媒體和資訊素養系列:

(6) 當個人資料遇上人工智能—負責任資訊處理工作坊 (新辦)

鍾麗玲女士, 個人資料私隱專員
彭思華先生, 個人資料私隱專員公署經理（企業傳訊部）

2026年3月26日

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

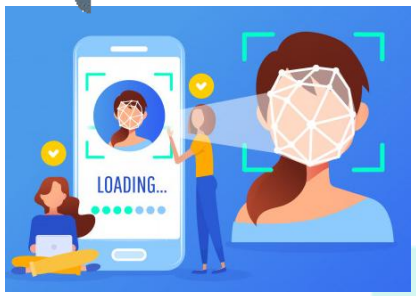
保障學生個人資料私隱及學校數據安全

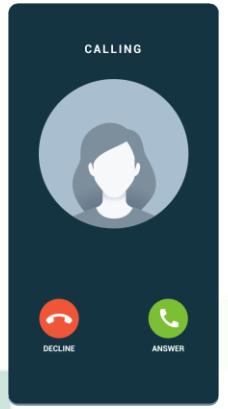
何謂「個人資料」？

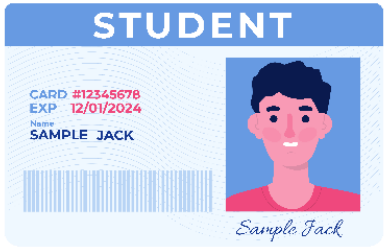
(a) 直接或間接與一名**在世人士**有關

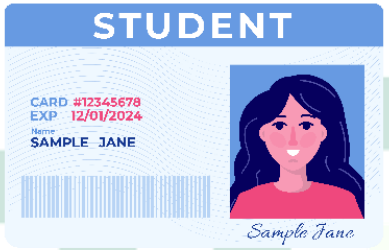
(b) 從該等資料直接或間接地**確定有關的個人的身分**是切實可行的

(c) 該等資料的存在形式令**查閱**及**處理**均是切實可行的









《私隱條例》的原則

- 任何人或機構在收集、持有、處理或使用個人資料的時候，必須遵從《私隱條例》內訂明的**六項保障資料原則**
- 該六項保障資料原則的規定涵蓋由**收集、保存、使用以至銷毀**個人資料的整個**生命周期**，資料使用者必須遵從

六項保障資料原則

https://www.youtube.com/watch?v=86wYYT8173Q

個案分享

個案背景

- 一所學校在其網頁中，上載有關「成績表現」的資訊，當中披露了學生的個人資料，包括個別**學生的照片、姓名及所獲取的成績**等詳情
- 該學校事前**未有獲得涉事學生的家長的同意**

《私隱條例》的規定

- 根據保障資料第3原則，除非得到有關資料當事人的**訂明同意**，否則個人資料只可使用（包括披露和轉移）於當初收集該資料時，擬將該資料用於的目的或直接相關的目的

