國立高雄師範大學
數位安全與治理指引

目錄

第一章　總則 2
第二章　資訊安全管理 2
第三章　個人資料保護 3
第四章　智慧財產權保護 4
第五章　人工智慧倫理 5
第六章　內部監督 7
第七章　附則 7

國立高雄師範大學 數位安全與治理指引

114 年 11 月 25 日 114 年第 2 次資安、個資暨智財保護管理審查會議通過
115 年 5 月 27 日 115 年第 1 次數位安全與治理查會議修正通過
115 年 9 月 16 日 115 學年度第 1 次行政會議通過

第一章 總則

第一條、 本校為推動人工智慧倫理、資訊安全管理、個人資料保護及智慧財產權保護，成立跨單位數位安全與治理委員會，負責本校數位安全與治理業務之政策、計畫、資源調度等統籌、協調與研議。

第二條、 本指引係提供本校各行政部門、學術單位、服務中心及研究中心(以下簡稱各單位)於辦理資訊安全管理、個人資料保護及智慧財產權保護、人工智慧倫理等事項之原則性與方向性規範，惟相關事項涉及法令或主管機關規範者，仍應依其規定辦理。

第三條、 各單位應依其業務性質，分別就人工智慧倫理、資訊安全管理、個人資料保護及智慧財產權保護事項，指定至少一名專責窗口，負責執行稽核、自我檢查、事件通報及相關政策推動等工作。

第四條、 各單位辦理資訊安全管理、個人資料保護及智慧財產權保護等相關業務，涉及人工智慧或生成式人工智慧之使用、評估、管理或風險控管事項，依本指引第五章「人工智慧倫理」之規定辦理。

第二章 資訊安全管理

第五條、 各單位應辦理下列資訊安全管理事項：

一、落實單位內資訊資產盤點與風險評鑑作業。

二、落實單位內資訊安全自我檢查作業。

三、遵守及宣導資訊安全規範與觀念。

四、為降低資通安全事件造成之損害，各單位應即時通報及處置，並加以記錄。

第六條、 協助本校資通安全政策之推動與執行。

第七條、 配合辦理本校資安稽核作業。

第八條、 各單位之公務電腦之使用原則：

一、使用具合法版權軟體，避免上網下載來路不明之軟體。

二、開啟作業系統自動更新並更新應用程式至最新版本。

三、安裝防毒軟體且定期掃描及更新病毒碼至最新版本。

四、電腦密碼設定須符合安全性原則並定期更新。

五、安裝本校「VANS 電腦組態蒐集工具」，以利電腦資源之管理。

六、不可使用有危害國家資通訊安全疑慮之軟體或硬體。

第九條、 行動裝置及可攜式媒體之使用原則：

一、行動裝置多採用鋰電池，請避免在高溫、潮濕或封閉空間中充電，並使用原廠或合格之充電器與線材。若發現裝置異常發熱、膨脹或發出異味，應立即停止使用，避免發生安全事故。

二、僅安裝可信任來源之軟體、避免開通不必要之軟體權限、定期更新軟體與作業系統。避免在裝置中儲存敏感或機密資料，以降低資料外洩風險。

三、校外人士不得擅自使用行動裝置連接內部系統或未經授權的資通設備。如使用校園 Wi-Fi 或相關資源，應依程序申請並限於授權範圍內使用，不得擅自拍攝、錄音、複製或外傳具敏感性與機密性的資料。各單位應注意校外人士於安全限制區域內之裝置使用行為，並於必要時進行使用管控。

第三章 個人資料保護

第十條、 各單位應辦理下列個人資料保護事項：

一、個人資料安全維護，防止單位內個人資料被竊取、竄改、毀損、滅失或洩漏。

二、落實單位內資料、文件二項資訊資產類別內涵個資之盤點與風險評鑑作業。

三、落實單位內個人資料保護自我檢查作業。

四、遵守及宣導各人資料保護規範與觀念。

五、為降低個人資料洩漏造成之損害，各單位應即時通報及處置，並加以記錄。

第十一條、 協助本校個人資料保護政策之推動與執行。

第十二條、 配合辦理本校個人資料保護稽核作業。

第十三條、 非工作期間，重要、機密文件不放置於桌上，且於下班或離開辦公室前應鎖入安全空間。

第十四條、 對於含有個人資料文件或檔案，其資訊不再屬必要或已超越資料保存年限者，應填報「資料處理申請單」，經權責單位主管核准後辦理刪除或銷毀程序，並留存相關刪除紀錄。

