臺北市公務員 AI 素養培育計畫

115 年 5 月 6 日核定

壹、 緣起

隨著人工智慧技術的快速發展，特別是生成式人工智慧，全球已正式進入以資料與演算法為核心的數位治理時代。AI 不僅改變產業運作模式，更正在重塑政府提供公共服務、進行政策分析及決策制定的方式。

在公共部門中，AI 已逐步應用於行政流程自動化、政策資料分析、民意回應及智慧服務設計等領域。其帶來之效益包括提升行政效率、縮短決策時間、強化政策精準度及提高公共服務品質。換言之，AI 已不再僅為輔助工具，而是影響政府治理能力與國家競爭力之關鍵基礎設施。然而，AI 的導入同時伴隨高度風險與治理挑戰。包括資料錯誤可能導致不公平決策、生成式 AI 產生錯誤資訊之風險、決策過程缺乏透明性與可解釋性，以及責任歸屬不明確等問題。特別是在涉及公民權益之行政裁量與政策執行過程中，若缺乏適當之治理機制，將可能對政府公信力造成重大影響。

依據經濟合作暨發展組織（OECD）於《Governing with Artificial Intelligence》（2025）報告指出，各國政府已廣泛採用 AI 於公共服務設計與提供，但在推動過程中普遍面臨人員能力不足、風險控管機制未健全與治理制度尚未成熟等共通問題。報告亦強調，公務員 AI 素養與治理能力，已成為 AI 政策成功與否之關鍵因素。

在此背景下，公務體系若未能即時建立 AI 素養培訓與治理能力，將面臨三項關鍵風險。首先是公務員自發使用 AI 工具而缺乏規範，可能造成資訊安全與決策錯誤風險；其次是各單位分散導入 AI 應用，缺乏整體治理架構，導致資源重複投入與政策不一致；最後為在面對社會輿論及監督時，缺乏明確之制度支撐，將影響政府信任基礎。

因此，臺北市政府為推動 AI 發展，以前瞻視野佈局數位轉型藍圖，深化跨機關之協作量能與資源整合，加速 AI 技術落實於市政治理與市民服務，設立「臺北市人工智慧推動小組」，以統籌本府 AI 發展方向及治理機制。

然而，建立系統化之公務員 AI 素養培訓體系，亦為推動數位治理之必要條

件。本計畫以分級培訓為核心，針對基層、中階及高階公務員之不同職能需求，設計具結構性之 AI 核心素養與能力指標，並建立培訓機制，從操作應用、導入規劃至治理決策，逐步建構完整之公務體系 AI 能力與治理架構。

此外，隨著代理人 AI（Agentic AI）的快速發展，人工智慧之角色已由單一的內容生成工具（Generative AI），逐步演進為具備「任務導向自主決策能力」（goal-driven autonomy）之智慧代理系統。此類系統通常基於大型語言模型（LLM）結合多代理系統（multi-agent systems）、工具調用機制（tool use / API calling）、任務拆解（task decomposition）與規劃能力（planning and reasoning），並透過記憶模組（memory module）與工作流程編排（workflow orchestration），可依據高階指令進行多步驟任務執行，包括資料檢索（retrieval-augmented generation, RAG）、跨系統資料整合、決策推理（reasoning loop）與結果回報，形成具持續運作能力之智慧協作體系。

對公務體系而言，代理人 AI 未來可廣泛應用於跨局處資料整合與語意對齊（data integration and semantic alignment）、陳情案件自動分類與分流（case triaging）、法規與政策文件比對分析（regulatory compliance analysis）、會議前決策支援資料準備（decision support preparation）、專案進度監測與異常預警（project monitoring and anomaly detection），以及民眾服務流程自動化（service workflow automation）等情境，具備顯著提升行政效率、降低人工作業負擔，並強化流程標準化與一致性之潛力。

然而，相較於傳統生成式 AI，代理人 AI 具備更高程度之自主性（autonomy）、跨系統操作能力（cross-system interaction）與持續執行特性（persistent execution），其運作涉及多步推理鏈（chain-of-thought reasoning）、多工具協同（tool chaining）與動態決策調整，若缺乏完善之治理機制（AI governance framework），例如權限控管（access control）、流程監督（human-in-the-loop, HITL）、人工覆核（human oversight）、操作日誌與審計追蹤（logging and audit trail），將可能導致錯誤決策擴散（error propagation）、責任歸屬不明（accountability ambiguity）及資訊安全風險（cybersecurity risk）等問題。