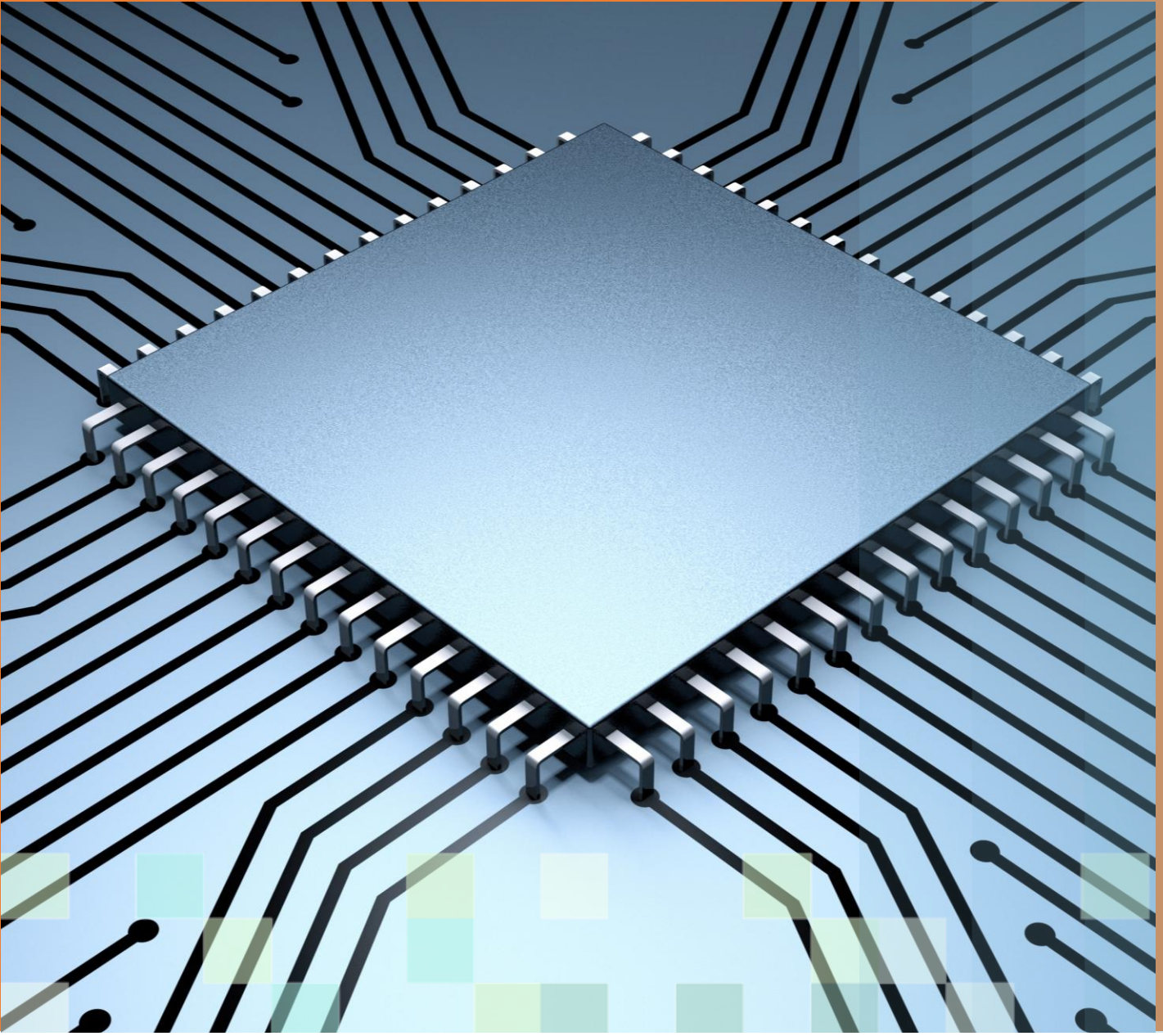
個案分享

結果

- 經公署介入後，該學校已修改網頁的相關內容，刪去當中可識別學生身分的資訊，**將有關資料匿名化**

借鑒

學校應在公開及披露學生的個人資料前，向家長**發出通告**，說明有關披露的目的及所涉及的資料等詳情，以**索取有關家長的訂明同意**



認識數據安全

《私隱條例》的相關規定

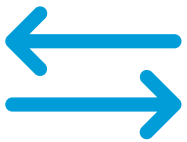
如涉及個人資料外洩，可構成違反保障資料第4原則

保障資料第4(1)原則

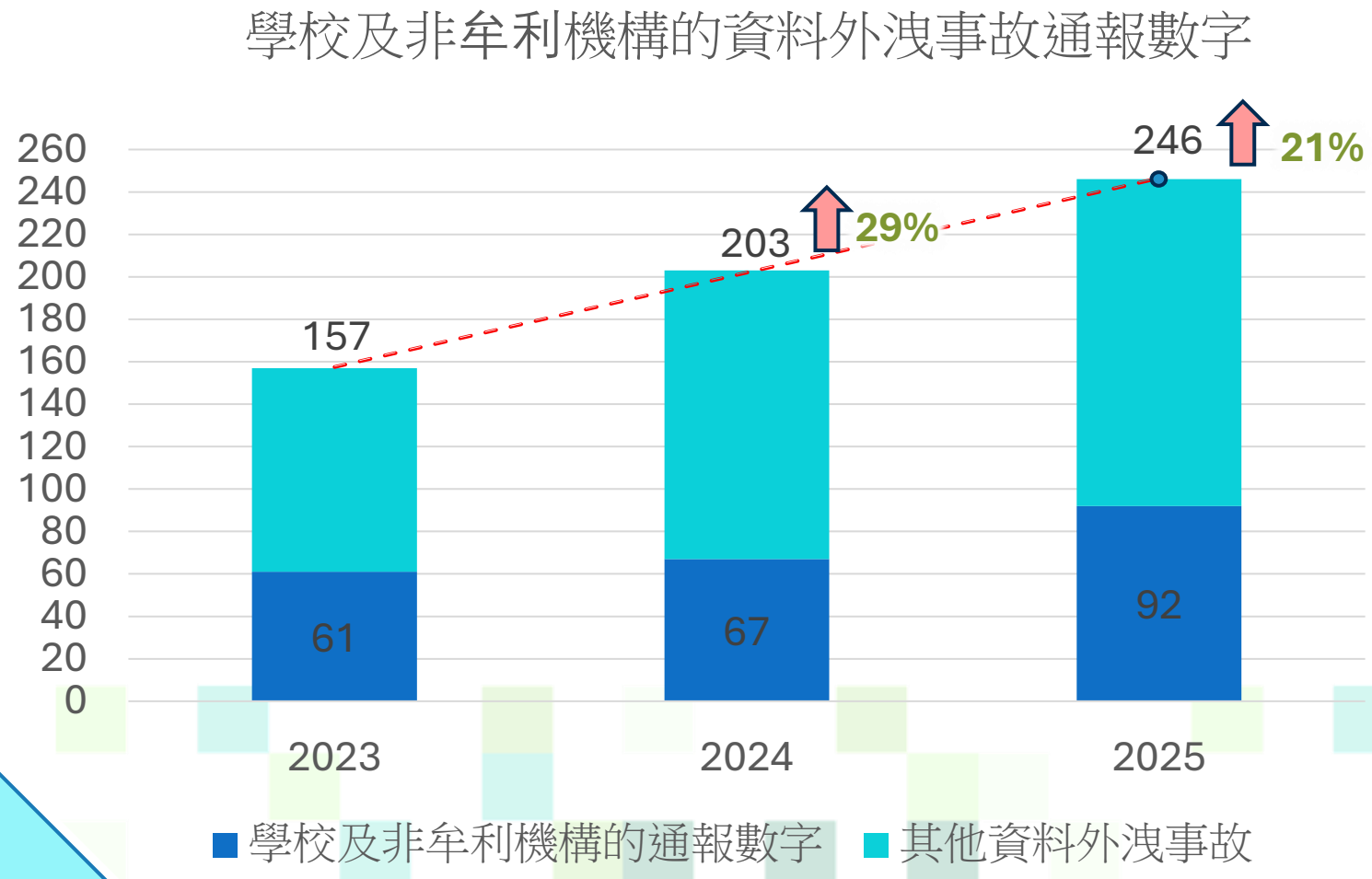
資料使用者須**採取所有切實可行的步驟**，確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響

