中小學使用「生成式人工智慧」注意事項2.1

（教師、行政人員及家長版）

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
中華民國115年2月11日臺教資（一）字第1152700391號函核定

為了幫助中小學教師、行政人員及家長提升「生成式人工智慧」（Generative AI，簡稱GenAI）工具使用素養，理解使用的倫理原則，並能在教育情境中落實安全、合規與負責任的使用方式，以善用相關技術並避免造成誤用或濫用，提供以下注意事項作為使用參考。

一、理解「生成式人工智慧」工具產生的內容可能有所偏誤

由於用來訓練「生成式人工智慧」工具的資料來自於既有的紀錄或經驗，如果這些訓練資料本身帶有成見及錯誤，那麼使用「生成式人工智慧」工具產出的結果就會有偏差或錯誤，且工具本身無法自行判斷所產出的結果是否正確和合理。

所以當我們在使用「生成式人工智慧」工具時，應該檢視與審查其產生的結果，以確保其正確性和合乎常理，並注意可能涉及偏見、歧視或不公平內容，並適時在教學現場予以補充說明，避免學生誤信或誤用。

二、理解「生成式人工智慧」工具可能會減少訊息的多樣性

如果用來訓練「生成式人工智慧」工具的資料受到地域或文化的限制，且不夠多元、廣泛，這些工具產生的結果可能僅能呈現單一文化的知識脈絡與觀點，甚至進一步強化原有的偏見。

所以當我們在使用「生成式人工智慧」工具時，對於生成的內容應持保留與批判的態度，進一步查證內容的可信度，並留意是否呈現文化刻板印象、或者觀點過於主觀狹隘。教師應適時在教學現場協助學生辨識不同觀點，避免將未經查證的生成內容直接用於教材、公告或教學文件。

三、理解「生成式人工智慧」內容的辨識工具僅能作為初步篩檢

隨著「生成式人工智慧」工具的快速發展，有許多可以協助辨識生產內容的工具，我們需要了解這些辨識工具有其限制

性，只能作為輔助與參考，仍須結合其他具可靠來源的知識或證據來協助辨識內容是否來自於生成式人工智慧工具，不將辨識結果視為絕對正確或唯一依據。

學校在處理學術不端或學生作業爭議時，應結合教師專業判斷、實際作品內容與學生學習歷程進行綜合研判，並向學生與家長清楚說明相關依據與程序，以維護教育專業與學生權益。

四、察覺「深偽技術」日益逼真會產生不實的內容

深偽（Deepfake）技術是能修改臉部影像的深度仿造技術，原理是使用「生成式人工智慧」工具創建的虛假內容。這項技術能運用既有圖片、影像或聲音等素材，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，並留意該內容是否為深偽技術合成，和判斷可能的目的與動機，特別是在教育現場或校內社群媒體中，不得轉傳、散布或引用未經查證的深偽影像或影片。教師與行政人員亦應提醒學生尊重他人肖像權與隱私，避免誤用或擅自編輯影像，並在遇到疑似深偽內容時，協助學生釐清來源與真偽。

此外，若發現學生接觸或遭受深偽技術（如AI換臉）製作之不當性影像，或涉及色情、暴力等違反兒少保護內容，教師與家長應優先協助學生截圖保留證據，切勿轉傳以免造成二度傷害。針對性影像事件，請向「衛生福利部性影像處理中心」（https://siarc.mohw.gov.tw）申訴以協助下架；針對其他網路不當內容，則可利用「iWIN網路內容防護機構」（https://i.win.org.tw）進行檢舉，並依校內程序啟動相關機制。

五、意識「生成式人工智慧」工具可能洩漏個人與組織的隱私與機密

部分用來訓練「生成式人工智慧」工具的資料庫目前在取得、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「生成式人工智慧」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，並優先使用教育版或經學校審查的安全版本，不得以個人帳號登入處理學生資料或校務文件。教師與行政人員亦應提醒學生避免在「生成式人工智慧」工具輸入自己的姓名、照片、聯絡方式或家庭資訊，並建立家長知情與同意機制，以確保未成年學生的資料使用安全。

六、避免過度依賴「生成式人工智慧」工具而侵犯智慧財產權與違反學術倫理

使用人工智慧工具生成教案、試題、計畫等相關教學內容時，須謹慎檢視內容及用詞是否符合教育現場的使用規範與標準。所以我們需規範使用「生成式人工智慧」於學業的時機與方式，並提醒學生使用時可能會侵害他人的智慧財產權，以及有違反學術倫理的疑慮，如沒有提供出處將造成概念上的抄襲。

教師與行政人員亦應確保自身在備課、編寫校務文件或公開發布資料時，正確標示生成內容的來源，不得將生成式人工智慧產製之內容當作原創作品。學校亦需建立明確的使用規範，協助學生理解作業可否使用生成式工具、應如何標註，以及哪些行為可能構成抄襲、代寫或學術不端，以維護學術誠信。

七、遵守「生成式人工智慧」服務使用規範

教師、父母或監護人應提醒學生，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。

建議中小學生皆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、酷英網E-BOT、均一教育平臺或CK-12 Flexi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。