因此，本計畫有必要將代理人 AI 納入公務員 AI 素養培育之核心範疇，透過系統性培訓，使公務人員不僅具備 AI 工具操作能力，更能理解其底層運作邏輯（model behavior）、系統架構（system architecture）與風險控管機制，進而具備規劃（planning）、導入（deployment）與監督（governance）代理人 AI 之能力，以確保其於公務場域中之安全、可靠與有效運作。

貳、 各國的 AI 素養

根據研究報告的分析，各國政府與產業界正積極合作推動人工智慧素養培訓，以奠定公共部門數位化轉型的基礎。國際間 AI 培訓趨勢主要涵蓋三大面向，模型訓練與系統開發（做 AI）、多元類型任務應用（用 AI），以及 AI 基礎原理引發的潛在風險與法規管理（管 AI）。

一、美國強調跨界合作與風險管控

美國總務管理局於 2023 年與史丹佛大學人類中心人工智慧研究所合作，為聯邦雇員推出 AI 培訓系列課程。課程旨在介紹 AI 的概念與理論，幫助聯邦雇員了解背後的技術基礎，並探討使用 AI 時可能發生的風險及降低風險的措施。主題涵蓋 AI 科學與技術基礎、基礎模型的機會與挑戰、實施安全穩健的 AI、公部門 AI 案例、偏見與資料隱私問題，以及 AI 創新的未來。

二、英國著重生成式 AI 的安全與負責任使用

英國中央數位及資料辦公室推出了一系列關於生成式 AI 數位學習課程，以協助公務員安全、負責任且高效率的使用 AI 工具。課程強調在適當階段使用與選擇合適的 AI 工具，並提出 10 項原則，包含合法與合乎道德使用、確保安全、進行有意義的人工控制、管理 AI 生命週期等。具體課程模組涵蓋生成式 AI 簡介、風險與道德、工具與應用、提示工程，以及策略與治理。

三、新加坡結合產業界資源的數位學習平台

新加坡推出政府數位學習平台 GovTech Digital Academy，與 Amazon Web Services、Coursera、Google、Microsoft 等業界知名企業合作，以多元形式進行培訓。平台中專為公共服務官員設計的數據與人工智慧素養課程，旨在提升數據與 AI 知識，內容包含理解數據科學及 AI 應用優劣、數據的重要性、數據視覺化圖

表、機器學習演算法，以及如何正確開展 AI 專案。

四、國際趨勢由生成式 AI 走向代理人 AI

近年政府與產業界 AI 應用正由單一問答與內容生成，逐步發展為可串接知識庫、表單系統、排程工具與業務規則之代理人 AI 架構。此一趨勢意味公務員未來所需能力，不僅是操作單一 AI 工具，更包括理解代理人 AI 之任務分派方式、工具調用範圍、權限設計、例外處理與人員覆核機制，方能在提升效率之同時，維持政府治理之可控性與可問責性。

參、 AI 素養

公務員 AI 素養係指公務人員在人工智慧技術快速發展之背景下，於公共行政情境中所應具備之整體能力體系。其內涵不僅包含對人工智慧基本原理之理解，更涵蓋實務應用能力、風險辨識能力、應用規劃能力及制度治理能力。此一素養之建構，係為確保 AI 應用能在提升行政效能之同時，兼顧公共責任與社會信任。本計畫依據公務體系不同職級之職責與決策權限，將 AI 素養區分為六個面向，並分別就其能力內涵與發展方向加以說明，表一為素養對應的能力指標，其中新增「代理人 AI 與流程協作」面向，以回應新一代 AI 系統由單點生成走向多步驟執行、跨系統協作與流程自動化之發展。

一、AI 基礎理解素養

AI 基礎理解素養係指公務員對人工智慧之基本概念、運作原理及其限制之理解能力。此一素養為所有 AI 應用之基礎，其核心在於建立正確認知，使公務員能理解 AI 並非具備自主判斷能力之決策者，而係透過資料訓練所形成之機率性預測系統。

在知識層面上，公務員應系統性理解人工智慧之主要技術類型，包括機器學習、深度學習與生成式人工智慧之差異與特性，並掌握其基本運作邏輯。亦應理解資料品質對模型輸出結果之影響，認識資料錯誤導致不準確之決策結果。同時，公務員應瞭解生成式 AI 之內容生成機制，特別是其可能產生幻覺與虛假資訊之風險。

