個人資料私隱專員公署及香港電腦教育學會
網絡研討會

人工智能於學校的應用與個人資料保障

鍾麗玲女士
個人資料私隱專員

2026年3月10日

守護私隱・改革創新
Protecting Privacy · Embracing Innovation

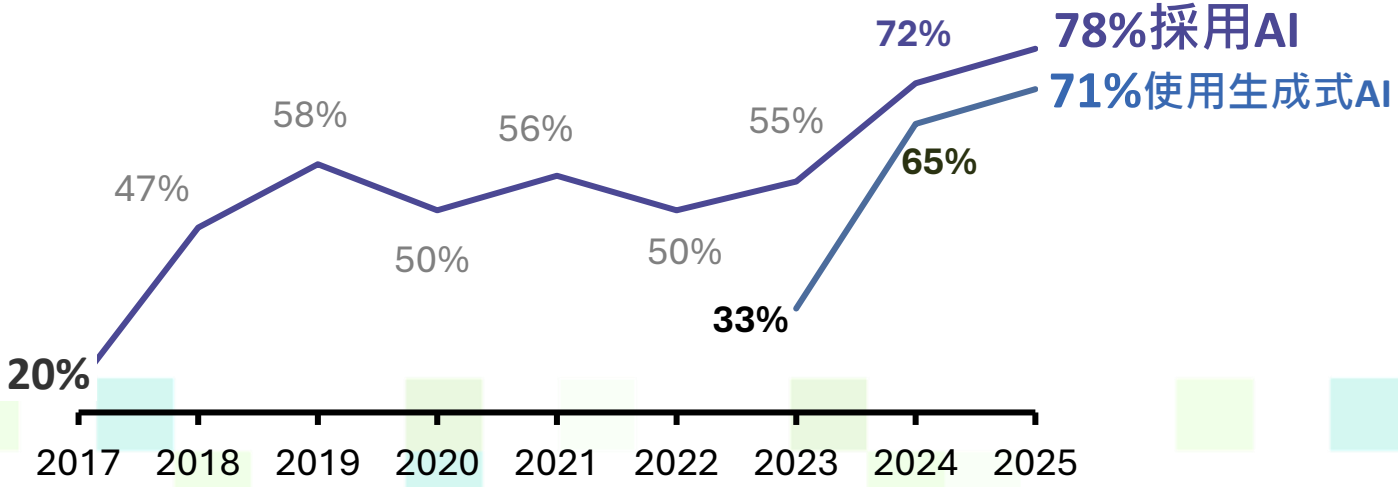
趨勢

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

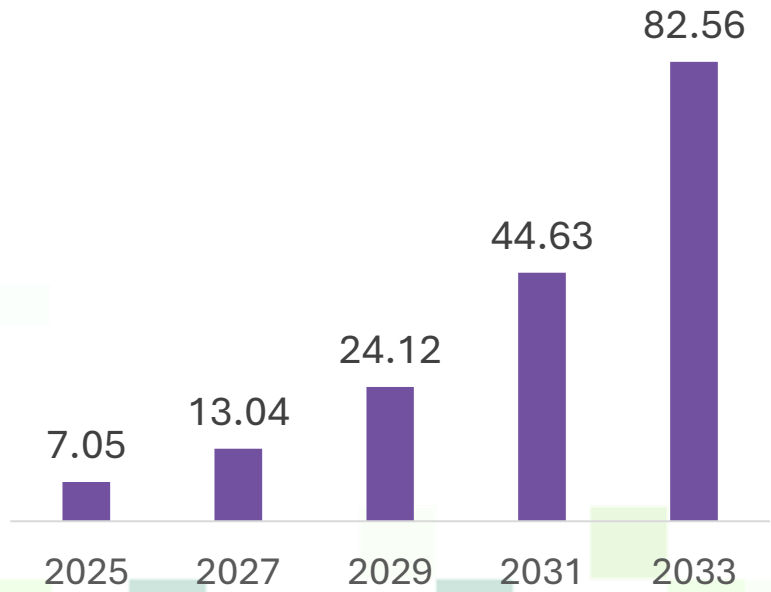


資料來源: McKinsey

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

趨勢

機構正積極採用 AI；AI教育市場規模將會擴張

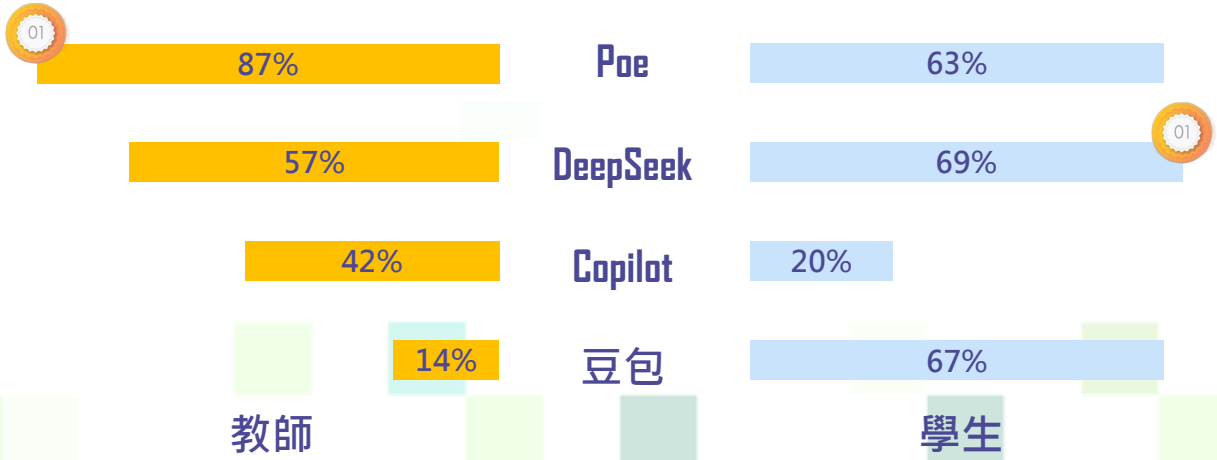
逾 90% 香港中小師生已用 AI 工具　無 AI 已不能學習工作　團體倡應用框架保障學生安全

團結香港基金最新調查顯示，香港中小學師生使用 AI 工具比例極高，教師達 91%，學生更高達 95%，反映 AI 已深度融入教與學過程。基金會於 2025 年 7 至 12 月期間，向中小學校長、教師及學生進行問卷調查，共收集 1,200 份有效問卷，當中學生佔 71%，教師佔 25%，參與學校以中學為主（90%）。調查結果顯示 AI 應用雖已普及，但也引發教師對學生思維能力發展及私隱保障憂慮。

資料來源: Unwirehk

香港中小學師生使用 AI 工具比例極高

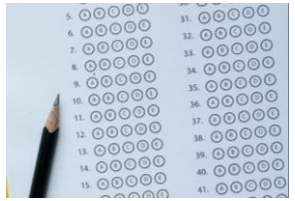
最常用的AI工具是Poe和DeepSeek 部分工具應用呈現世代差異



資料來源: 團結香港基金

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

資料來源: 香港01

生成式練習平台

- 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

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

科技

AI殺死大學? 教授ChatGPT教學逼瘋學生，怒告學校討要8000美元學費!