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被查閱、處理、刪除、喪失或使用



資料外洩事故通報趨勢



- 私隱專員公署於2025年共接獲246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92宗（約37%），比2024年上升約37%，較2023年的61宗上升約50%

個案（1）一間教育機構因密碼管理欠佳而導致學生和家長的個人資料被未獲授權查閱

背景

一間教育機構的資訊管理系統遭黑客利用**暴力攻擊**獲取了管理員帳戶密碼，並建立了具有管理員權限的新帳戶，以查閱當中的個人資料。事故影響**超過24,000名家長及學生用戶的個人資料**。該機構調查後發現，是次事故源於**密碼管理欠佳**。

補救措施

1. **採用雙重認證功能**為帳戶提供額外的保護；
2. **設定高強度密碼**；
3. **定期清理不必要的帳戶**；及
4. **加強培訓**提高員工的資料保障意識。

個案（2） 即時通訊軟件帳戶遭騎劫

背景

私隱專員公署曾接獲23宗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。

事件涉及近**2,600名服務使用者、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**。

補救措施

1. **加強即時通訊軟件帳戶的保安措施**，例如啟用帳戶的雙重認證功能、定期檢查已連結的裝置及登出不再使用或不明的裝置連結；及
2. **制訂指引**向員工述明安全使用即時通訊軟件的注意事項，包括小心留意網頁連結，不要誤按虛假的即時通訊軟件網頁版，及切勿向他人透露任何密碼或驗證碼等。

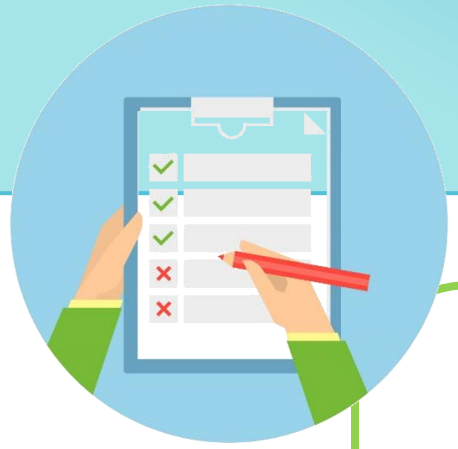
個案（3）一名中學教師沒有適當地設定內部檔案的存取權限

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

1. 停止了所有用戶建立或使用雲端的範本功能；及
2. 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。



借鑑

學校應：

- **制訂保障資料政策和程序**，並**加强保安措施**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。

《資訊及通訊科技的保安措施指引》

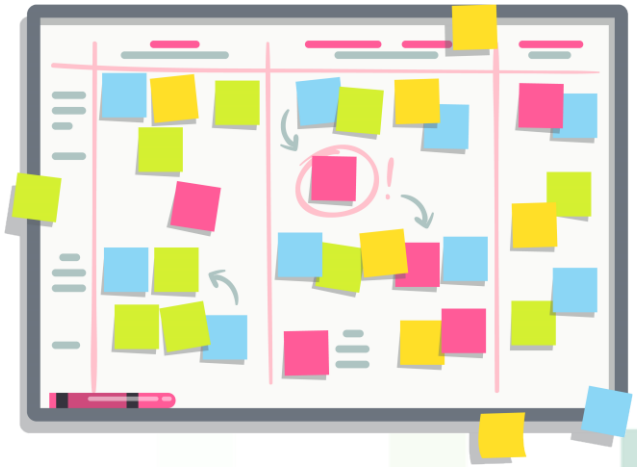
1. 資料管治和機構性措施
2. 風險評估
3. 技術上及操作上的保安措施
4. 資料處理者的管理
5. 資料保安事故發生後的補救措施
6. 監察、評估及改善
7. 其他考慮

下載指引

下載小冊子

資料外洩事故應變計劃

資料外洩事故應變計劃是載列機構一旦發生資料外洩時會**如何應對的文件**。一套全面的資料外洩事故應變計劃有助機構**快速應對及有效管理事故**。



資料外洩事故應變計劃應：

- 概述發生事故後**須執行的程序**
- 資料使用者由事故開始到完結就**識別、遏止、評估**以至**管理事故**所帶來的影響的策略

如何處理資料外洩事故

1. 立即收集重要資料
2. 遏止事件擴大
3. 評估事件可造成的損害
4. 考慮作出資料外洩通報
5. 記錄事故

PCPD.org.hk

指引資料

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

資料外洩事故的處理及通報指引

引言

良好的資料外洩事故處理作為營商之道

採取良好的資料外洩事故處理政策及措施不但能協助資料使用者減低外洩事故所帶來的損害，還能透過有關資料使用者處理外洩事故以及訂立清晰的後續行動方案，展現其願意承擔責任的精神。另一方面，作出資料外洩通報除了能協助受影響的資料當事人採取適當的應對保護措施，亦有助有關資料使用者減低訴訟風險和維持其商譽及生意關係，而在個別情況下，甚至能保持公眾對有關機構的信心。