在技能層面上，公務員應能辨識不同 AI 技術之基本特性，並初步判斷其適

用情境。例如，能區分 AI 適合用於行政輔助或資料整理等低風險任務，或不適合直接用於涉及公民權益之裁量決策。亦應具備檢視 AI 輸出內容之能力，能辨識其是否存在錯誤、不一致或不合理之處，並進行必要之修正與補強。

在態度層面上，公務員應建立審慎使用 AI 之觀念，不將 AI 輸出結果視為最終答案，並強化風險與責任意識。公務員應理解，即使使用 AI 工具，最終行政決策仍須由人員負責。亦應重視資料安全與公共信任，確保 AI 應用過程符合政府治理之基本原則與社會期待。

二、AI 工具應用素養

AI 工具應用素養係指公務員能在符合法規與風險控管前提下，將人工智慧工具有效整合至日常行政作業流程之能力。其核心不在於單純熟悉工具操作，而在於理解 AI 在不同業務情境中的適用範圍、限制與風險，並透過適當的人機協作方式，提升行政效率與決策品質。此一素養亦強調 AI 應用應服務於公共價值與行政專業，而非取代公務員之專業判斷。

在知識層面上，公務員應系統性理解各類 AI 工具之功能特性與應用範圍，包括生成式 AI 於文字生成、資料整理與知識輔助等應用，以及其在行政流程中之可能角色。公務員亦應掌握提示語設計之基本原則，例如如何透過角色設定、任務說明、格式限制與條件設定，引導 AI 產出符合行政需求之內容。同時，應理解 AI 工具之運作限制，包括其可能產生之錯誤、幻覺與資訊不完整問題，以及其不適用於高風險決策之特性。另在制度面上，公務員亦須瞭解資訊安全與個人資料保護相關規範，清楚辨識何種資料可輸入 AI 系統、何種資料應避免使用，以確保符合法規要求。

在技能層面上，公務員應具備實際操作 AI 工具之能力，並能將其應用於各類行政情境。例如，在公文處理方面，能運用 AI 協助撰寫草稿、整理條列重點及進行語句優化；在會議管理方面，能利用 AI 整理逐字紀錄、萃取決議事項並形成摘要；在政策作業方面，能協助進行資料彙整、重點分析及簡報架構規劃。公務員亦應具備提示語設計與優化能力，能依據不同任務需求調整指令，使 AI 輸出更精確與符合實務需求。同時，亦須具備檢核與修正 AI 產出內容之能力，包含辨識錯誤資訊、不當語句或不符合政策脈絡之內容，並進行人工補強與調整，使最終成果符合行政品質要求。更進一步，公務員應能將 AI 工具整合至既有工作流程中，形成穩定且可重複使用之作業模式。

在態度層面上，公務員應建立正確之人機協作觀念，理解 AI 僅為輔助工具，其產出結果需經人工判斷與負責，不應直接取代專業決策。同時，應強化風險與責任意識，對於 AI 產出內容保持適度懷疑與檢核，避免因過度依賴而導致行政錯誤。公務員亦應高度重視資訊安全與資料保密原則，對於涉及機密、公務敏感或個人資料之資訊，應採取保守處理方式，避免輸入外部系統。最後，應培養持續學習與適應能力，面對 AI 工具快速演進之趨勢，主動更新知識與技能，並在應用過程中維持公共服務導向，確保 AI 應用不偏離公平性、正確性與公共利益之核心價值。

三、AI 技術模型素養

AI 技術模型素養係指公務員對人工智慧模型之基本原理、技術特性及應用限制之理解能力。此一素養之核心，在於使公務員能從技術層面理解不同 AI 系統之運作邏輯，並據以判斷其適用性與風險，而非僅依賴工具表面功能進行應用。相較於基礎理解與工具操作，此一面向更著重於判斷、比較與選擇，為中階以上人員推動 AI 導入之重要能力基礎。

在知識層面上，公務員應理解人工智慧主要模型之分類與差異，包括辨別式 AI 模型與生成式 AI 模型之基本原理與應用範疇。辨別式 AI 模型多用於分類與預測任務，例如案件審查、風險評估與資料分析；生成式模型則用於內容生成，例如公文撰寫、摘要生成及客服系統。公務員亦應瞭解模型之運作限制，包括訓練資料依賴性、模型錯誤來源及黑箱特性，並認識可解釋性在公共決策中的重要性。

