應對濫用人工智能深度偽造技術

給學校及家長的智慧錦囊

PCPD
HK

PCPD.org.hk

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

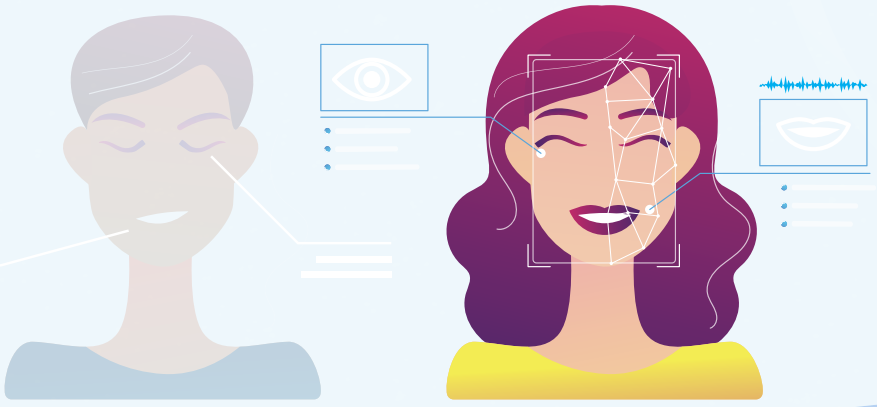
A. 引言

深度偽造(深偽)是「深度學習」和「偽造」組成的合併詞，一般而言，泛指利用深度學習(即人工智能(AI)的一種技術)製作出有關個別人士及/或物件的影像、音頻及影片內容，而該內容看似逼真但卻是偽造的。深偽技術可以利用影像、影片及錄音內的個人資料，模仿並替換某人的面貌、聲音或動作，令人信以為真。如果深偽技術被惡意使用，可能會對個人造成傷害。除卻其他相關法例的規定，任何在製作深偽內容的過程中涉及使用個人資料，均受《個人資料(私隱)條例》(《私隱條例》)所規管。

兒童及青少年未必能充分理解自己的私隱權或披露其個人資料所帶來的風險，因而特別容易受深偽技術所影響。有些學生甚至會在不了解使用深偽技術可能會帶來後果的情況下，製作或分享惡意深偽內容。本單張旨在為學校[1]及家長提供實用建議，協助他們處理涉及兒童及青少年的深偽技術相關事故，並保障兒童及青少年的個人資料私隱。

B. 常見的深偽技術種類

- ***換臉：***在相片或影片中，將某人的臉更換為另一張人臉。
- ***面部再現(傀儡)：***在即時或預錄影片中，將某人的面部動作(例如：表情、嘴唇動作)複製至另一人之上。
- ***人臉生成：***生成逼真但並非真實存在的人臉影像。
- ***同步口形：***將某人嘴唇動作的影片與某段音訊(通常是經語音模仿或修改)進行匹配，使其看起來說出實際並未發表之言論。
- ***語音模仿：***製作與某人的聲音極為相似(包括口音及語調)的說話。



[1] 本指引所指的「學校」泛指小學、中學，以及專上院校(例如大學)。

C. 在校內使用深偽技術

負責任地使用深偽技術可以支援學校教學，令學習更具沉浸感和趣味性，例如：透過虛擬角色的影片講解課堂內容或重現歷史事件場景。然而，如果深偽技術被濫用，則可能對他人，尤其是兒童及青少年造成傷害。

校內常見濫用深偽技術的類型

- ***影像性暴力：*** 犯事者可能在未經同學同意下，偽造同學的露骨影像或影片，有時會牽涉性勒索，令同學的聲譽受損，並引致嚴重的精神傷害或心理傷害。
- ***網絡欺凌及騷擾：*** 深偽內容可用作羞辱或中傷同學，例如憑空捏造令人尷尬的情況，令同學受情緒困擾。
- ***詐騙：*** 罪犯或會利用語音或影片模仿家長、學生或教師以詐取敏感的個人資料或進行詐騙。
- ***假新聞及虛假信息：*** 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。