05月16日 18:44 新浪網

資料來源: 新浪網

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**

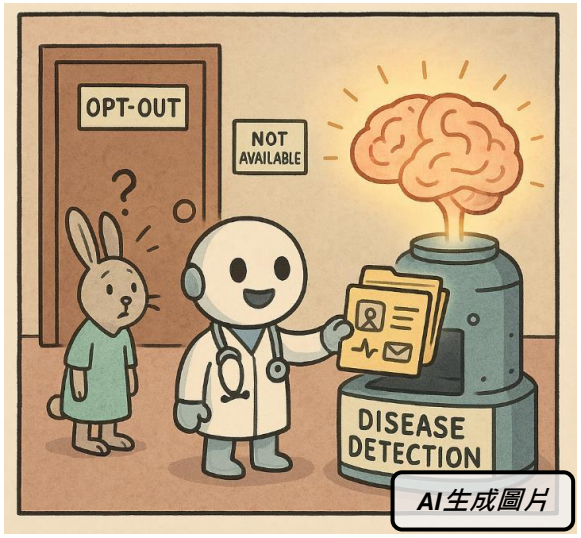
人工智能 (AI)帶來的私隱風險

資料外洩風險

AI系統如被用作**處理個人資料**，一旦設定或功能設計不當，可能導致**資料被公開**

資料收集過量

AI傾向於**收集和保留盡可能多的數據**，包括個人資料



資料的使用

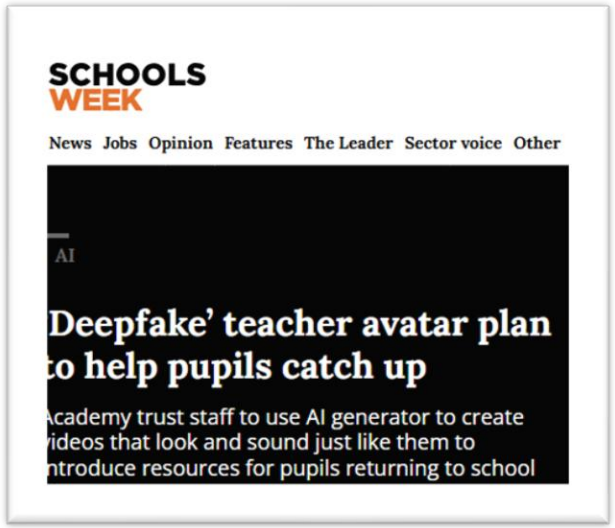
AI系統開發者在**資料當事人不知情或未得到其同意的情況下**，將其個人資料**用於訓練AI**

資料準確性

即使AI系統中儲存了**過時或不準確的個人資料**，開發者亦未必能夠更正或刪除這些資料

在校內使用深偽技術

建設性用途


SCHOOLS WEEK

News Jobs Opinion Features The Leader Sector voice Other

AI

Deepfake' teacher avatar plan to help pupils catch up

Academy trust staff to use AI generator to create videos that look and sound just like them to introduce resources for pupils returning to school

令學習更具沉浸感及趣味性

資料來源: Schools Week

濫用深偽技術的類型

影像性暴力

未經同學同意下，偽造同學的**露骨影像或影片**

詐騙

利用語音或影片**模仿父母、學生或教師**以**詐取**敏感的**個人資料**或進行**詐騙**

網絡欺凌/騷擾

憑空捏造令人尷尬的情況，以**羞辱或中傷同學**，令同學受情緒困擾

假新聞/虛假信息

利用深偽影片或影像**散播假新聞及假資訊**，**扭曲**同學對**事實的理解**或在同學之間**引起混亂**

深度偽造的濫用

近期AI聊天機械人被濫用作生成色情內容的事件在世界各地引起軒然大波

AI爭議｜印尼、馬來西亞憂慮AI生成色情內容　暫時封鎖Grok服務

科技
撰文：曾曉汶
發布時間：2026/01/12 12:00

調查馬斯克旗下Grok　涉於X平台生成色情深度偽

2026年1月11日　時事脈搏 國際

AI｜Grok涉色情內容或遭英國禁用X 馬斯克:打壓言論自由

美國富商馬斯克(Elon Musk)旗下人工智能(AI)聊天機械人Grok，被指生成涉及色情內容，印尼昨日宣布暫時封鎖Grok服務以保護婦女、兒童和大眾，成為全球首個全面封鎖Grok的國家。英國政府亦稱，若Grok不遵守當地法律，將考慮禁用馬斯克旗下社交媒體X。馬斯克批評英國政府法西斯(fascist)及打壓言論自由。

放大圖片

馬斯克旗下AI聊天機器人被指涉色情內容

2026-01-07 15:20:12 來源：新華網

新華社倫敦1月6日電　美國企業家埃隆·馬斯克旗下人工智能企業xAI的聊天機器人"格羅克（Grok）"，因新增圖像編輯功能被用戶用於生成涉及成年女性和未成年人的深度偽造色情內容。英國等多個國家對此予以譴責。

資料來源: 新華網；經濟日報；信報；香港01

Joint Statement on AI-Generated Imagery and the Protection of Privacy

23 February 2026

The co-signatories below are issuing this Joint Statement in response to serious concerns about artificial intelligence (AI) systems that generate realistic images and videos depicting identifiable individuals without their knowledge and consent.