在技能層面上，公務員應能依據業務需求，初步判斷不同 AI 模型之適用情境。例如，能辨識某項任務應採用資料分析模型或生成式工具，並理解其可能產生之風險。公務員應具備辨識模型應用限制之能力，包括判斷模型是否可能產生錯誤結果、是否適用於涉及公民權益之決策，以及是否需要額外之人工覆核機制。同時，亦應能在導入規劃過程中，提供模型選擇與應用方式之初步建議，作為跨部門協作與決策參考。

在態度層面上，公務員應建立對 AI 技術之理性與審慎態度，不將模型結果視為絕對正確之依據，而應視其為輔助判斷之工具。同時，應強化對模型錯誤與不確定性之敏感度，避免在缺乏理解之情況下過度依賴 AI 進行決策。公務員亦應重視模型應用對公共利益與公平性之影響，並培養跨領域整合思維，使技術理

解能與行政業務、政策目標及治理要求相互結合，確保 AI 應用之合理性與正當性。

四、AI 應用案例與場景演練素養

AI 應用案例與場景演練素養係指公務員能透過實際案例理解人工智慧在公共行政中的應用方式，並依據業務需求進行情境判斷與應用設計之能力。此一素養之核心，在於將抽象的 AI 技術轉化為具體行政場景，並透過案例分析與模擬演練，培養公務員在真實情境中正確運用 AI 之能力。

在知識層面上，公務員應瞭解人工智慧於公共部門之典型應用案例，包括行政文書處理、資料分析、民意回應及智慧服務設計等面向，並理解不同應用場景之功能與限制。同時，應認識各類應用情境之風險差異，例如低風險之行政輔助作業與高風險之政策判斷或公民權益相關決策，並掌握 AI 導入之基本流程與應用模式。亦應瞭解國內外政府推動 AI 應用之發展方向，以建立整體應用視野。

在技能層面上，公務員應能依據實務需求，分析業務流程並辨識適合導入 AI 之作業項目，例如文件整理、資料彙整或簡易客服回應等低風險應用。同時，亦應能進行情境分析，判斷 AI 應用之適當性，包括是否需要人工覆核、是否涉及高風險決策，以及是否需配套治理措施。公務員應具備初步規劃 AI 應用之能力，例如設計試點案例、提出應用構想及評估其可能效益與風險，使 AI 應用能逐步落實於行政實務中。

在態度層面上，公務員應建立以問題為導向之應用思維，從實際業務需求出發，合理選擇 AI 應用方式，而非盲目追求技術導入。同時，應強化風險意識，對於涉及政策判斷或公民權益之情境，採取審慎態度並保留人工決策機制。公務員亦應培養跨部門合作與經驗分享之態度，透過案例交流與實務演練，促進 AI 應用知識之擴散與組織學習能力之提升。

五、AI 案例與發展趨勢素養

AI 案例與發展趨勢素養係指公務員能理解國內外人工智慧應用案例及其發展趨勢，並將相關經驗轉化為政策判斷與行政應用參考之能力。此一素養之核心，在於透過觀察與分析不同政府及產業之 AI 實踐經驗，建立宏觀視野，使公務員能在快速變動的科技環境中，掌握 AI 發展方向並進行適切回應。

在知識層面上，公務員應瞭解國際間政府推動 AI 應用之主要模式與政策方向，包括智慧公共服務、資料驅動決策及數位治理轉型等趨勢，並認識 OECD 等

國際組織所提出之 AI 治理原則與發展框架。亦應理解產業界 AI 應用之發展現況，例如智慧製造、金融科技、智慧醫療及智慧城市等領域，並掌握其技術應用模式與發展趨勢。同時，公務員應理解 AI 技術發展對公共治理與國家競爭力之影響，建立整體性認知。

在技能層面上，公務員應能分析國內外 AI 應用案例，並從中萃取可供參考之成功經驗與潛在風險。例如，能比較不同國家在 AI 導入策略、治理機制及應用範圍上的差異，並評估其在本機關或本地情境中之可行性。公務員亦應能判斷產業應用與政府應用之差異，並將發展趨勢轉化為政策規劃或業務推動之參考依據，提升決策品質與前瞻性。