警告： 製作及/或披露惡意深偽材料可能招致法律責任。

D. 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

以下實用建議可協助學校及家長減低兒童及青少年的影像、影片或聲音被濫用或用作製作惡意深偽內容的風險。

學校

- **減少原材料**
  - 在可行情況下，避免發布可以清晰識別個別學生的相片或影片，並優先採用不聚焦在面貌的團體照。
  - 避免上載特寫肖像及高清相片或影片至公開的網頁或網上平台。

- **限制查閱**
  - 學生的相片及影片應只在學校管理的系統(例如：內聯網、家長平台)內分享，並設有「角色為本」的存取控制權限。
  - 定期審視學校網站及社交媒體，並移除不再需要的內容。
- **確保數據安全**
  - 將學生的個人資料儲存在設有查閱限制及審計日誌、安全穩妥的平台。
  - 對可以查閱儲存學生個人資料的平台的帳戶採用多重身份認證。
- **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。
- **加強意識**
  - 定期為教職員提供網絡風險培訓，包括深偽技術風險、辨認深偽的技術(例如驗證視像通話真實性的方法以及偵測工具的局限)及法律考慮因素。
  - 為學生提供工作坊，講解深偽技術所涉及的私隱風險、惡意深偽的法律後果，以及可能對個人造成的傷害。

家長

- **限制分享**
  - 在網上發布子女的相片或影片前「停一停，諗一諗」，避免公開任何已分享的影像。
  - 審視自己及子女的社交媒體私隱設定，將帳戶設定為私人，並只允許已核准的朋友追蹤。
- **確保數據安全**
  - 在所有儲存家庭相片及影片的社交媒體及雲端帳戶使用高強度和獨特的密碼，並使用多重身份認證。
  - 及時更新智能電話及其系統和應用程式，避免授權應用程式存取整個相片庫。
- **與子女溝通**
  - 營造一個安全及不批判的空間討論深偽技術及性勒索等網絡風險。
  - 鼓勵子女在相信或分享影片或語音片段（尤其是來歷不明的影片或語音片段）前「停一停、諗一諗」，當在網上遇到陌生人接觸時向你求助。
  - 向子女解釋製作及/或分享惡意深偽內容可能帶來的傷害及法律後果。
  - 教育子女製作深偽內容時負責任地使用他人的個人資料，並解釋濫用個人資料的後果（見E部分）。
- **掌握最新消息**
  - 留意來自政府、私隱專員公署、警務處、學校及其他具信譽的機構有關深偽技術的指引、更新及資訊。

學校應該如何處理深偽事故？

濫用或惡意使用深偽技術所引致的事故中，可能涉及同學作為受害人、犯事者或兩者皆是。在此情況下，學校應根據現有的學校政策或程序，例如危機處理或反欺凌指引(如適用)作出應對。以下為建議步驟：

- 優先考慮受影響同學的福祉，必要時尋求專業(例如：社工、輔導員)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。
- 向學校管理層及/或負責處理相關問題的指定團隊報告事故。
- 指示學生停止分享深偽材料，並盡快將材料刪除。
- 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(如適用)。
- 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(見E部分)。
- 如懷疑涉及罪案，應向警方查詢或報案。如涉及濫用個人資料或「起底」的情況，可聯絡私隱專員公署尋求協助或作出投訴。