While AI can bring meaningful benefits for individuals and society, recent developments - particularly AI image and video generation integrated into widely accessible social media platforms - have enabled the creation of non-consensual intimate imagery, defamatory depictions, and other harmful content featuring real individuals. We are especially concerned about potential harms to children and other vulnerable groups, such as cyber-bullying and/or exploitation.

資料來源: Global Privacy Assembly

應對濫用人工智能深度偽造技術

- 常見的深偽技術種類
- 在校內使用深偽技術
- 如何預防濫用或製作惡意的深偽內容：保障個人資料私隱的建議
- 學校及家長應如何處理深偽事故
- 潛在法律後果

常見的深偽技術種類

1 換臉

2 面部再現（傀儡）

3 人臉生成

4 同步口形

5 語音模仿

資料來源: CyberDefender; HKCert

如何預防濫用或製作惡意的深偽內容

保障個人資料私隱的建議

學校

1. 減少原材料

- **儘量減少發布**可以**清晰識別個別學生**的相片或影片
- **平衡保護私隱及發放資訊，儘量避免上載特寫肖像及高清相片**

2. 限制查閱

- **考慮**將學生的相片及影片**在學校管理的系統內分享**
- 定期**審視網站及社交媒體**，並**移除不再需要的內容**

3. 確保數據安全

- 將學生的個人資料儲存在**安全穩妥的平台**
- 採用**多重身份認證**

4. 制定應變計劃

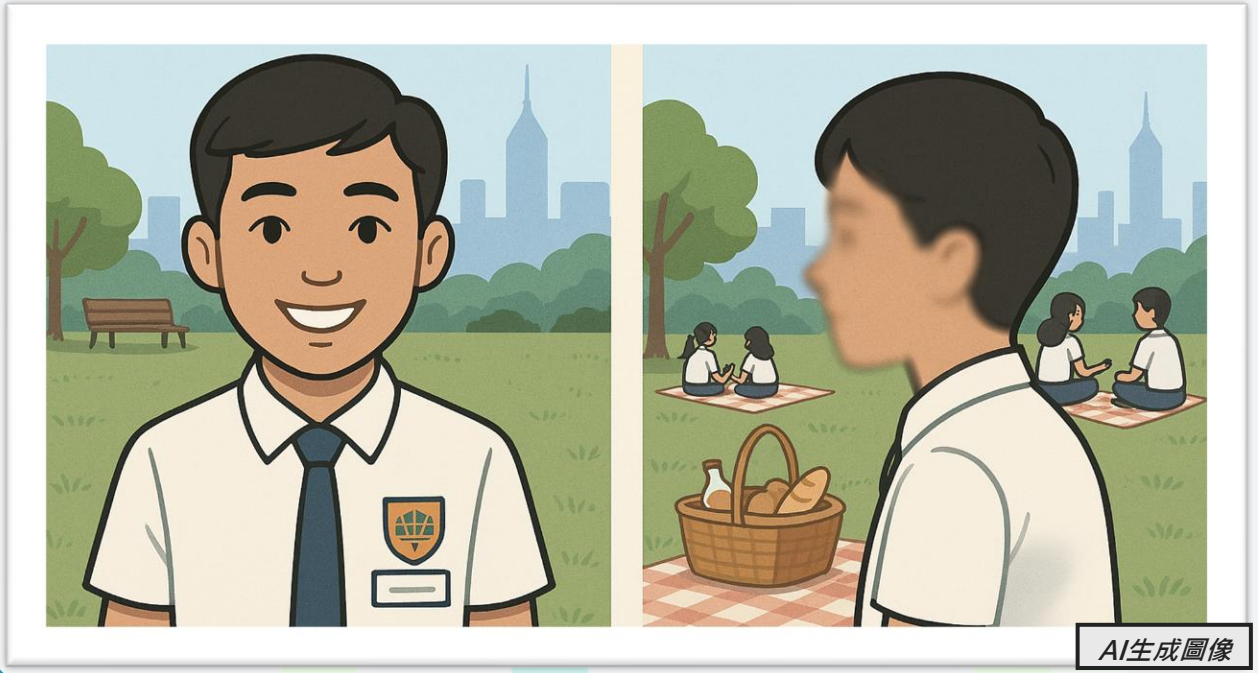
- 設立**清晰程序**應對深偽事故，並**組織危機處理小組**處理相關工作

5. 加強意識

- 為**教職員**提供**網絡風險培訓**
- 為**學生**提供**工作坊**，講解深偽技術

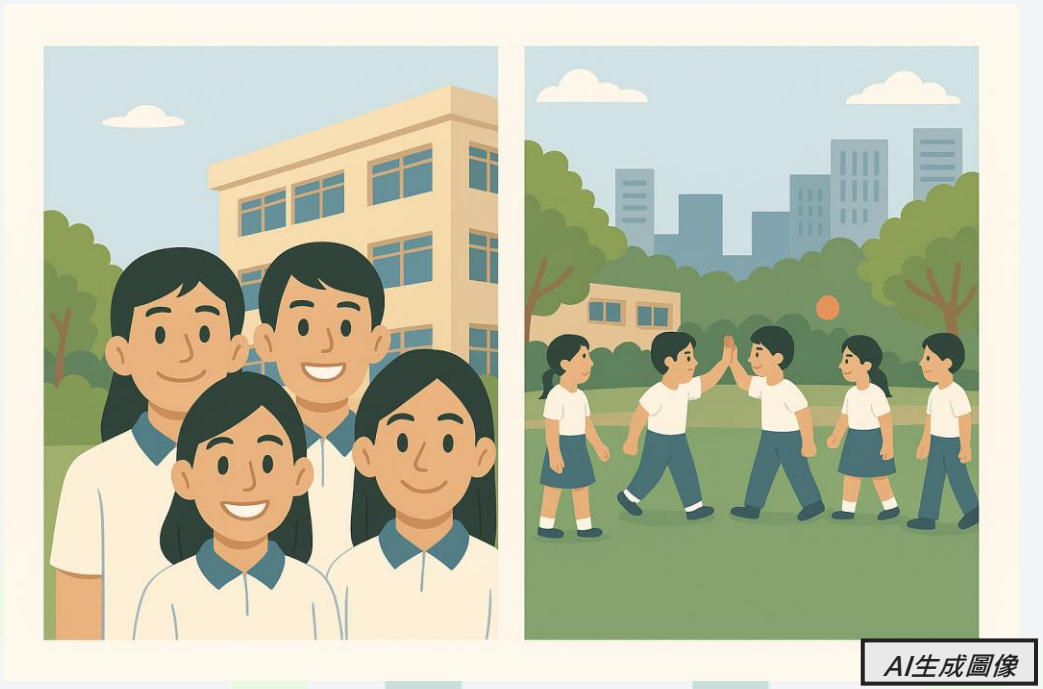
相片例子

例子1



AI生成圖像

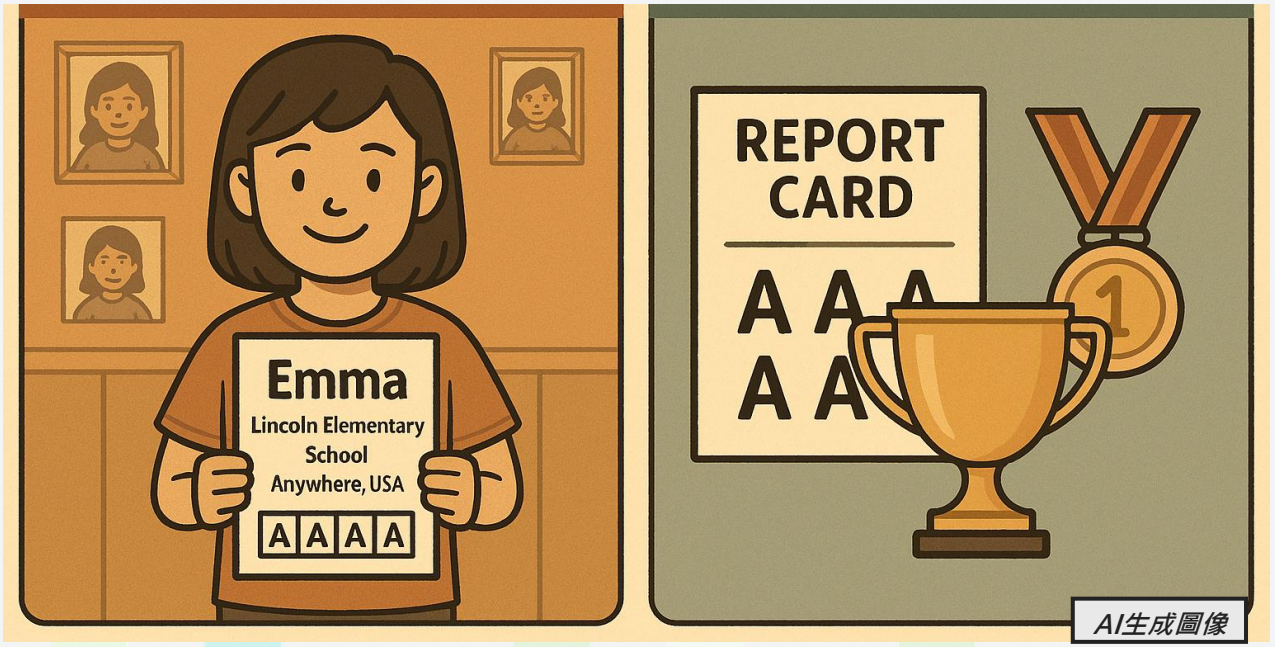
例子2



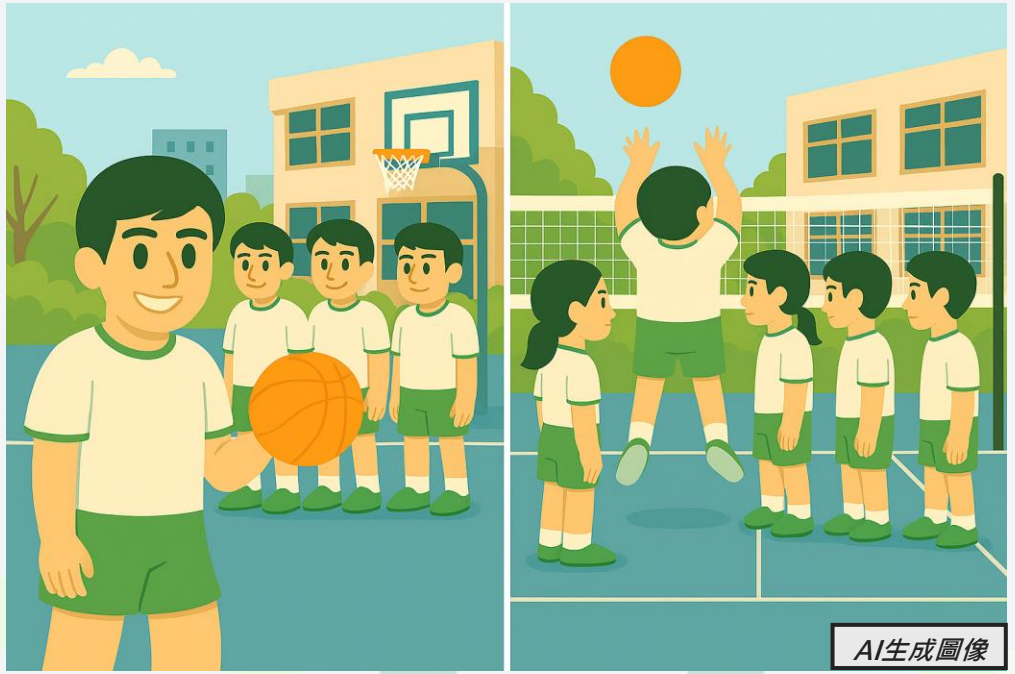
AI生成圖像