第十五條、 對於含有個人資料檔案儲存及傳輸均須實施檔案加密。

第十六條、 落實本校「數位安全與治理執行辦法」處理個人資料檔案之人員對於個人資料之蒐集、處理或利用，應尊重當事人之權益及意願，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

第十七條、 落實本校「數位安全與治理執行辦法」涉及蒐集個人資料者，注意資料蒐集最小化、存取控制及詳閱設定內容等。

第十八條、 因應校務所需蒐集、處理及利用個人資料，應依據個人資料保護法及相關規定辦理隱私權政策暨告知事項聲明：

一、個人資料蒐集之目的：辦理本校人事管理、學生(含入學前報名、畢業和結業生)資料管理、教育或訓練、產學合作、資通安全與管理、學術研究、調查、統計與研究分析、圖書館與出版品管理、稅務行政、存款與匯款、契約、類似契約、保險、保健醫療服務、衛生行政、國內外交流業務及其他校務相關業務之需要。

二、蒐集之個人資料類別:識別類(例如:姓名、身分證統一編號、護照號碼、電話號碼、行動電話、通訊及戶籍地址、電子郵遞地址、工作單位、職稱與緊急聯絡人姓名電話地

址)、特徵類(例如:出生年月日、國籍、性別)、家庭情形、教育、技術或其他專業(例如:學校紀錄、資格或技術、職業專長、著作、應考人紀錄）、受僱情形、健康紀錄及符合蒐集目的之各項個人資料類別等。

三、個人資料利用之期間、地區、對象及方式:

（一）期間：個人資料蒐集之特定目的存續期間、依相關法令規定、契約約定或本校因執行業務所必須之保存年限。

（二）地區：本國與境外學術研究交流地區。

（三）對象：本校及其他與本校有業務往來之公務及非公務機關。

（四）方式：以自動化機器或其他非自動化之利用方式。

四、可依個人資料保護法，就個人資料行使以下權利：

（一）查詢或請求閱覽。

（二）請求製給複製本。

（三）請求補充或更正。

（四）請求停止蒐集、處理或利用。

（五）請求刪除。

惟依相關法令規定、契約約定或本校因執行業務所必須者，得不依請求為之。

五、個人資料之提供：

（一）若拒絕提供個人資料，本校將無法提供相關服務，亦可能無法維護相關權益。

（二）請依各項服務需求提供正確、最新及完整的個人資料，若個人資料有任何異動，請主動向本校各單位申請更正。

（三）若提供錯誤、過時、不完整或具誤導性的資料，而損及相關權益，本校將不負相關賠償責任。

（四）若未滿二十歲，應讓當事人的法定代理人閱讀、瞭解告知聲明；但當事人已接受本服務，視為當事人已取得法定代理人之同意。

六、個人資料之保密：本校將善盡個人資料保護之責。如因天災、事變或其他不可抗力致使個人資料被竊取、洩漏、竄改、遭其他侵害者，將於查明後以電話、電子郵件或網站公告等方法，擇適當方式通知。

七、當個人資料使用方式與原先蒐集的目的不同時,本校會在使用前先徵求個人書面同意,個人可以拒絕本校利用個人資料，但可能導致權益受損。

八、其他注意事項

（一）請妥善保管帳號、密碼等相關資料，勿將其提供給第三者，尤其是密碼；在使用本校單一登入系統所提供之各項服務功能後，請務必登出帳號。若是與他人共享電腦或使用公共電腦，切記要在離開前關閉瀏覽器視窗，以防止他人讀取您的資料。

