

附表 1：本部文件資料分級及適用 AI 工具對照表（核定工具清單）

發布日期：115 年 10 月 日
 規範依據：環境部及所屬機關(構)文件資料使用 AI 管理原則第三點第五款、第四點及第七點至第十點規定

文件與資料分級	對應公務具體文件 / 資料範例	適用 AI 工具	使用規範與防護限制
第一級：公開文件資料	依法應主動公開、已合法對外公開或經核定將對外公開之資料，例如新聞稿、社群媒體圖卡、公開統計資料、開放資料集、已發布法規公告、對外宣導文宣或對外回應資料。	得使用商業生成式 AI 工具。	使用前仍應確認資料確屬公開或可公開；不得輸入尚未核定公開、含未依法得公開之個人資料、密等或依法限制閱覽之內容。 產出內容正式運用或對外發布前，應經人工核實。
第二級：內部文件資料	僅供內部業務使用、不宜廣泛對外流通之資料，例如內部不公開會議紀錄、行政作業說明、一般內部作業資料、內部教育訓練教材或不涉個人資料及評選敏感事項之內部彙整資料。	限用環境部核定具備外部服務商資料不留存機制之 AI 工具	AI 服務提供商不得將輸入資料及運算軌跡作為 AI 模型訓練或改善服務之用。 產出內容正式運用前，應經人工核實。
第三級：限閱文件資料	尚未公開之政策草案、採購評選文件、個人資料案件、車牌辨識結果、環境稽查計畫或其他依法應限制閱覽之資料。	未經不可逆去識別化或仍屬限閱內容者，限用本部指定之封閉網路運算環境內之 AI 工具（如國家高速網路與計算中心算力環境）。經不可逆去識別化並經業務單位主管核可後，得比照第二級內部文件資料辦理。	非經不可逆去識別化並經業務單位主管核可，不得輸入商業 AI 工具。使用 AI 工具應留存使用紀錄至少半年；法令、契約或個案規定較長者，從其規定。紀錄內容包括提示詞、附件、AI 工具輸出結果及操作帳號，並應依同級資料保護。 產出內容正式應用前，應經人工核實並經業務單位主管核定。
第四級：密等文件資料	涉及密等及密等以上之資料、具體稽查行動與查核名單、資訊安全架構或個人資料	經業務單位主管核定後，限用本部指定之封閉網路運算環境內 AI	應依國家機密保護、資通安全及個人資料保護等相關規定從嚴辦理。

	料保護法第六條第一項所定之個人資料項目等應嚴格限制知悉範圍之資料。	工具；嚴禁使用任何商業 AI 工具或外部雲端服務。	使用 AI 工具應留存使用紀錄至少半年；法令、契約或個案規定較長者，從其規定。紀錄內容包括提示詞、附件、AI 工具輸出結果及操作帳號，並應依同級資料保護。 產出內容正式應用前，應經人工核實並經業務單位主管核定。
--	-----------------------------------	---------------------------	--

補充使用規範與注意事項：

- 一、核定工具清單動態調整：本附表所稱環境部核定 AI 工具及帳號，由環境資訊科技司會同業務需求辦理資訊安全、個人資料保護及服務條款評估後核定或公告；實際工具、帳號、可處理資料等級及防護條件，得視採購、建置及資安風險滾動檢討調整。
- 二、分級確認、標示及帳號限制：使用 AI 工具前應先判斷文件資料分級；第三級、第四級文件資料分類須經業務單位主管或其授權人員複核，分級疑義從嚴認定。第二級以上文件資料應於頁眉、浮水印、系統標籤或交付清冊標示分級屬性；不得以個人帳號、自費商業版或非本部核定或指定工具處理。
- 三、外部人員及委外團隊管理：外部人員接觸或使用本部第二級以上文件資料前，應以書面切結適用本原則並簽署本部所定保密切結書及連帶保證書；涉及委辦計畫者，應納入契約，並限用環境部環境資訊科技司提供或核定之 AI 工具及帳號，衍生經費由業務單位分攤。專案結束或契約終止時，應立即停用使用權限，相關文件資料除依法令或契約應保存者外，應返還、刪除或銷毀。