相片例子

例子3


Emma
Lincoln Elementary School
Anywhere, USA
AAAA
REPORT CARD
A A A
A A
AI生成圖像

例子4


AI生成圖像

學校應該如何處理深偽事故？

學校

優先考慮受影響同學的福祉
必要時尋求**專業支援**

妥善保管相關證據
並依循「**需要知道**」**知情原則**及**機密原則**處理

報告事故至學校管理層
或負責處理相關問題的**指定團隊**

指示學生
- **停止分享**深偽材料
- 盡快將材料**刪除**

調查
該些深偽材料是否**未經所涉人士同意**而製作及 / 或發布

通知受影響學生的家長或監護人

清晰地向製作者及發布者傳達
製作或分享惡意深偽材料可能帶來的**法律後果**

向警方和私隱專員公署查詢或報案
如懷疑涉及**罪案**，或**濫用個人資料**或「**起底**」的情況

其他公署因應AI的發展發布的指引

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

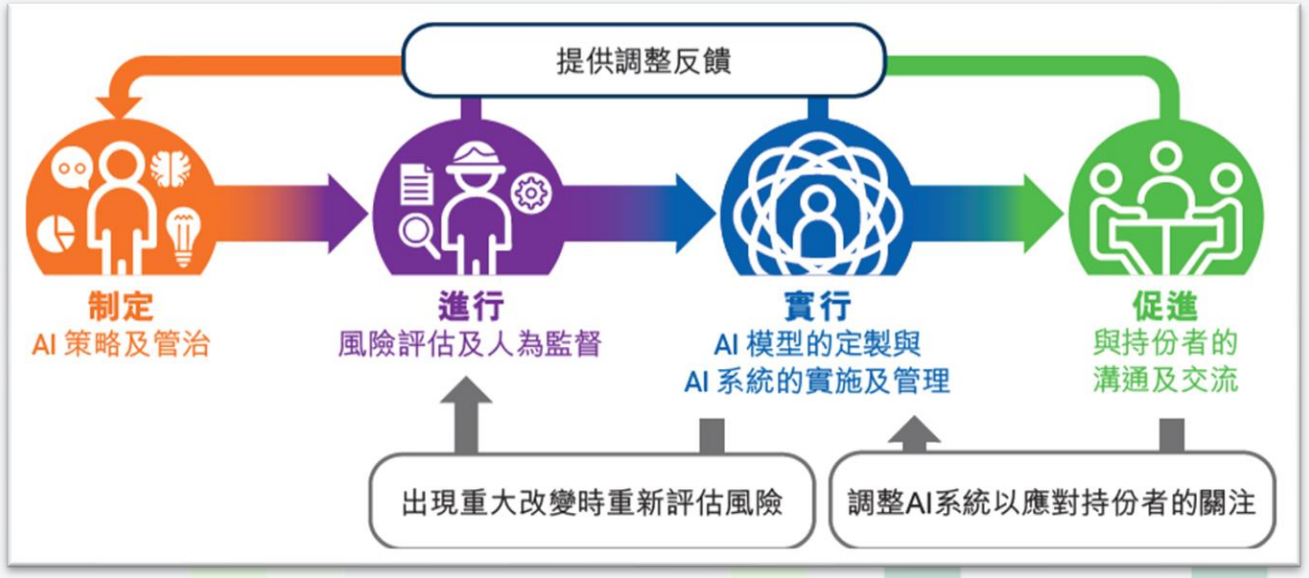
遵從其他相關內部政策

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**

《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



《人工智能 (AI): 個人資料保障模範框架》

制定
AI 策略及管治

- **AI 策略**
- **管治考慮**
- **管治架構**
- **培訓及加強認識**

進行
風險評估及人為監督

較低 — ***AI系統的風險程度*** — *較高*

人在環外
AI在沒有人為介入下作出決定

人為管控
人類決策者監督AI的運作，在有需要時介入

人在環中
人類決策者在決策過程中保留控制權以防止及/或減低AI出錯

《人工智能 (AI): 個人資料保障模範框架》

實行
AI 模型的定製與
AI 系統的實施及管理

數據準備

AI的定製及實施

管理與持續監察

促進
與持份者的
溝通及交流

- 提供資訊
- 可解釋的 AI
- 資料當事人的權利及反饋
- 語言及方式

守護私隱·改革創新
Protecting Privacy · Embracing Innovation

聯絡我們

電話: 2827 2827
傳真: 2877 7026
網站: 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

追蹤我們

私隱公署PCPD
香港个人资料私隐专员公署
Office of the Privacy Commissioner for Personal Data, Hong Kong