（二）本校保留隨時修改本聲明規範之權利，並將修訂後之規範公告於本校網站，不另作個別通知；如有未盡事宜，依本校學則、個人資料保護法及相關法令之規定辦理。

第四章 智慧財產權保護

第十九條、　各單位應辦理下列智慧財產權保護事項：

一、落實單位內智慧財產權保護稽核作業。

二、落實單位內智慧財產權保護自我檢查作業。

三、遵守及宣導相關智慧財產權規範與觀念。

四、為降低智慧財產權侵害事件造成之損害，各單位應即時通報及處置，並加以記錄。

第二十條、　協助本校智慧財產權保護政策之推動與執行。

第二十一條、配合辦理本校智慧財產權保護稽核作業。

第二十二條、支持教師自編教材或講義授課，提升教師正確著作權及智慧財產權觀念。

第二十三條、積極參與學校智慧財產權課程或研討會、座談會、研習或相關活動，強化智慧財產權觀念，賦予正確資訊與合理運用概念。

第二十四條、影印、掃描書籍時應「遵守智慧財產權觀念」及「禁止不法影印、下載及散布」或類似警語等相關規定。

第二十五條、應使用正版教科書或透過二手書活動取得教科書。

第二十六條、使用電腦應「尊重與保護智慧財產權」、校園網路使用規範及合法軟體，共同建立校園資訊安全環境。

第五章 人工智慧倫理

第二十七條、為促進校內人員於教學、學習、研究與行政流程中合理、負責且審慎地運用人工智慧技術，並確保校園知識生態、學術倫理與資訊安全，特訂定本章規範。

第二十八條、人工智慧、生成式人工智慧及 AI 工具定義如下：

一、人工智慧（Artificial Intelligence, AI）：指利用演算法、統計方法、機器學習、深度學習或其他計算技術，使系統具備感知、推理、學習、決策、自動化處理或輔助人類執行任務能力之科技。其應用包括但不限於自然語言處理、模式辨識、資料分析、預測模型與自動化技術。

二、生成式人工智慧（Generative AI）：指以機器學習、深度學習或類神經網路模型，透過學習大量資料，能自主生成文本、圖像、音訊、影音、程式碼或其他形式內容之人工智慧技術。生成式 AI 具有高度模擬人類創作之能力，其生成內容可能含模型幻覺、偏誤或未經驗證訊息，需由使用者審慎判斷與負責。

三、AI 工具：指具備本條所述人工智慧或生成式人工智慧功能之軟體、平台或系統，包含開源與商業服務（如大型語言模型、影像生成工具、智慧輔助系統等）。

第二十九條、各單位應辦理下列人工智慧倫理事項：

一、協助單位內應用人工智慧工具確實依據本校相關法規辦理。

二、落實單位內人工智慧使用倫理自我檢查作業。

三、遵守及宣導人工智慧使用倫理相關規範及概念。

第三十條、　本校為行政、教學及學習目的使用生成式 AI 模型者，應遵循智慧財產權之商標法、專利法、著作權法、營業秘密法等相關規定，並主動披露使用資訊及參酌本指引辦理。

第三十一條、 蒐集資料訓練 AI 模型階段，訓練資料如受著作權法保護(以下稱原始著作)，涉及「重製」原始著作之行為，除有著作權法第 44 條至第 65 條合理使用之情形外，應取得著作財產權人之同意或授權，始得為之。

第三十二條、 利用生成式 AI 模型生成內容者(以下稱「AI 利用人」)：

一、如係單純下指令，並未投入精神創作，由生成式 AI 模型獨立自主運算而生成全新內容，該 AI 生成內容不受著作權法保護。

二、在 AI 模型生成內容之階段，如僅係將訓練資料中之原始著作予以重製再現作後續商業利用(例如：將 AI 生成圖像印製海報販售)，亦會涉及原始著作之「重製」等利用行為，建議 AI 利用人先向 AI 模型之開發或管理者釐清有無取得著作財產權人之授權及得否轉授權第三人進行商業利用，以免產生著作權糾紛。

第三十三條、 使用生成式 AI 人工智慧應遵守資通安全、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。

第三十四條、 涉及資訊安全、個人資料保護及智慧財產權管理執行業務，參照本校「數位安全與治理執行辦法」辦理。

第三十五條、 AI 工具使用涉及之學務與教務相關細部作業，教師教學與研究應用之宣導與執行，由教務處及通識教育中心統籌推動；學生學習與評量規範由學生事務處負責；行政人員公務作業之應用指引且涉及校園網路資訊安全、合法軟體管理及圖書版權相關事項由圖書資訊處辦理；校園影印與版權宣導相關事項由總務處負責。

