行政院各機關

使用AI參考指引

2023年10月15日

簡報大綱

一、參考指引背景簡介

二、參考指引具體要點

三、國科會綜整回應

一、參考指引背景簡介（一）

- 行政院教育科學文化處於112年8月31日發布。
- 生成式AI快速發展，尤其是ChatGPT於2022年底發布後，影響遍及全球產官學研各界。
- 生成式AI模型是一種電腦程式，旨在創建類似於人類製作的新內容：但（一）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；（二）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。

一、參考指引背景簡介（二）

- 生成式AI可協助政府在處理業務或提供服務時提升效率，但也期望各行政機關在使用生成式AI的同時，能保有執行公務之機密性及專業性，因此訂定「行政院及所屬機關(構)使用生成式AI參考指引」。

- 透過該指引，揭示各行政機關(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，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。

一、參考指引背景簡介（三）

- 為促成各行政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，續將依程序簽核函頒各機關參考，並請各部會視業務需要，訂定使用生成式AI之規範或內控管理措施。
- 因AI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。

持續關注國際發展趨勢與滾動修正

養成對生成式AI的正確觀念

- 掌握自主權與控制權
- 客觀且專業評估生成式AI產出之資訊與風險

界定技術/工具運用的責任

- 保持公務之機密性及專業性
- 注意著作權及人格權等

建立必要的安全與內控機制

- 秉持負責任及可信賴之態度使用
- 得視需求訂定內控管理措施

二、參考指引具體要點（一）

一、為使行政院及所屬機關（構）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，仍需業務承辦人就其風險進行客觀且專業的最終判斷，不得取代業務承辦人自主思維、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（此所稱機密文書，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、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。

二、參考指引具體要點（二）

五、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）同意公開之資料，亦不得向生成式AI詢問可能涉及機密業務之問題，或運用生成式AI蒐集或處理個人資料。

六、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。

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。

二、參考指引具體要點（三）

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）以外之其他機關得參照本參考指引，另訂各該機關使用生成式AI之規範。

三、國家科學及技術委員會綜整回應（一）

1.行政院及所屬機關（構）於執行業務及提供服務上使用生成式AI的需求各異，爰各機關（構）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。

2.本指引（草案）雖非屬法律，不具強制性亦無明定罰則，惟規範行政院及所屬機關（構）秉持負責任及可信賴的態度運用生成式AI，具政策宣示效應及示範作用，可引導各界養成對生成式AI的正確觀念，降低可能帶來的風險。

三、國家科學及技術委員會綜整回應（二）

1.本指引（草案）所稱「資訊」，參照政府資訊公開法對於政府資訊之定義 ，已包含文字、影、音、圖、訊號、軟體等類型。

2.國科會之可信任人工智慧對話引擎（TAIDE）之建置，是希望提供一個能夠讓政府或業者繼續發展其專屬的內部應用系統或加值服務之生成式AI基礎模型。未來行政院及所屬機關（構）若導入TAIDE於其業務或服務進行加值應用，其應用原則亦適用本指引相關規範。

三、國家科學及技術委員會綜整回應（三）

5.行政院及所屬機關（構）若有使用生成式AI執行業務或提供服務，則應向該業務或服務之有關對象進行揭露，使其知曉。

6.行政院及所屬機關（構）得依採購性質及管理需求，自行決定要求得標者注意本指引之方式。

以上報告　敬請指教