本指引旨在協助資料使用者準備及處理資料外洩事故，以防止類似事件再次發生，從而減低對有關資料當事人所帶來的損失和損害，特別是當外洩事故涉及敏感個人資料。

甚麼是個人資料？

資料外洩事故通常涉及個人（例如機構的顧客、服務使用者、僱員及求職者）的個人資料。根據《個

甚麼是資料外洩事故？

資料外洩事故一般指資料使用者[2]持有的個人資料懷疑或已經遭到外洩，令有關資料當事人的個人資料有被未獲准許的或意外的查閱、處理、刪除、喪失或使用的風險。

一些資料外洩事故的例子包括：

- 遺失載有個人資料的可攜式裝置，例如手提電腦、USB儲存裝置、可攜式影碟或後備磁帶
- 不當處理個人資料，例如不當地棄置、把電郵發送予非指定的收件人或被未經授權的職員查閱資料系統
- 資料使用者載有個人資料的資料系統被非法侵入或被未經授權的第三方查閱
- 第三方以欺騙手法從資料使用者取得個人資料
- 在電腦安裝檔案分享軟件而導致資料外洩

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(1)及(2)原則**。**保障資料第4(1)原則**規定資料使用者須採取所有切實可行的步驟，確保由資料使用者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，尤其須考慮—