在態度層面上，公務員應建立國際視野與前瞻思維，持續關注 AI 技術與政策發展動態，避免因資訊落差而影響決策判斷。同時，應培養開放學習與跨領域理解之態度，主動吸收產業及國際經驗，並轉化為公共治理之應用知識。公務員亦應強化公共價值導向，確保 AI 應用之發展不僅追求效率與創新，更須符合公平性、正當性與社會信任之原則。

六、 代理人 AI 與流程協作素養

代理人 AI 與流程協作素養係指公務員能理解代理人 AI 之運作邏輯、任務分工方式、工具串接能力與治理需求，並能在公共行政情境中，妥善設計、使用、監督與管理代理人 AI 系統之能力。此一素養之核心，在於使公務員能從單次提示操作，進一步進入跨步驟流程協作與任務自動化思維，並確保代理人 AI 之應用仍維持可控、可監督與可問責之治理原則。

在知識層面上，公務員應理解代理人 AI 與一般生成式 AI 之差異，認識代理人 AI 可透過任務拆解（task decomposition）、工具呼叫（tool calling）及多輪回饋完成較複雜之行政流程。並應瞭解其可能涉及之權限管理、流程紀錄、錯誤傳遞、資安風險與責任歸屬問題，特別是當代理人 AI 連結機關內部系統或跨機關資料來源時，更須明確掌握其治理要求。

在技能層面上，公務員應能辨識適合導入代理人 AI 之行政流程，例如資料蒐整、跨文件摘要、案件初步分流、進度提醒、知識查找及標準流程輔助等低至

中風險任務。並能初步設計代理人 AI 之任務邊界、工具使用範圍、人工覆核點（human-in-the-loop）與例外處理機制，確保其運作符合行政需求。中高階人員亦應能評估代理人 AI 導入之效益、風險與治理需求，作為推動試辦與制度設計之依據。

在態度層面上，公務員應建立「可授權但不可放任」之治理觀念，理解代理人 AI 雖可協助執行流程，但不得取代公務員對重要判斷、裁量與責任之承擔。同時，應重視人機協作、流程透明、紀錄留存與持續監督，使代理人 AI 之應用建立在安全、穩健與公共利益優先之基礎上。

表一：能力指標

向度	能力指標		
	知識	技能	態度
AI 基礎原理與相關風險治理議題	➢ 理解人工智慧基本概念、主要技術類型及生成式 AI 運作原理 ➢ 瞭解資料與模型之關聯性及資料錯誤對結果之影響 ➢ 認識 AI 於公務場域之主要風險類型	➢ 能辨識不同 AI 技術特性並判斷其適用情境 ➢ 能初步進行 AI 應用風險判斷，區分可用與應限制之場景 ➢ 能辨識 AI 產出之錯誤或不可靠資訊並進行修正	➢ 建立審慎使用 AI 之觀念，不盲目依賴 AI 結果 ➢ 強化風險與責任意識，理解最終決策由人負責 ➢ 重視資料安全與公共信任，確保 AI 應用符合治理原則
AI 工具操作	➢ 理解常見 AI 工具類型及其行政應用功能 ➢ 瞭解提示語設計基本原則 ➢ 認識 AI 工具使用之資安與個資保護原則	➢ 能操作 AI 工具完成公文撰寫、簡報設計與資料整理 ➢ 能撰寫有效提示語，引導 AI 產出符合需求內容 ➢ 能辨識並修正 AI 輸出內容之錯誤與不當資訊	➢ 建立人機協作觀念，將 AI 視為輔助工具 ➢ 強化資料保密意識，避免不當輸入敏感資訊 ➢ 培養持續學習與適應新工具之能力
AI 技術模型	➢ 理解辨別式 AI 與生成式 AI 模型之基本原理與差異	➢ 能初步判斷不同 AI 模型之適用業務情境	➢ 建立正確認知，不將 AI 視為絕對正確之工具

