中小學使用「生成式人工智慧」注意事項2.0

（學生版）

中華民國113年7月1日 臺教資（三）字第1132702614號函 核定
中華民國114年12月23日 臺教資（一）字第1142704025號函 核定

近年來，「生成式人工智慧」（Generative AI，簡稱GenAI）工具迅速發展，為社會帶來許多新的機會和改變；同時，「深偽技術」（Deepfake）也逐漸成熟，這些技術改變了我們原本獲取知識、傳播訊息和創造內容的方式，但也增加了許多使用上的風險。為了幫助學生提升「生成式人工智慧」工具使用素養，理解使用的倫理原則，善用相關技術並避免造成誤用或濫用，同時能在家長或學校老師的指導與同意下遵守各工具年齡分級與帳號申請規範，提供以下注意事項作為使用參考。

一、可能會產生偏誤的內容

「生成式人工智慧」工具的資料來源是歷史紀錄或舊經驗，如果這些資料本身具有成見或錯誤，那麼使用「生成式人工智慧」工具的結果也會存在偏差或錯誤，因為這些工具無法自行判斷結果的正確性和合理性。

所以我們在使用「生成式人工智慧」工具時，應該仔細檢視內容，並以批判性思考判斷其是否公平、全面或具有偏見，遇有疑慮應向老師或家長詢問，不宜直接採信或用於作業、報告或公開發表的內容。

二、可能會減少訊息的多樣性

「生成式人工智慧」工具的資料會受到其來源的影響。如果資料不夠多元、廣泛，那這些工具產生的結果可能只會呈現單一文化的知識，造成知識量嚴重性不足，不僅正確性堪慮，甚至會讓人產生偏見。

所以我們在使用「生成式人工智慧」工具時，需要結合自己的經驗和批判性思維來檢視結果，而不是全盤接受生成的內容，並留意其中是否涉及文化刻板印象或不公平的描述，如對內容有疑慮，應向老師或家長請教，不可以直接將生成內容作為作業或報告的原始答案。

三、發現深偽技術會產生不實的內容

Deepfake是能修改臉部影像的「深度偽造技術」，原理是使用「生成式人工智慧」創建虛假的內容。這項技術能利用既有的圖片、影像或聲音素材，製造出看似真實的影片和圖像，甚至假新聞。

所以當我們在觀看網路內容時，不要輕易相信未經審核的影片或照片，並留意這些內容是否由深偽技術合成，和判斷可能的目的與動機，也要尊重他人的肖像權與隱私，不轉傳、下載或散布可能由深偽技術合成的影片或圖片。

此外，如果不幸發現自己或他人遭到深偽技術（如AI換臉）製作不當的性影像，請不要害怕，這不是你的錯。請記得先截圖保留證據，並向「衛生福利部性影像處理中心」線上申訴（https://siarc.mohw.gov.tw），由專業單位協助移除下架，切勿轉傳造成二度傷害。

四、可能造成個資、隱私和機密的洩漏

部分「生成式人工智慧」工具的資料在取得、儲存和使用上都還沒有完備的法令、規範及倫理上的監管機制。因此，在使用這些工具時，提供的個人資料、敏感訊息及機密數據，都可能會被收錄到訓練資料庫中，作為未來回應他人的內容。

所以我們在使用「生成式人工智慧」工具時，應該審慎評估提供的資訊，是否具有機密性、隱私性與敏感性，以保護個人與組織的隱私與機密。

五、遵守「生成式人工智慧」服務使用規範

中小學學生使用「生成式人工智慧」工具應遵守各平臺註冊年齡限制及相關規範。

國小學生建議使用為教育目的而設計的生成式人工智慧的服務或產品，如教育部因材網生成式AI學習夥伴e度或教育部酷英網E-BOT等生成式的教育工具，在校應於教師引導或指導下使用，若為非在校使用，亦請家長陪伴使用。

國高中學生亦建議使用為教育目的而設計的生成式人工智慧的服務或產品，在校應於教師引導或指導下使用；如需使用非為教育目的而設計的生成式人工智慧的服務或產品，除需符合前述註冊年齡限制及相關規範外，在校應於教師引導或指導下使用，若非在校使用，則需得到父母或監護人同意和監督。