17

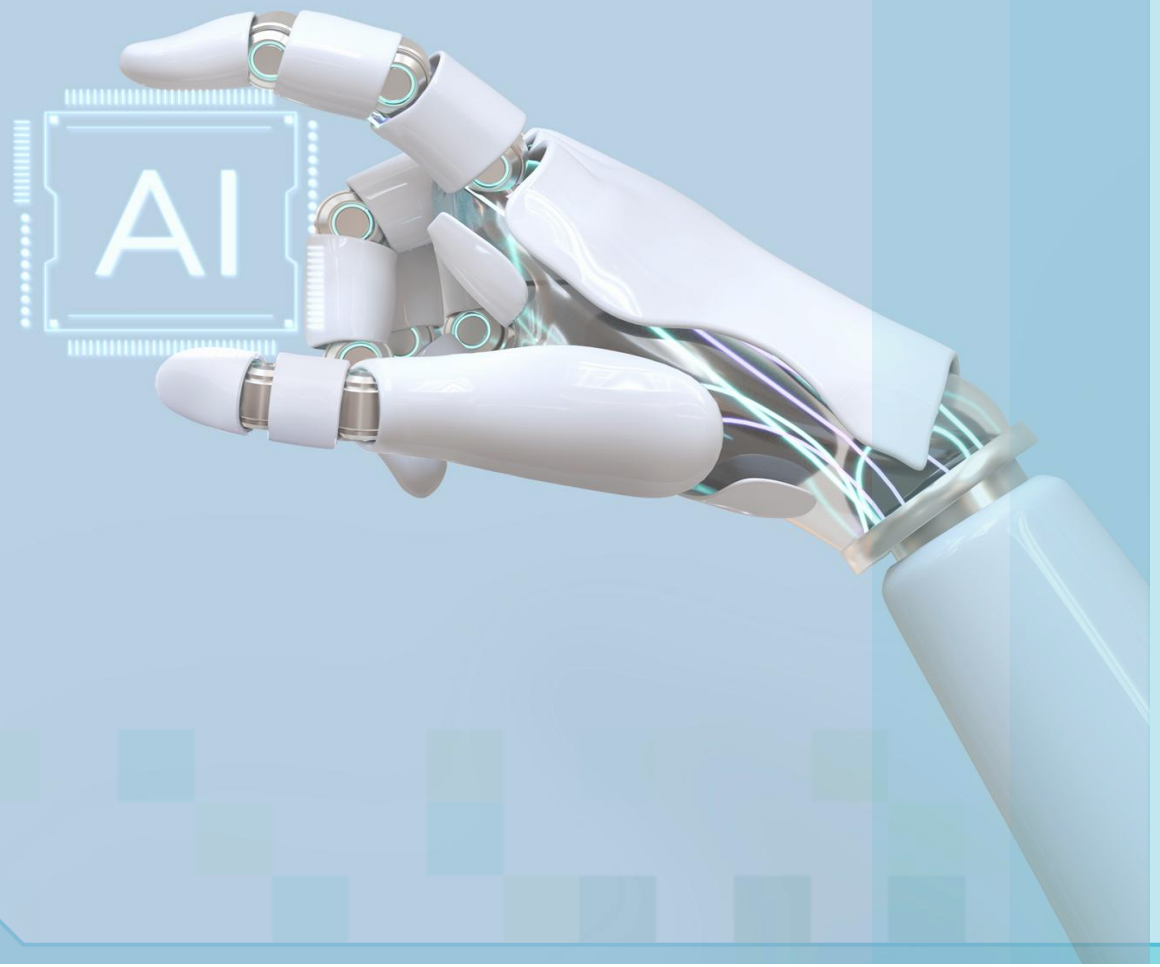
PCPD HK

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



認識AI安全
及私隱風險

趨勢

機構正積極採用 AI；AI教育市場規模將會擴張

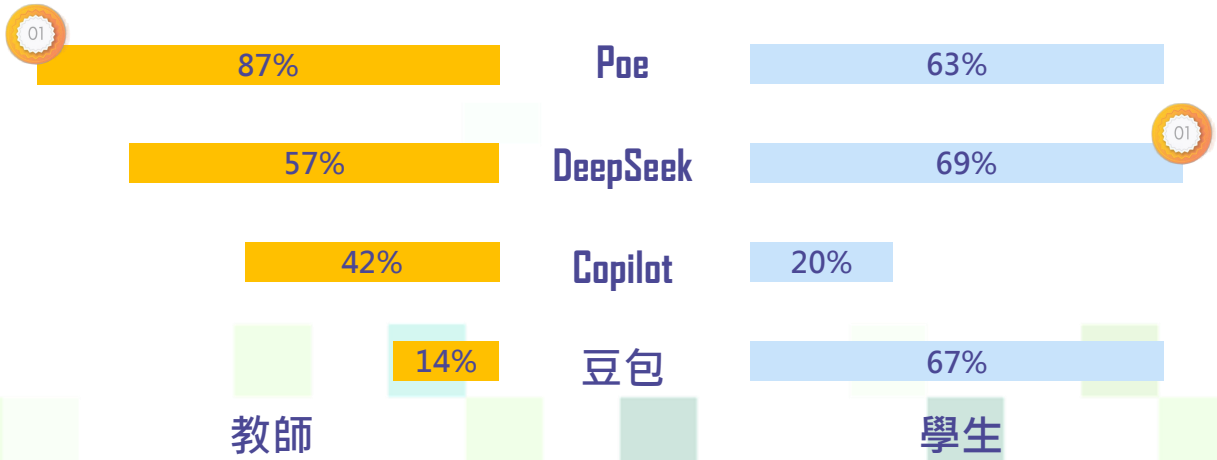
逾 90% 香港中小師生已用 AI 工具　無 AI 已不能學習工作　團體倡應用框架保障學生安全

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

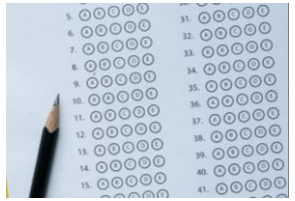
最常用的AI工具是Poe和DeepSeek 部分工具應用呈現世代差異



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(一)

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**

AI教學風波(二)