家長應該如何處理深偽事故？

當子女捲入濫用或惡意深偽事故，不論子女是受害人、犯事者或接收者，作為家長難免感到不知所措及困擾。建議家長及監護人以關懷及支持的態度作出回應。

- **如果子女是濫用或惡意深偽的受害人：**
  - 理解到事故可能會對子女造成創傷，並向他們提供情緒支援及安慰。
  - 營造安全空間讓子女談及他/她的感受。如有需要，尋求社工等專業人士的支援。
  - 將子女的帳戶設定為私人，並鼓勵他們暫停使用社交媒體，確保數碼環境安全。
  - 妥善保管相關證據以便作出跟進行動，並協助子女向有關當局(包括學校及執法機關)查詢或舉報。
  - 協助子女向網上平台舉報並要求移除深偽材料。如有需要，可向私隱專員公署尋求協助，以移除有關材料。
  - 留意任何威脅或勒索的跡象。如有需要，聯絡執法機關。
- **如果子女製作、接收及/或分享深偽材料：**
  - 引導子女停止製作及/或分享這些濫用或惡意材料，並立即刪除該些內容。
  - 在可行情況下，要求有關網上平台移除相關內容。
  - 向子女解釋製作及/或分享惡意深偽內容可能帶來的傷害及法律後果。
  - 教育子女製作深偽內容時負責任地使用他人的個人資料，並解釋濫用個人資料的後果(見E部分)。

E. 潛在法律後果

大部分現實世界的法律同樣適用於數碼世界。在現行法律下，製作及/或披露惡意深偽材料可能導致法律後果。

根據《私隱條例》，如果在製作及/或披露深偽材料時使用個人資料[2]，而該使用目的超出了收集資料時的原有目的(或直接與該目的有關的目的)，便可能違反保障資料第3原則中的使用限制，除非有關個人已給予明示及自願同意。如果以不合法或不公平的方式收集個人資料，亦可能違反保障資料第1原則有關收集資料的規定。

在較嚴重的個案中，製作及/或披露惡意深偽材料可能構成刑事罪行。尤其是，在未經當事人同意的情況下披露包含個人資料的深偽材料，而披露者的意圖是導致或罔顧是否會(或相當可能會)導致當事人或其家人蒙受任何指明傷害[3](包括身體傷害或心理傷害)，便可能構成《私隱條例》下的「起底」罪行。

惡意使用深偽技術亦可能干犯其他刑事罪行，例如：

刑事罪行	*相關法例*
未經當事人同意下發布或威脅發布以深偽技術製作、經修改的私密影像	《刑事罪行條例》[4]
利用深偽技術製作兒童色情物品	《防止兒童色情物品條例》[5]
利用深偽技術進行欺詐活動	《盜竊罪條例》[6]

[2] 根據《私隱條例》第2(1)條，「個人資料」指符合以下說明的任何資料：(a)直接或間接與一名在世的個人有關的；(b)從該資料直接或間接地確定有關的個人的身分是切實可行的；及(c)該資料的存在形式令予以查閱及處理均是切實可行的。「切實可行」指合理地切實可行。

[3] 根據《私隱條例》第64(6)條，指明傷害就某人而言，指(a)對該人的滋擾、騷擾、纏擾、威脅或恐嚇；(b)對該人的身體傷害或心理傷害；(c)導致該人合理地擔心其安全或福祉的傷害；或(d)該人的財產受損。

[4] 見《刑事罪行條例》第159AA條及第159AAE條。

[5] 見《防止兒童色情物品條例》第3條。

[6] 舉例而言，《盜竊罪條例》第16A條下的「欺詐罪」及第17條下的「以欺騙手段取得財產」。

PCPD.org.hk

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

政府資助機構
Government-funded organisation

電話：2827 2827
傳真：2877 7026
地址：香港灣仔皇后大道東248號大新金融中心13樓1303室
電郵：communications@pcpd.org.hk

私隱專員公署網頁
pcpd.org.hk

下載本刊物

免責聲明

本刊物所載的資訊和建議只作一般參考用途，並非為法例的應用提供詳盡指引，亦不構成法律或其他專業意見。私隱專員並沒有就本刊物內所載的資訊和建議的準確性或個別目的或使用的適用性作出明示或隱含保證。相關資訊和建議不會影響私隱專員在《個人資料（私隱）條例》下獲賦予的職能及權力。

二零二五年十二月