	➢ 瞭解不同模型在公共行政中的應用場景與限制 ➢ 認識 AI 模型之黑箱特性與可解釋性問題	➢ 能辨識模型可能產生之錯誤與限制 ➢ 能協助評估模型應用之風險與可行性	➢ 強化批判性思考，理解模型輸出需審慎判讀 ➢ 重視模型應用對公共利益之影響
AI 應用	➢ 瞭解 AI 於各局處常見應用案例與實務情境 ➢ 理解不同應用場景之風險程度差異 ➢ 認識 AI 導入流程與基本應用模式	➢ 能依實務情境設計適合之 AI 應用方式 ➢ 能進行場景分析，判斷 AI 使用之適當性 ➢ 能提出初步 AI 應用規劃或改善建議	➢ 建立問題導向思維，從業務需求出發應用 AI ➢ 強化風險意識，避免不當擴大 AI 使用範圍 ➢ 培養跨部門合作與經驗分享之態度
AI 案例與發展趨勢	➢ 瞭解國際政府 AI 應用發展趨勢與政策方向 ➢ 認識產業 AI 應用模式及跨領域發展趨勢 ➢ 理解 AI 對公共治理與國家競爭力之影響	➢ 能分析國內外 AI 案例並萃取可行策略 ➢ 能判斷產業與政府 AI 應用之差異與連結 ➢ 能將發展趨勢轉化為政策或業務規劃參考	➢ 建立國際視野，關注 AI 發展動態 ➢ 培養前瞻思維，主動思考 AI 導入機會 ➢ 強化公共價值導向，確保科技發展符合社會需求
代理人 AI 與流程協作	➢ 理解代理人 AI 之基本概念、與生成式 AI 之差異及其運作邏輯 ➢ 瞭解任務拆解、工具串接、權限管理與流程紀錄等治理需求 ➢ 認識代理人 AI 在公共行政流程中的應用情境與主要風險	➢ 能辨識適合導入代理人 AI 之行政流程與任務邊界 ➢ 能初步規劃人工覆核點、例外處理機制及工具使用範圍 ➢ 能協助評估代理人 AI 導入之效益、風險與治理需求	➢ 建立可授權但不可放任之治理觀念 ➢ 重視流程透明、紀錄留存與責任可追溯性 ➢ 強化人機協作與公共利益優先之態度

肆、 課程規劃

為有效提升公務員人工智慧素養，本計畫依據第三章所建構之六大 AI 素養

面向，並配合公務體系不同職級之職能需求，規劃分級、模組化之課程體系。透過基層操作應用、中階應用規劃及高階治理決策之分層設計，使 AI 能力培養具備系統性與延續性，逐步建構完整之公務體系 AI 能力架構。本計畫之課程規劃以基礎理解、工具應用、技術判斷、場景演練、趨勢分析及代理人 AI 流程協作為核心模組，並採理論與實務並重之教學方式，結合案例分析、情境模擬與實作演練，以強化學習成效與實務應用能力，同時支援本市人工智慧推動小組推動跨機關 AI 應用、治理規範及能力擴散之重要基礎。

一、 課程架構設計原則

本計畫課程設計依據以下四個原則進行規劃，首先，採分級培訓原則，依據公務員職級區分為基層、中階及高階三個層級，並依其業務職責與決策權限，配置相對應之課程內容。基層以工具操作與基礎應用為主，中階強調應用規劃與風險判斷，高階則聚焦於政策制定與治理決策。其次，採模組化設計原則，將課程內容劃分為六大模組，各模組可依實際需求彈性組合或分階段推動，以利不同機關或單位進行客製化導入。第三，強調實務導向原則，透過行政案例、情境演練及操作練習，使學員能將 AI 應用能力直接轉化至日常業務中，避免流於理論講授。最後，導入風險治理導向原則，於各課程中融入資訊安全、資料保護與責任意識等內容，使 AI 應用與公共治理原則相互結合，以回應本市人工智慧推動小組於 AI 應用發想、導入評估、風險控管及治理決策之任務需求。

另為回應 AI 技術快速由生成式應用進展至代理人協作模式，本計畫亦納入 Human-in-the-loop 原則，強調凡涉及代理人 AI 之課程設計，均須同步納入權限設計、人工覆核、流程紀錄、例外處理與資安控管等內容。

二、 課程模組規劃

本計畫課程依據六大 AI 素養面向，規劃如下六大模組：

1.AI 基礎原理與相關風險治理模組

本模組為所有課程之基礎，主要協助學員建立對人工智慧之正確認知，理解其運作原理與限制。課程內容包括人工智慧基本概念、生成式 AI 運作機制、資料偏誤與模型限制，以及 AI 應用可能產生之風險，如幻覺、資訊錯誤與問責問題。同時，亦納入資訊安全與個資保護等相關規範。本模組之目標在於使學員能理解 AI 之本質，並具備基本風險辨識能力，作為後續應用之基礎。