美大學教授用AI批改論文並生成反饋，引起學生不滿

事件發展

學生發現評語部分載有教授與AI的對話紀錄

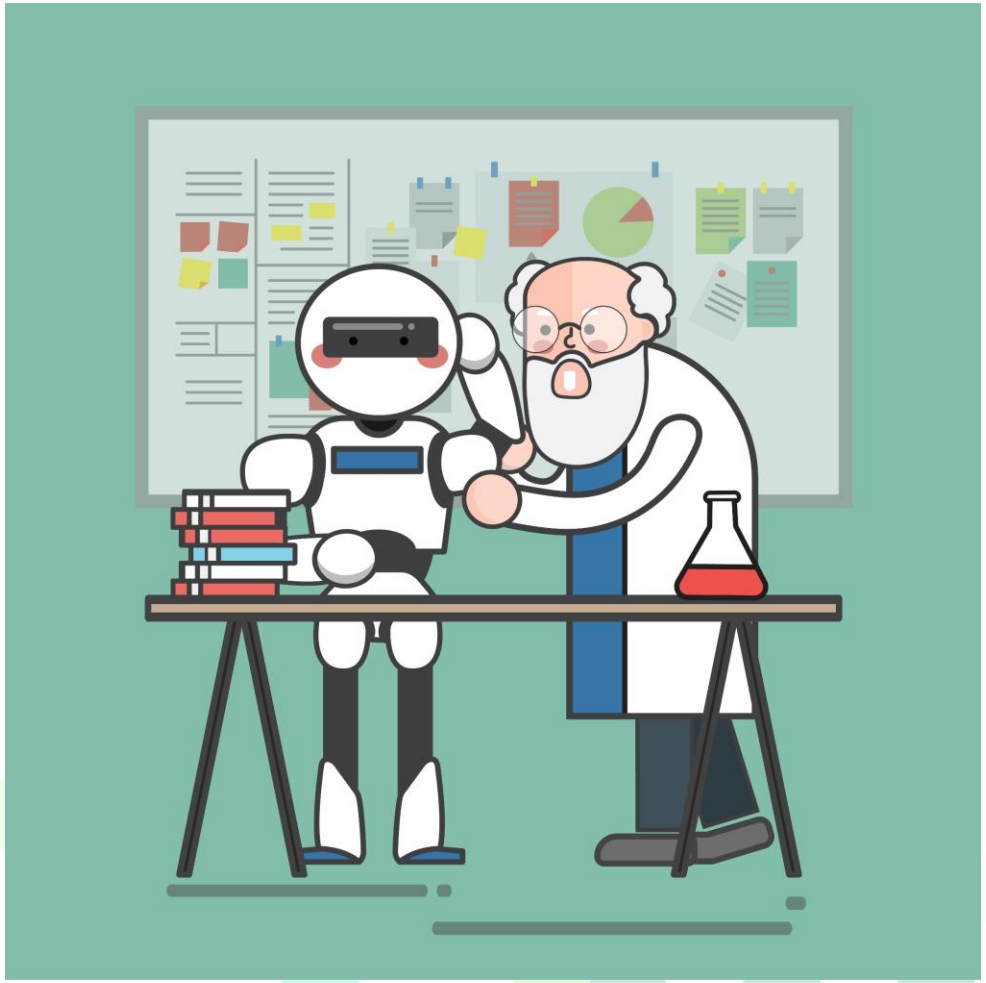
- 教授要求AI使用的評分標準
- 教授指示AI給學生一些「非常正面的評語」

質疑教授沒有親身批改論文

- 學生感到「受到了不公正待遇」

事件後續

- 教授澄清有閱讀學生的論文，並在學校允許的情況下使用AI作為參考
- 學生最終決定轉學



資料來源: 新浪網

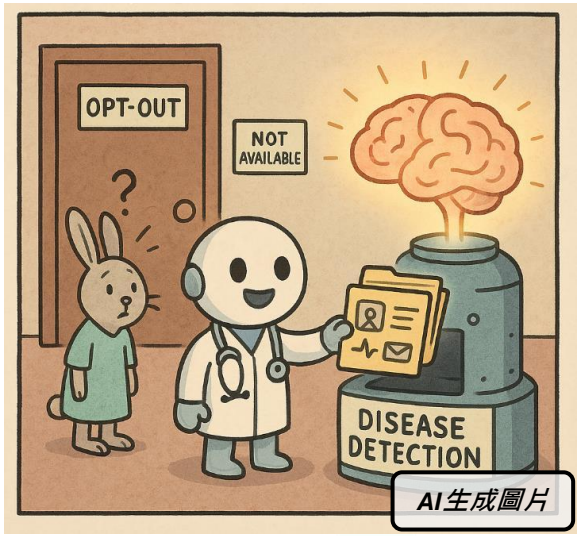
學校使用AI帶來的個人資料私隱風險

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

《AI 部署模式與資訊保安要求比較》

資訊保安考慮因素	本地 AI（校內部署） 使用開源模型	私有雲 AI 使用開源模型	公有雲 AI 使用開源與閉源模型
伺服器位置 / 資料主權	資料存放於校內	建議設於香港	建議設於香港
供應商政策 - 是否使用用戶資料作模型訓練	資料存放於校內	建議不使用用戶資料作訓練	建議不使用用戶資料作訓練
供應商資料保留政策及審計記錄	校內控制	建議零資料保留	建議零資料保留
個人資料去識別化 （Anonymisation）	建議	必須	必須
資料保障管理制度認證 （ISO 27001）	建議 (校內負責獲取)	必須	必須
AI事故應變計劃	高控制權 學校完全自主	中控制權 學校主導+雲支援	低控制權 依賴供應商合約
服務端安全護欄 (Guard Rail)	必須（如技術可行）	必須（如技術可行）	必須（如技術可行）
資料外洩防護措施 （DLP）	建議	建議	建議
設備實體保安	學校責任	供應商責任	供應商責任

資料來源:香港教育城

《AI 供應商資料保留與模型訓練政策一覽》

Provider	Data Retention
Amazon Bedrock	Zero retention
Azure	
NVIDIA	
Perplexity	

Provider	Data Retention
Alibaba Cloud Int.	Prompts are retained for unknown period
Cloudflare	
OpenAI	

Provider	Data Retention
Google AI Studio	Retained for 55 days
xAI	Retained for 30 days

資料來源: *https://openrouter.ai/docs/guides/privacy/logging*

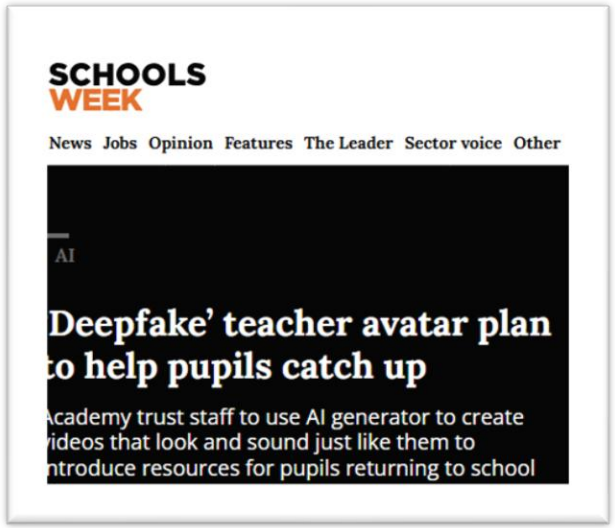
Provider	Train on Prompts
Chutes	May train
Cirrascale	
DeepSeek	
OpenInference	

- Microsoft will not use your prompts or completions to train or improve models
- Zero retention available for enterprise customers upon request

