# 國立高雄餐旅大學永續發展與校務研究中心使用生成式人工智慧處理校務研究資料作業規範

中華民國 115 年 9 月 15 日 115 學年度第一學期第二次中心會議通過
中華民國 115 年 10 月 15 日 115 學年度第一學期第三次中心會議修正後通過

**第一條 訂定目的及依據**

國立高雄餐旅大學（以下簡稱本校）永續發展與校務研究中心（以下簡稱本中心）為規範相關人員合法、安全及客觀使用生成式人工智慧（Generative Artificial Intelligence，以下簡稱生成式 AI），提升校務研究分析效能，並確保校務資料安全、個人資料保護、學術倫理及決策責任，依個人資料保護法、資通安全管理法、本校個人資料保護管理要點及資訊安全政策，並參照行政院及所屬機關（構）使用生成式 AI 參考指引，訂定本規範。

**第二條 用詞定義**

本規範用詞，定義如下：

一、**生成式 AI**：指利用演算法、模型及資料集，自動生成文字、數據、程式碼、圖表、影像或音訊等內容之資訊技術或工具。

二、**校務研究資料**：指本中心為支援校務發展、精進教學品質、評估學生學習成效及資源配置決策，所蒐集、處理或利用之結構化及非結構化資料，包括學生學籍、成績歷程、教職員資料、問卷調查及質性意見等。

三、**機敏資料**：指個人資料保護法第六條第一項所定之特種個人資料、得以直接或間接方式識別特定個人之一般個人資料，及未經本校核定公開之校務決策機密資料或智慧財產。

四、**去識別化**：指個人資料以遮蔽、代碼化、雜湊、彙總或統計概化等技術處理，使其無從直接或間接識別特定當事人。

**第三條 適用對象**

本規範適用於本中心編制內人員、專任與兼任研究人員、專案助理、兼任助理，及參與或受託執行本校校務研究專案之人員（以下統稱使用者）。

**第四條 使用原則**

使用者使用生成式 AI，應遵循下列原則：

一、**輔助工具原則**：生成式 AI 僅得作為研究分析之輔助工具，使用者應全程掌握研究設計及流程，不得將資料分析之詮釋及最終決策判斷全權交由生成式 AI 為之。

二、**當責與客觀原則**：使用者應對校務研究成果負最終責任，不得以生成式 AI 產出結果為由，免除專業審查、資料覆核或研究倫理責任。

三、**資料最小化原則**：使用生成式 AI 時，輸入之資料範圍應以達成特定分析目的所必要者為限。

四、**公平與非歧視原則**：使用者應主動檢視分析過程及結果，是否因訓練資料或模型預設偏誤，對特定性別、族群、入學管道或弱勢學生群體產生系統性偏見或負面標籤。

**第五條 資料安全及使用環境限制**

使用者使用生成式 AI 工具，應遵守下列資料安全規定：

一、**禁止輸入未去識別化之機敏資料**：教職員工生個人資料、個別諮商紀錄、性別平等事件及獎懲調查資料、人事薪資資料及未公開之重大財務決策資料，未經本中心主管核准並完成去識別化者，不得輸入未經本校授權之外部雲端生成式 AI 服務；申請核准時，應填具附表一之檢核表。

二、**質性文本處理限制**：學生回饋問卷、教學評鑑質性意見及訪談逐字稿等非結構化資料，於輸入外部生成式 AI 工具進行主題分析或情緒辨識前，應先移除姓名、學號、系所全稱、特定時間與地點等足以識別個人之資訊。

三、**模型與服務選用**：

(一) 優先使用本校自建之地端部署模型，或本校採購並具資通安全契約保障之企業級授權服務（如契約明定不保留使用者輸入資料、不將對話資料用於模型訓練）。

(二) 不得使用經主管機關認定為危害國家資通安全產品之軟硬體、雲端服務及人工智慧模型。

**第六條 許可及限制使用範圍**

使用者使用生成式 AI 之業務情境，區分如下：

一、**許可使用情境**：

(一) 統計及資料科學程式碼（如 R、Python、SQL）之撰寫、除錯及效能最佳化。

(二) 國內外校務研究及高等教育評鑑文獻之檢索策略研擬及摘要整理。

(三) 研究假設建立之輔助發想。

(四) 已完成去識別化或經統計彙總之資料圖表語意摘要及排版潤飾。

二、**限制及禁止使用情境**：

(一) 利用生成式 AI 產生未經統計驗證之虛構指標或數值。

(二) 未經專案小組審查，逕以生成式 AI 產出之預測性推論（如休學或退學機率、學業不適應指標），作為對個別學生差別待遇或限制其權益之行政處分依據。

(三) 利用生成式 AI 產生或改寫有侵害他人智慧財產權之虞之內容。

**第七條 產出查核及可重現性**

為防範生成式 AI 產生錯誤資訊或虛構內容（即模型幻覺），使用者應履行下列查核義務：

一、報告引用之校務統計數字、比率、排名及法規依據，應逐筆與本校原始校務資料或法規原文核對，不得直接採用生成式 AI 產生之數值或內容。

二、使用者應留存關鍵分析之原始資料擷取紀錄、資料清理程式碼、主要提示詞及分析紀錄，以確保校務研究結果之透明性及可重現性。

**第八條 使用情形揭露**

本中心產出之校務研究專題分析報告、年報、決策簡報或教育部計畫管考成果，於研究過程中實質使用生成式 AI 協助者，應於報告之「研究方法」或「附註說明」中揭露下列事項：

一、所使用之生成式 AI 工具名稱、版本及授權類型。

二、生成式 AI 工具於該研究案中之具體角色及使用範圍（如輔助程式撰寫、質性文本

編碼建議、文字校對等）。

**第九條 資通安全及個人資料事件通報**

使用者於使用生成式 AI 過程中，發生或疑似發生機敏校務資料外洩、個人資料遭侵害或違反本校資通安全相關規定之情事時，應立即採取下列措施：

一、中止該生成式 AI 作業，並保全相關操作紀錄。

二、立即通報本中心主管，並依本校個人資料外洩事件應變及通報作業程序與資通安全事件通報作業規定，通報本校資通安全權責單位。

三、採取損害控制措施，評估受影響之人員範圍及權益，並依個人資料保護法等相關規定辦理補救及通知當事人事宜。

**第十條 教育訓練及保密切結**

本中心每年應至少辦理一次使用者生成式 AI 素養、資料隱私安全及演算法偏誤防範之教育訓練。新進人員到職時，應先研讀本規範，並簽署資料保密及生成式 AI 使用切結書。

**第十一條 未盡事宜及施行程序**

本規範未盡事宜，依相關法令及本校相關規定辦理。

本規範經本中心會議通過，陳請中心主任核定後發布施行；修正時，亦同。

**本規章負責單位：永續發展與校務研究中心**

**附表**

**附表一：校務研究資料輸入外部生成式 AI 前檢核表**