

屏東縣政府 函

地址：900219屏東縣屏東市自由路527號
聯絡人：黃怡婷
聯絡電話：08-7320415-3651
傳真：08-7322779
電子信箱：a002524@ptc.edu.tw

受文者：屏東縣立里港國民中學

發文日期：中華民國114年2月14日
發文字號：屏府教發字第1145024367號
速別：普通件
密等及解密條件或保密期限：
附件：如說明三 (376530000A114502436700-1.pdf)

主旨：為強化機關資安防護及資訊安全，請檢視各式資通安全管理工作項目及資通安全責任等級應辦事項，以維資訊安全要求及完成應辦事項，請查照。

說明：

- 一、依據本府114年2月7日屏府行訊字第1140033289號函辦理。
- 二、基於國家資通安全考量，公務機關禁止使用 DeepSeek AI 產品，以避免使用者相關數據或資訊遭資安疑慮的產品傳送，造成危害國家資通安全的疑慮。
- 三、機關使用網際網路生成式AI服務，應依據「行政院及所屬機關（構）使用生成式AI參考指引」（如附件）辦理。
- 四、請檢視各業管使用之資通訊設備之密碼設定，包含個人電腦、伺服器、資通訊系統、防火牆、印表機、監視系統…等，勿使用預設密碼，應設定密碼且使用強密碼原則並定期更換，以維護資通訊設備與系統之資通安全，避免遭有心人士竄改密碼與盜取資料造成資安危害。

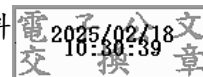
- 五、資通訊設備應具備防護機制，機關防火牆應妥適設定防護政策，僅開啟必要之服務及連線政策、應用程式與連線模式，關閉其餘所有政策，以防護機關存取網際網路服務之資通安全。倘提供遠端管理連線，應限制遠端管理來源IP位址。
- 六、提高電子郵件警覺性，勿隨意開啟與業務無關之電子郵件及連結與附件，必要時與寄件者確認電子郵件相關內容。
- 七、注意各式設備與資訊系統之安全性更新，倘接獲資通安全漏洞修補更新通知，請評估進行更新。
- 八、各辦公場所提供服務民眾之網路(包含無線網路服務)，應與公務網路實體隔離。公務電腦不可連接服務民眾使用之網路。
- 九、各機關開放機關內部同仁及委外廠商進行遠端維護資通系統，應採「原則禁止、例外允許」方式辦理。依資通安全管理法施行細則第4條及資通安全責任等級分級辦法附表十中有關遠端存取相關規定辦理。開放遠端存取期間原則以短天期為限，並建立異常行為管理機制。於結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道(如VPN)登入密碼。
- 十、為避免公務及機敏資料遭不當竊取，導致機關機敏公務資訊外洩或造成國家資通安全危害風險，請勿採購大陸廠牌資通訊產品，現行使用中之產品應盡速完成汰換。
- 十一、機關辦理採購時，如涉及經濟部投資審議委員會公告之「具敏感性或國安(含資安)疑慮之業務範疇」，應確實於招標文件中載明不允許在臺陸資廠商(陸資資訊服務業

者)參與。

十二、餘有本文未載明項目，請依資通安全相關辦法及要求辦理。

正本：各國小、各高國中

副本：本府教育處終身教育科、本府教育處國民教育科、本府教育處特殊及學前教育科、本府教育處學生事務科、本府教育處學務管理科、屏東縣體育發展中心、屏東縣家庭教育中心、本縣教育網路中心、本府教育處教學發展科



行政院及所屬機關（構）使用生成式 AI 參考指引

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）之新內容；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，有可能真偽難辨或創造不存在之資訊，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」（以下簡稱本參考指引），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，於確認系統環境安全性後，得依文書或資訊機密等級分級使用。

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、著作權及相關資訊使用規定，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，訂定使用生成式 AI 之規範。