資料來源: *https://www.microsoft.com/en-us/legal/terms-of-use?oneroute=true*

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**

有圖未必有真相

製作深度偽造影片並不困難

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

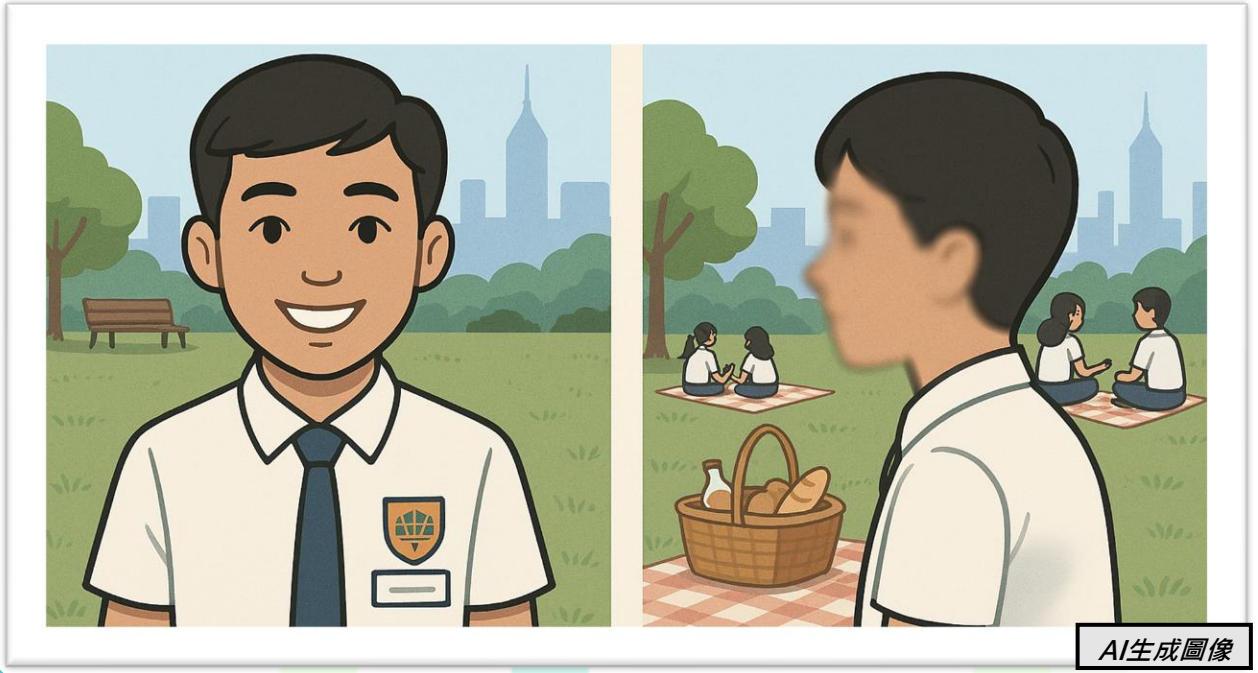
- 設立**清晰程序**應對深偽事故，並**組織危機處理小組**處理相關工作

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

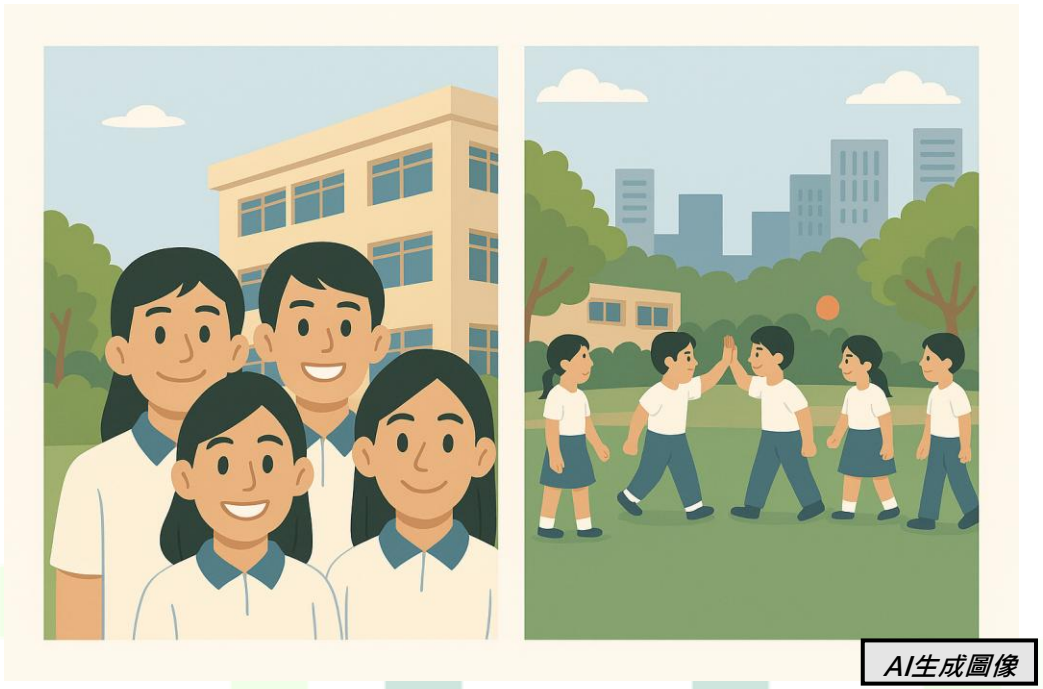
相片例子

例子1



AI生成圖像

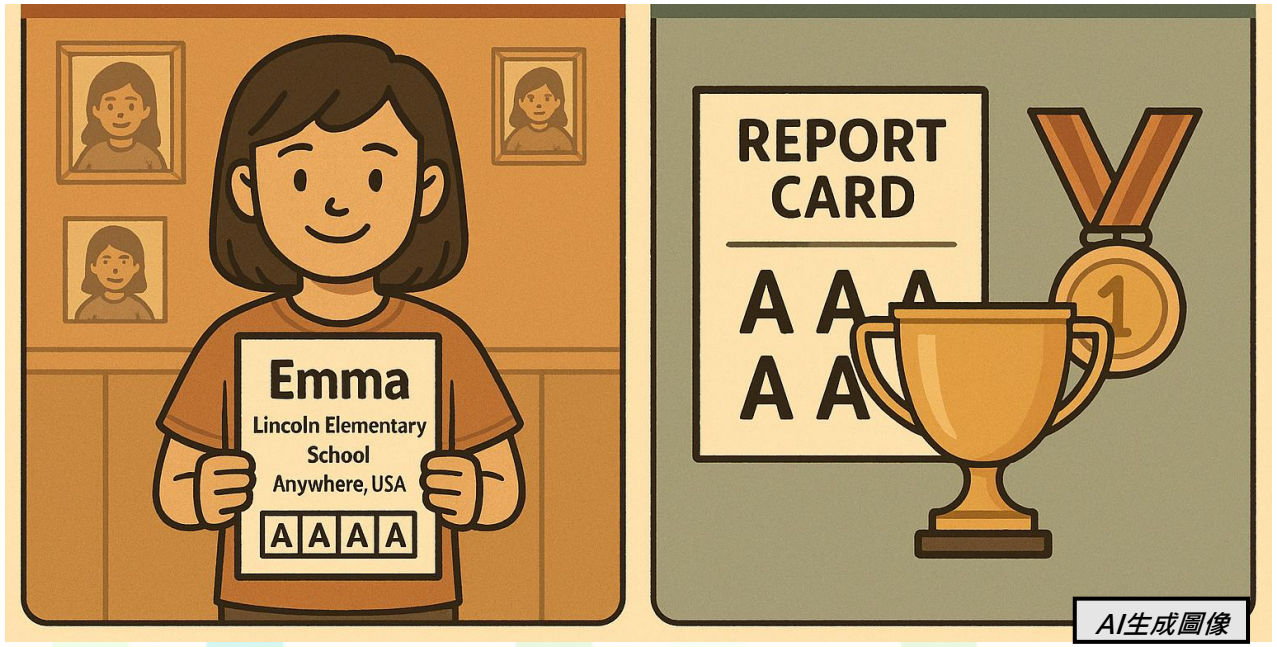
例子2



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