第三十六條、 校內人員於教學、學習、創作、研究或行政活動中使用人工智慧工具時，應秉持以下 AI 工具應用倫理之基本原則，以誠信、負責與透明之態度，使其使用不侵害學術品質，並確保人類專業判斷為最終決策基礎：

一、合法性與合規原則：

（一）使用者應遵守本國法規及本校資訊安全、學術倫理與智慧財產權相關規範。

（二）AI 生成內容不得未經查證即引用，並不得用於規避學術誠信要求或作業、測驗評量規範。

（三）使用 AI 工具於需處理個人資料、敏感資訊或具風險之情境時，應事先評估並遵守法規，不得將受保護之資訊輸入非經授權之 AI 平台。

（四）於測驗、評量、線上考試、學習診斷或其他需驗證個人能力之活動中，應維持評量之公平性與學術誠信。如教師或相關單位訂有禁止或限制使用人工智慧工具之規範，學生應依規範行之，以確保評量結果能真實反映個人表現。

（五）教師得依課程性質、教學目標或評量方式，訂定人工智慧工具使用之合理界線與指引，並應於事前充分告知學生，以維護教學品質與評量公正性。

二、透明與揭露原則

（一）AI 生成內容若使用於正式產出（如研究成果、課堂作業、行政文件、報告等），應依用途、領域及相關規範適當揭露 AI 使用方式、工具名稱、資料來源及其限制。

（二）研究人員須遵守學術期刊、研究計畫與倫理規範中關於人工智慧協作者或工具使用之揭露要求。

三、資訊驗證與品質原則

（一）使用者對 AI 工具產生之內容負有查證義務，應具備批判性思辨，避免使用含錯誤

資訊、不當推論、偏誤或歧視之內容。

（二）使用者應確保生成內容與事實相符，不得以未經驗證之 AI 生成資訊作為唯一判斷或研究依據。

四、人類主體性與責任歸屬原則

（一）使用者應保持人類最終決策與專業判斷角色，不得將人工智慧之結果視為可直接替代人類責任。

（二）使用人工智慧所產生的法律、倫理或學術責任，均由使用者本人負擔，並不得主張僅因為工具生成而免責。

五、公平性與避免偏見原則

（一）AI 的使用應避免再製或強化性別、族群、年齡、身心狀態等偏見。

（二）使用者應關注 AI 模型在訓練資料中可能隱含的偏誤，並依場域情境採取必要之避險措施。

六、安全性與風險管理原則

（一）使用者於選用 AI 工具前，應瞭解工具之資安風險、資料處理方式及可能之誤用情形。

（二）對具高度風險之 AI 應用（如個資處理、學生評量、行政決策輔助）應依循本校相關辦法或送「數位安全與治理委員會」議處。

（三）教師於規劃或執行各類測驗及評量時，應以維護評量公平與誠信為原則，並採具體可行之措施以降低人工智慧不當使用所可能造成之影響。

（四）若於評量過程或結果中出現疑似人工智慧不當使用之情形，教師得依職責採行適當方式確認學生之實際表現，並依本校相關規範處理，以維護學術誠信與評量正確性。

第三十七條、 本章訂定之使用原則提供人工智慧倫理工具應用原則參考，個別情境如教學、研究、行政、測驗評量、資料處理等之實務規範及程序，由本校另訂相關法規辦理。

第六章 內部監督

第三十八條、 內部監督以資安及個資內部稽核之方式進行監督，依本校資訊資產及資通系統風險高低、教學單位特性訂定先後順序，規劃全校各單位分年分階段進行內部稽核。

第三十九條、 各單位於稽核前應填列資安及個資稽核相關表單，並備妥相關文件，以利稽核進行。

第四十條、 各單位應積極進行因資安及個資稽核所提出之矯正與預防措施，確保符合相關法規，降低資訊安全與個資風險。

第七章 附則

第四十一條、 本指引經數位安全與治理委員會、行政會議通過，陳請校長核定後實施，修定時亦同。