

國家科學及技術委員會新聞稿

「行政院及所屬機關(構)使用生成式 AI 參考指引(草案)」 引導各機關以負責任及可信賴態度使用生成式 AI

日期：112 年 8 月 31 日

發稿單位：前瞻應用處

聯絡人：賴怡臻科長

電話：02-2737-7128

E-mail：yclai@nstc.gov.tw

國家科學及技術委員會(國科會)今(31)日赴行政院院會報告「行政院及所屬機關(構)使用生成式 AI 參考指引(草案)」(以下簡稱本指引)，有鑑於生成式 AI 可以協助政府在處理業務或提供服務時提升效率，也期望各機關在使用生成式 AI 的同時，能保有執行公務之機密性及專業性，因此訂定本指引，揭示各機關(構)使用生成式 AI 時，應秉持負責任及可信賴之態度，以及安全性、隱私性與資料治理、問責等原則，並掌握自主權與控制權。

跨部會及專家協作形成本指引

111 年底以來，使用生成式 AI 已蔚為風潮，為促成各機關在使用上有一致的認知與基本原則，國科會研擬本指引，除參考各國政府之審慎因應作法、與 AI 技術、法制專家學者及 12 個相關部會協作之外，並於公共政策網路參與平臺徵詢民眾意見。經綜整參考各界意見後，提出本指引草案。

指引包含總說明及十點規定：總說明闡述生成式 AI 之定義、可能風險，以及使用生成式 AI 的態度及原則；使用生成式 AI 主要規定有：須客觀且專業的判斷生成資訊、製作機密文書禁止使用、不得提供應保密及個資等資訊、封閉式地端環境使用須確認系統環境安全性、使用應適當揭露、各機關得另訂定規範或內控措施、採購事項得標者需注意本指引規定等。(參見附件)

國科會將滾動修正本指引

生成式 AI 已應用於各行各業，並逐漸對民生社會產生舉足輕重的影響。因應 AI 發展日新月異，國科會將持續觀察全球相關趨勢與作法，滾動調整本指引，使規範保留彈性，促進風險管理與產業創新發展之間取得平衡。

行政院及所屬機關（構）使用生成式 AI 參考指引（草案）

112 年 08 月 31 日

近年來生成式 AI 快速發展，影響遍及全球產官學研各界。其中 ChatGPT 於 2022 年底發布後，更掀起全球熱潮，且功能極為多元，已被視為人工智慧之一項重大突破。參考歐盟之定義，生成式 AI 模型是一種電腦程式，旨在創建類似於人類製作（human-made）的新內容；其大量蒐集、學習與產出之資料，可能涉及智慧財產權、人權或業務機密之侵害，且其生成結果，因受限於所學習資料之品質與數量，而有可能真偽難辨或創造不存在的資訊，須客觀且專業評估其產出資訊與風險。

考量行政院及所屬機關（構）（以下簡稱各機關）利用生成式 AI 協助執行業務或提供服務，有助於行政效率之提升，且為保持執行公務之機密性及專業性，並促使各機關使用生成式 AI 有一致之認知及基本原則，爰參考各國政府之審慎因應作法，研訂「行政院及所屬機關（構）使用生成式 AI 參考指引」，供各機關依循。各機關得視使用生成式 AI 之業務需求，參酌本參考指引另訂使用規範或內控管理措施。

衡酌 AI 發展具重要性且與資訊安全及國家安全息息相關，本參考指引明確揭示各機關人員使用生成式 AI 時，應秉持負責任及可信賴之態度，掌握自主權與控制權，並秉持安全性、隱私性與資料治理、問責等原則，不得恣意揭露未經公開之公務資訊、不得分享個人隱私資訊及不可完全信任生成資訊。因 AI 之發展日新月異，後續亦將觀察全球 AI 發展趨勢與因應作為，及各機關於人工智慧應用之推動情形，持續滾動修正本參考指引。

本參考指引（草案）共計十點如下：

- 一、為使行政院及所屬機關（構）（以下簡稱各機關）使用生成式 AI 提升行政效率，並避免其可能帶來之國家安全、資訊安全、人權、隱私、倫理及法律等風險，特就各機關使用生成式 AI 應注意之事項，訂定本參考指引。
- 二、生成式 AI 產出之資訊，須由業務承辦人就其風險進行客觀且專業之最終判斷，不得取代業務承辦人之自主思維、創造力及人際互動。

- 三、製作機密文書應由業務承辦人親自撰寫，禁止使用生成式 AI。
前項所稱機密文書，指行政院「文書處理手冊」所定之國家機密文書及一般公務機密文書。
- 四、業務承辦人不得向生成式 AI 提供涉及公務應保密、個人及未經機關（構）同意公開之資訊，亦不得向生成式 AI 詢問可能涉及機密業務或個人資料之問題。但封閉式地端部署之生成式 AI 模型，須確認系統環境安全性後，方得依機密等級分級使用。
- 五、各機關不可完全信任生成式 AI 產出之資訊，亦不得以未經確認之產出內容直接作成行政行為或作為公務決策之唯一依據。
- 六、各機關使用生成式 AI 作為執行業務或提供服務輔助工具時，應適當揭露。
- 七、使用生成式 AI 應遵守資通安全、個人資料保護、著作權與相關資訊使用規定，並注意其侵害智慧財產權與人格權之可能性。各機關得依使用生成式 AI 之設備及業務性質，訂定使用生成式 AI 之規範或內控管理措施。
- 八、各機關應就所辦採購事項，要求得標之法人、團體或個人注意本參考指引，並遵守各該機關依前點所訂定之規範或內控管理措施。
- 九、公營事業機構、公立學校、行政法人及政府捐助之財團法人使用生成式 AI，得準用本參考指引。
- 十、行政院及所屬機關（構）以外之機關得參照本參考指引，訂定各該機關使用生成式 AI 之規範。