2.AI 工具應用模組

本模組著重於 AI 工具在行政實務中的應用，協助學員提升日常工作效率。課程內容涵蓋 AI 平台操作、提示語設計技巧，以及 AI 於公文撰寫、會議紀錄整理、政策摘要及簡報製作等應用。並透過實作演練，使學員熟悉工具操作與應用方式。此外，本模組亦強調安全使用原則，避免機敏資料外洩，並培養學員對 AI 輸出內容進行檢核與修正之能力。

3.AI 模型模組

本模組主要針對中階以上人員設計，協助其理解 AI 技術模型之特性與差異。

課程內容包括辨別式 AI 與生成式 AI 模型之基本原理、應用場景與限制，以及模型之可解釋性與黑箱問題。透過案例說明，使學員能理解不同模型之適用情境。本模組之目的在於培養學員之技術判斷能力，使其在規劃 AI 導入時，能進行適當之模型選擇與風險評估。

4.AI 應用案例與場景演練模組

本模組透過實際案例與情境模擬，培養學員將 AI 應用於行政實務之能力。課程內容包括各局處實際應用案例分析，以及不同情境之應用判斷演練，例如行政文書處理、資料分析及民眾服務等場景。並透過分組討論與案例分析，使學員能理解 AI 應用之可行性與風險。本模組之核心在於強化學員之實務判斷能力，使其能在真實情境中正確運用 AI。

5. 政府與產業 AI 案例與發展趨勢模組

本模組著重於建立學員之宏觀視野，使其理解 AI 發展趨勢與政策方向。課程內容涵蓋國際政府 AI 應用案例、OECD 治理框架及產業 AI 發展趨勢，如智慧製造、金融科技及智慧城市等領域。透過案例分析，使學員能掌握 AI 發展脈動。本模組之目的在於提升學員之政策敏感度與前瞻思維，使 AI 應用能與國際趨勢接軌。

6.代理人 AI 與流程協作模組

本模組旨在協助學員理解代理人 AI 於公共行政中的應用模式與治理要求。課程內容包括代理人 AI 之基本概念、任務拆解與工具串接邏輯、行政流程中的應用情境、人工覆核與權限控管設計、流程紀錄與責任追溯機制，以及代理人 AI 試辦之規劃方法。透過案例分析與模擬演練，使學員能判斷哪些行政流程適合導

入代理人 AI、如何設定其任務邊界與監督節點，並建立可控、可審核、可逐步擴充之導入模式。

三、 分級課程配置

1. 基層公務員課程規劃

向度	課程
AI 基礎原理與相關風險治理議題	AI 原理(必修)(3 小時) AI 平台應用(必修)(3 小時)
AI 工具操作	AI 與公文報告的應用(3 小時) AI 與簡報設計(3 小時)
AI 模型	大語言模型與聊天機器人(3 小時) 代理人 AI 入門與行政協作(3 小時)
AI 應用與場景演練	AI 應用案例(各局處)(3 小時)
AI 案例與發展趨勢	政府 AI 應用趨勢與代理人 AI 案例(3 小時)

2. 中階公務員課程規劃

向度	課程
AI 基礎原理與相關風險治理議題	AI 原理(必修)(3 小時) AI 平台應用(必修)(3 小時)
AI 工具操作	AI 與數據分析(3 小時)
AI 技術模型	辨別式 AI 模型與公務應用(6 小時) 生成式 AI 模型與公務應用(6 小時)
AI 應用與場景演練	AI 應用案例(各局處)(3 小時) 代理人 AI 流程設計與試辦演練(3 小時)
AI 案例與發展趨勢	AI 政府發展趨勢(國外專家)(3 小時) 產業 AI 發展趨勢(3 小時) 代理人 AI 治理與導入案例(3 小時)

3. 高階公務員課程規劃

向度	課程
AI 基礎原理與相關風險治理議題	AI 原理(必修)(3 小時) AI 平台應用(必修)(3 小時)
AI 工具操作	代理人 AI 應用策略與導入原則(3 小時)
AI 技術模型	AI 政策與決策框架(3 小時) 代理人 AI 決策支援與風險控管(3 小時)