六、遵守倫理與誠信使用原則

（一）生成式人工智慧是協助學習的工具，不能取代自己的思考與判斷，應先自行閱讀與思考，再視需要使用工具輔助。

（二）使用「生成式人工智慧」工具時，應尊重他人的權利與尊嚴，不得輸入或產生含有歧視、霸凌、仇恨或不尊重他人之內容。

（三）不可以將自己或他人的姓名、照片、聯絡方式、住址、學號等個人資料，或家庭、學校的機密資訊輸入至「生成式人工智慧」工具。

（四）完成作業或報告時，如依老師或學校規定使用「生成式人工智慧」工具協助構思或潤飾，應依規定註明所使用的工具及用途，不得將生成內容直接當作自己原創作品繳交。

（五）遵守學校訂定之資訊倫理與學術誠信規範，不得使用「生成式人工智慧」工具從事抄襲、代寫、作弊或其他違反校規與法令之行為。

所以我們在使用「生成式人工智慧」工具時，應該審慎評估提供的資訊，是否具有機密性、隱私性與敏感性，以保護個人與組織的隱私與機密。

生成式人工智慧技術的發展，為我們的生活帶來了許多便利，並廣泛運用在各種情境中，卻也伴隨著一定的風險和挑戰。在這個數位時代，我們應該：

1. 保持對資訊來源保持的高度警覺。
2. 不要輕易相信未經證實的訊息。
3. 學會如何辨別虛假資訊。

同時，我們要提升自己思辨的能力：

1. 批判性地分析和評估生成式人工智慧工具所產生的內容，避免被誤導，並留意其中是否包含偏見或文化刻板印象。
2. 遵守相關的道德和法律規範（例如：尊重智慧財產權），確保使用「生成式人工智慧」工具時不違反社會常規與資訊倫理，並遵守學術誠信，不將生成內容直接作為個人原創作業。

最後，我們應該加強自己的數位素養能力，才能在享受科技進步帶來高度便利的同時，減少科技帶來的風險，讓負面影響降到最小，並以負責任的態度善用「生成式人工智慧」工具。

附錄

中小學使用「生成式人工智慧」注意事項2.0（學生版）示例

一、**可能會產生偏誤的內容：**當我們要求「生成式人工智慧」建議旅遊行程時，如果這些工具沒有當地的氣候環境、地理位置、社會人文及文化限制等資料，答案可能會來自於各種網路遊記文章的綜合體，也可能提供你一份不順路、非當季的活動行程，甚至還可能是虛構景點的行程。因此，當AI給出的資訊看起來奇怪、不合常理或與課本不同時，我們要停下來檢查內容，不要直接用在作業或報告上，並主動向老師或家長確認資訊是否正確。

二、**可能會減少訊息的多樣性：**當我們向「生成式人工智慧」詢問法律或文化問題時，這些工具可能會只根據研發者自己國家的法律和文化習俗產生答案。比如當你要求「生成式人工智慧」生成一張新娘圖片時，它可能只會產生一張穿著白紗禮服的西方臉孔女性，而不是根據使用者當地的文化習俗來產生不同膚色或其他婚禮的服飾。因此，當AI的答案只呈現某一種文化、觀點或價值時，我們要記得它可能忽略其他觀點，需要自己多方查證，避免被單一視角誤導。

三、**發現深偽技術會產生不實的內容：**網路上常有知名人士發表演說或鼓勵投資的影片，面對這些內容，我們必須謹慎且小心求證知識的內容和來源。在深偽技術蓬勃發展的網路環境中，這些影片可能未取得影片主角的同意，或在他們根本不知情的狀況下，被深偽技術整合他們的臉（聲音）到假圖片或假影片中。因此，看到不尋常或煽動性的影片時，不要急著相信或轉傳，應先詢問老師或家長，也不要把未查證的影片當成作業或報告內容。

四、**可能造成個資、隱私和機密的洩漏：**當我們不清楚「生成式人工智慧」的原理及規範的情況下，以個人或學業資料為題材向它詢問答案，可能導致個人的機密被收錄到它的資料庫中。而當其他的使用者再度詢問類似問題時，「生成式人工智慧」以收錄的資料庫回答問題，就有機會造成個人隱私或學業資料外洩，形成資安漏洞。因此，我們不把自己的姓名、住址、電話、照片、學校資料或家庭狀況輸入給「生成

式人工智慧」工具，避免讓敏感資訊被記錄或外洩。

五、**遵守「生成式人工智慧」服務使用規範：**有些同學可能看到廣告或影片介紹生成式人工智慧工具，就想自己註冊帳號來寫作業；但這些平臺會要求輸入Email、電話或住址等個人資料，對年紀較小的學生來說風險很高。因此，如因課業需要使用，使用為教育目的而設計的生成式人工智慧的服務或產品，如教育部因材網生成式AI學習夥伴e度或教育部酷英網E-BOT等生成式的教育工具，在校於教師引導或指導下使用，並遵守各平臺註冊年齡限制及相關規範。

國高中學生亦建議使用為教育目的而設計的生成式人工智慧的服務或產品，在校於教師引導或指導下使用；如需使用非為教育目的而設計的生成式人工智慧的服務或產品，除需符合前述註冊年齡限制及相關規範外，在學校使用時，能在教師引導或指導下使用，若非在校使用，則需得到父母或監護人同意和監督。

六、**遵守倫理與誠信使用原則：**有些同學可能會把整篇生成式人工智慧工具生成的內容直接交出去當作自己的報告，或請生成式人工智慧工具寫出一整篇作文，這樣不但不代表自己的學習成果，也可能侵犯智慧財產權或違反學校的學術誠信規範。因此，我們使用生成式人工智慧工具時應該先自己思考，再把生成式人工智慧工具當作輔助工具；若老師規定可以使用生成式人工智慧工具，就要按照要求註明使用方式，不可以把生成出來的內容當自己的原創作品，更不能用來作弊、抄襲或代寫作業。