建議選擇使用為教育目的而設計的「生成式人工智慧」工具，是守護學習品質與資訊安全的一大關鍵，因為其具備「蘇格拉底式教學」功能（Cardoso-Silva, J., 2024; OECD, 2026; Sal Khan, 2024），透過提問啟發學生思考，引導學生自己找到解決方案，並有效過濾網路謠言與偏見，提供更精準、健康的知識環境（MIT Sloan Teaching & Learning Technologies, n.d.），亦符合《人工智慧基本法》保障隱私與安全應用之立法精神，同時

也呼應聯合國教科文組織（UNESCO, 2023）對生成式人工智慧工具應用風險的提醒。

考量科技變動快速，本注意事項僅列出本部建置或具公益性之平臺；若需使用其他商用版的「生成式人工智慧」工具，應經由學校評估資安風險，並在師長指導下審慎使用。

八、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。

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，我們應該保持對資訊來源的高度警覺，不要輕易相信未經證實的訊息，並學會如何辨別虛假資訊。同時，我們要提升自己思辨的能力，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。遵守相關的道德和法律規範，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。

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。

附錄1

中小學使用「生成式人工智慧」注意事項2.1（教師、行政人員及家長版）示例

一、理解「生成式人工智慧」工具產生的內容可能有所偏誤：當我們要求生成式人工智慧工具建議旅遊行程時，如果系統本身的資料庫中沒有該地區的氣候環境、地理位置、社會人文以及文化限制等資料，提供的內容可能來自各種網路遊記文章的綜合體，結果就有可能是一份不順路、充滿非當季活動，甚至包含了虛構景點的行程。在教育現場中，我們也需依據課綱、教科書與可靠資料來源進行比對，避免錯誤資訊直接用於教學或傳達給學生。

二、理解「生成式人工智慧」工具可能會減少訊息的多樣性：當我們向生成式人工智慧工具詢問法律或文化問題時，這些工具可能會是基於研發者國家的法律和文化習俗產生的答案。好比我們要求人工智慧工具生成一張新娘圖片時，它可能產生一張穿著白紗的西方臉孔女性，而不是根據使用者當地的文化習俗來產出不同膚色或其他婚禮的服飾。因此在教材、公告或教學應用中，我們應避免直接採用單一文化視角的內容，並協助學生辨識不同觀點。

三、理解「生成式人工智慧」內容的辨識工具僅能作為初步篩檢：當我們使用生成式人工智慧內容辨識工具時，可以快速比對兩篇文章或多篇文章的相似程度，但這些比較結果僅能作為參考。要判斷文章是否為文字或概念抄襲，或根本是由生成式人工智慧工具創造的內容，都仍需要個人比對資料、詳細閱讀理解後，才能進行判斷。在校園情境中，任何學術不端的研判仍需結合學生作品、歷程與教師專業，而非僅以偵測結果作為唯一依據。

四、察覺「深偽技術」日益逼真會產生不實的內容：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）到一些完全虛假或有損名譽的影像作品中。在校園內更應提醒學生不

得轉傳、散布或引用這類未經查證的內容，同時協助學生辨識網路影像真偽。

五、意識「生成式人工智慧」工具可能洩漏個人與組織的隱私與機密：當我們不清楚生成式人工智慧工具的原理及規範，以公司個人資料文件或商業機密為題材向這些工具詢問解答，個人或公司文件、機密程式碼便有可能被收錄到這些工具的訓練資料庫中，而當其他的使用者再度詢問類似問題時，生成式人工智慧工具以收錄的資料庫回答問題，就有機會造成個人隱私或公司機密外洩，形成資安漏洞。

六、避免過度依賴「生成式人工智慧」工具而侵犯智慧財產權與違反學術倫理：當我們使用生成式人工智慧工具產生計畫書時，若有些用詞或字句非一般使用的習慣，應進行修正；或用於出題時，應檢視題目的合宜性及答案的正確性。在作業、教案、校內文件中，如使用生成式人工智慧工具協助生成內容，皆需依規定註明來源，不可將生成出來的內容當作原創作品；並應向學生清楚說明哪些作業可使用生成式人工智慧工具、使用範圍與標註方式，以維護學術誠信。

附錄2

參考文獻

Cardoso-Silva, J. (2024, July 11). *Book review: Brave new words: How AI will revolutionize education (and why that's a good thing)* by Sal Khan. *LSE Impact Blog*. https://blogs.lse.ac.uk/impactofsocialsciences/2024/07/11/brave-new-words-how-ai-will-revolutionize-education-review/

Khan, S. (2024). *Brave new words: How AI will revolutionize education (and why that's a good thing)*. Viking.

MIT Sloan Teaching & Learning Technologies. (n.d.). *When AI Gets It Wrong: Addressing AI hallucinations and bias*. https://mitsloanedtech.mit.edu/ai/basics/addressing-ai-hallucinations-and-bias/

OECD (2026), *OECD Digital Education Outlook 2026: Exploring Effective Uses of Generative AI in Education*, OECD Publishing, Paris, https://doi.org/10.1787/062a7394-en. https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/01/oecd-digital-education-outlook-2026_940e0dd8/062a7394-en.pdf

United Nations Educational, Scientific and Cultural Organization. (2023). *Guidance for generative AI in education and research*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000386693