AI 應用與場景演練	跨局處代理人 AI 試辦案例研討(3 小時)
AI 案例與發展趨勢	AI 政府發展趨勢(國外專家)(3 小時) 產業 AI 發展趨勢(3 小時) AI 政策與治理框架(3 小時) AI 制度建構與組織變革(3 小時) 代理人 AI 治理與組織轉型(3 小時)

伍、 未來展望

隨著人工智慧技術持續演進，其對政府治理模式、公共服務提供方式及政策決策機制之影響將日益深化。未來，AI 不僅將成為提升行政效率之工具，更將逐步轉化為政府進行智慧治理與政策創新的核心基礎設施。因此，公務員 AI 素養之培養，應由短期訓練逐步轉化為長期制度建構，並持續滾動調整與精進。本計畫推動後，預期將分短、中、長期不同階段逐步發展，形成具體成效與長期制度化成果。尤其當 AI 由內容生成進一步走向可執行流程之代理人 AI 時，政府更需及早建立相應之人才能力與治理制度。

一、短期展望

於短期階段，本計畫將以建立基礎 AI 素養為核心目標，優先推動基層與中階公務員之培訓，使公務體系普遍具備基本 AI 理解與應用能力。透過系統化課程推動，預期可達成以下成果。第一，提升公務員對 AI 之正確認知，降低誤用與過度依賴之風險；第二，透過 AI 工具應用，有效減少行政文書處理時間，提升作業效率；第三，建立基本風險意識，使公務員能辨識 AI 應用之適用範圍與限制。短期內亦可透過案例蒐集與實務分享，累積初步應用經驗，為後續擴散與制度建構奠定基礎。短期亦可先選定低風險行政流程，進行代理人 AI 應用示範，例如會議資料整備、知識查找與標準表單輔助，以建立導入經驗，並參考本市人工智慧推動小組相關示範案例及經驗回饋，作為後續課程規劃之基礎。

二、中期展望

於中期階段，本計畫將進一步推展至應用導入與制度雛形建立。在本市人工智慧推動小組政策引領下，各機關可依業務特性，逐步推動 AI 應用試點計畫，並透過跨部門合作，建立共享之應用經驗與推動模式。在此階段，預期可達成以下目標。第一，形成具代表性之 AI 應用案例，涵蓋行政效率提升、資料分析及民眾服務等面向；第二，建立 AI 應用評估機制，包括風險分級、成效指標及導

入流程標準化；第三，促進跨機關協作，逐步形成整體推動架構。同時，亦將逐步建立內部 AI 治理雛形，包括資料使用規範、風險控管機制及基本責任制度，使 AI 應用由零星嘗試轉為有系統之推動模式。在此階段，亦可推動代理人 AI 試辦機制，建立跨局處協作流程、權限分級、人工覆核節點及成效評估模式。

三、長期展望

於長期階段，本計畫將朝向公務員具備制度化與治理深化能力，建立完整之公務體系 AI 治理架構，使 AI 應用能穩定融入政府運作。預期發展方向包括具備建立機關層級之 AI 使用規範與治理制度，明確界定不同應用情境之風險分級與責任歸屬之能力。其次公務員具備完善 AI 採購與合規制度能力，確保外部系統符合資訊安全與法規要求。長期亦將推動 AI 應用與政策制定之整合，使 AI 成為支援政策分析與決策之重要工具，進一步提升政府治理能力。並進一步建立代理人 AI 之採購、驗證、監理與稽核制度，確保其在公共行政中之長期應用具備合法性、穩定性與可問責性。

四、未來願景

綜言之，本計畫之最終目標，在於建構公務員具備 AI 應用能力與治理能力之現代公務體系，使人工智慧技術能在確保風險可控與責任明確之情況下，發揮其最大效益。未來公務體系之 AI 發展，將朝向建立全體公務員之基本 AI 素養與代理人 AI 協作能力，使 AI 應用成為日常行政之常態。強化中階公務員應用規劃能力，促進 AI 導入之制度化與規模化並提升高階決策者之治理能力，確保 AI 應用符合公共利益與社會期待。透過本計畫之推動，期待逐步實現以 AI 為基礎之智慧治理模式，提升政府行政效能、政策品質與公共服務水準，並強化政府之透明性、信任度與國際競爭力。未來亦應逐步形成臺北市政府在代理人 AI 應用與治理上的示範模式，作為智慧城市治理升級之重要基礎。