下載指引

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

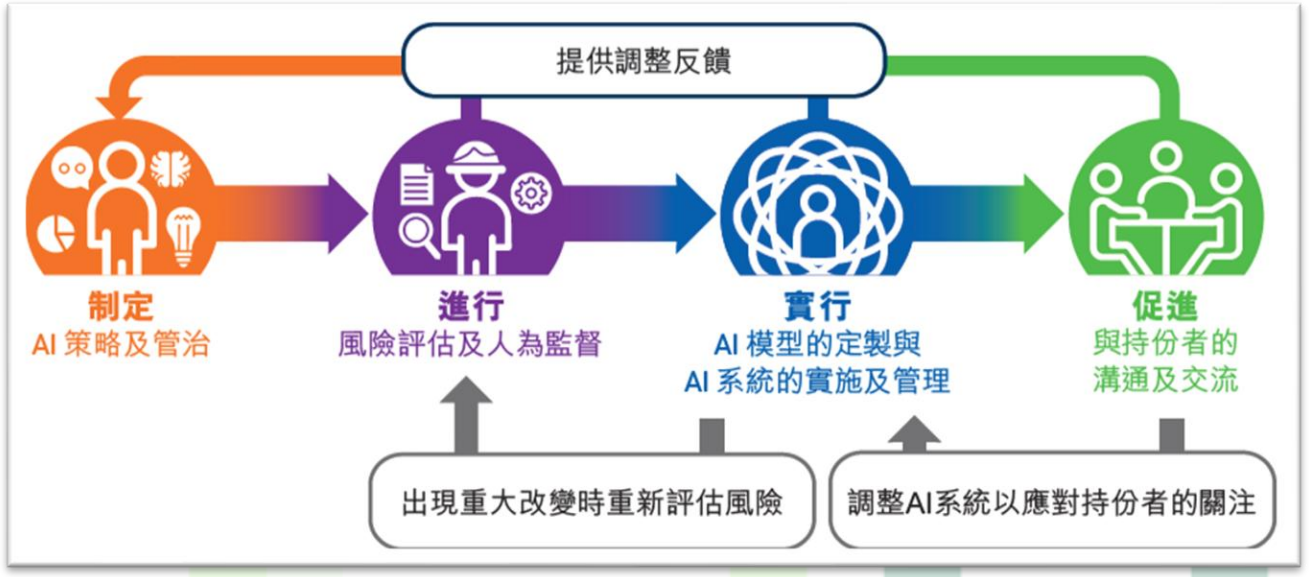
遵從其他相關內部政策

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

較低 — ***AI系統的風險程度*** — *較高*

進行
風險評估及人為監督

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

《個人資料匿名化入門指南》

- 介紹匿名化的基本概念，並概述機構進行匿名化處理資料的建議步驟
- 透過個案分析，闡釋機構如何在實際運作中應用這些匿名化步驟

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

PCPD HK
PCPD.org.hk
個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data
中國香港 Hong Kong, China

謝謝！

答問環節