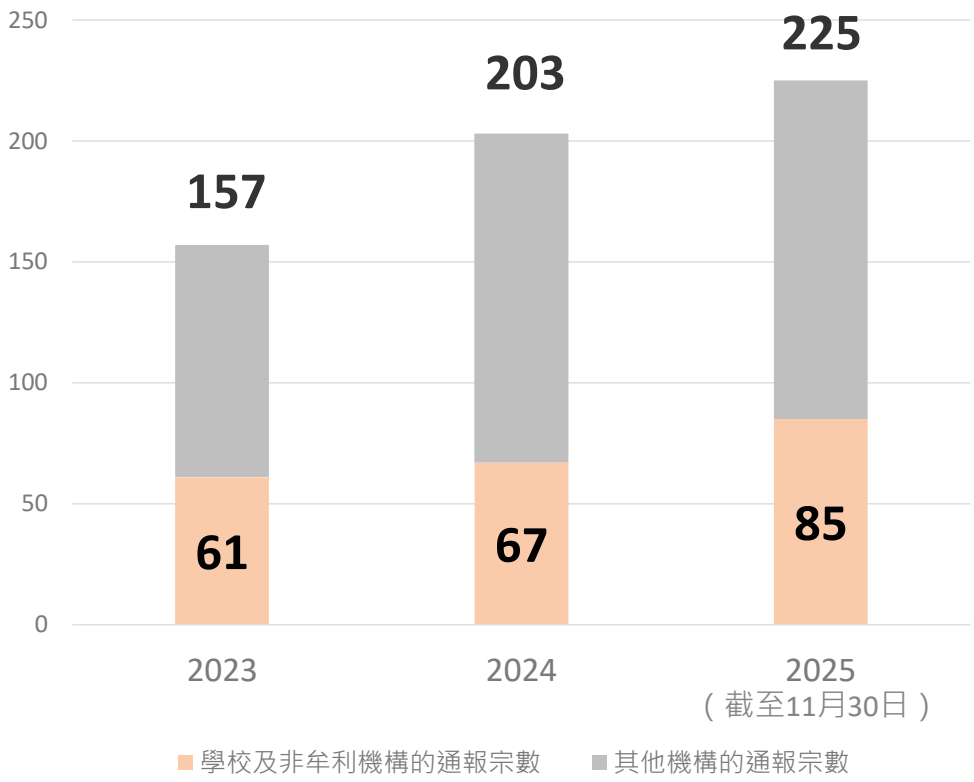
《人工智能 (AI): 個人資料保障模範框架》

協助機構遵從《私隱條例》的規定

向採購、實施及使用任何種類的AI系統（包括生成式AI）的機構，就保障個人資料私隱方面提供有關AI管治的建議及最佳行事常規



資料外洩事故通報趨勢



- 2024年，私隱專員公署接獲203宗資料外洩事故通報
- 當中來自學校及非牟利機構的個案佔67宗（約33%），比2023年上升約10%
- 於2025年首11個月，私隱專員公署共接獲85宗來自學校及非牟利機構的資料外洩事故通報，與去年同期相比增加24宗（約40%），佔整體個案總數約38%

法律責任
保障資料第4原則

資料外洩事故可構成違反《私隱條例》附表1的保障資料第4原則

保障資料第4(1)原則

資料使用者須採取**所有切實可行的步驟**，以確保所持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。

保障資料第4(2)原則

如資料使用者聘用 (不論是在香港或香港以外聘用) 資料處理者，以代該資料使用者處理個人資料，該**資料使用者須採取合約規範方法或其他方法**，以防止轉移予該資料處理者作處理的個人資料被未獲准許或意外地查閱、處理、刪除、喪失或使用。

學校資料外洩事故分享：個案(1)

一名中學教師沒有適當地設定內部檔案的存取權限

背景

- 一名中學教師在離職前將文件連同**117名學生的個人資料製成雲端範本供內部使用**。
- 然而，該名教師沒有適當地設定有關檔案的存取權限，以致**學生可以未經准許查閱相關檔案**。
- 當中載有學生的姓名、性別、就讀小學名稱、成績、跨境生和有特殊學習需要的學生標示及分班結果。

補救措施

- 停止了所有用戶建立或使用雲端的範本功能；及
- 制定守則述明教職員透過雲端分享檔案時需注意的事項，例如**確保在分享檔案之前設定存取權限**等。

學校資料外洩事故分享：個案(2)

即時通訊軟件帳戶遭騎劫

背景

- 私隱專員公署不時接獲有關社福機構及學校的資料外洩事故通報，表示用作與服務使用者、學生及／或學生家長通訊的**即時通訊軟件帳戶遭騎劫**，騙徒繼而盜用有關即時通訊軟件帳戶**假冒受害機構**，向通訊錄的聯絡人發送訊息企圖騙取金錢。

- 事件涉及**服務使用者、學生、學生家長及／或職員**的姓名及手提電話號碼等個人資料。

學校資料外洩事故分享：個案(2)

保障WhatsApp帳戶的措施

啟用WhatsApp雙重認證功能

定期在WhatsApp設定中檢查已連結裝置

切勿向他人透露任何密碼或驗證碼

小心誤按虛假的WhatsApp網頁版

切勿從非官方渠道下載及使用WhatsApp應用程式

一旦收到可疑訊息，先確認發送者的身分

切勿隨意打開連結或披露個人資料

學校資料外洩事故分享：個案(2)
復原遭盜用WhatsApp帳戶

1. 以你的手機號碼登入 WhatsApp

2. 輸入你於SMS短訊收到的 6 位數驗證碼來驗證手機號碼

3. 當你輸入驗證碼後，盜用你的帳戶的人便會被自動登出

- 如需輸入**雙重認證驗證碼**，而你不知道此驗證碼，那**可能是盜用你的帳戶的人已啟用雙重認證功能**
- 若你沒有此驗證碼，**等待7日後**便能登入你的帳戶

資料來源：WhatsApp

提升數據安全
學校可採取以下措施

- **制訂保障資料政策和程序**，並**加強保安措施**以保障個人資料；
- **採取措施及監管機制，確保教職員遵從**相關政策和程序的要求行事；及
- **為教職員提供全面的培訓**，加強他們保障個人資料私隱的意識，減低人為錯誤的風險。

PCPD HK

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

數據安全熱線
Data Security Hotline
2110 1155

數據安全快測
Data Security Scanner
https://www.pcpd.org.hk/Toolkit/tc/

數據安全專題網頁
Data Security Webpage
https://www.pcpd.org.hk/tc_chi/data_security/index.html

聯絡我們

查詢 2827 2827　傳真 2877 7026

網址 www.pcpd.org.hk

電郵 communications@pcpd.org.hk

地址 香港灣仔皇后大道東248號大新金融中心13樓1303室

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

追蹤我們
最新資訊

PCPD.org.hk