

保障個人資料人工智能沙盒

框架

目標

2023 年 10 月，中國內地發布《全球人工智能治理倡議》，提倡「發展人工智能應堅持『以人為本』理念，以增進人類共同福祉為目標，以保障社會安全、尊重人類權益為前提，確保人工智能始終朝着有利於人類文明進步的方向發展」，並堅持發展和安全並重的原則。

2025 年 2 月舉行的巴黎人工智能行動峰會上，包括中國在內逾 60 個國家及其他國際組織就「為人類和世界而設具包容性及可持續的人工智能」發表聯合聲明，其中包括呼籲機構採取能「讓人工智能以人權為依歸，以人為本、合乎道德、安全、可靠及值得信賴」的策略。

2024 年 6 月，個人資料私隱專員公署（「私隱專員公署」）發布《人工智能（AI）：個人資料保障模範框架》（「《模範框架》」），提供國際認可及切實可行的建議和最佳行事常規，以協助機構在採購、實施及使用人工智能（「AI」），包括生成式 AI 時，遵從《個人資料（私隱）條例》（「《私隱條例》」）的相關規定。《模範框架》旨在協助機構在善用 AI 之餘，保障個人資料私隱。2025 年 3 月，私隱專員公署亦發布《僱員使用生成式 AI 的指引清單》（「《生成式 AI 指引清單》」），以協助機構制定僱員在工作時使用生成式 AI 的內部政策或指引，及遵從《私隱條例》的規定。

數字政策辦公室（「數字辦」）制定了《人工智能道德框架》，為機構就 AI 技術開發及應用項目提供指導，使其能夠識別及管理與 AI 應用項目有關

的潛在風險及相關事宜。數字辦亦發布《香港生成式人工智能技術及應用指引》(《數字辦指引》)，為 AI 生態圈中各持份者建構一套符合香港情境、具本地特色的治理框架，平衡 AI 的創新發展、應用與責任。

為積極主動對接國家「十五五」規劃堅持統籌發展和安全的指導方針，並支持行政長官 2025 年施政報告中推進香港的 AI+發展的政策，私隱專員公署及數字辦合作推出「保障個人資料人工智能沙盒」(「沙盒」) 計劃，並獲得香港數碼港(「數碼港」)、香港生產力促進局(「生產力局」、資訊科技教育領袖協會以及香港電腦教育學會擔任支持機構。沙盒旨在協助參與學校(「參加者」)在營運中安全及負責任地採用 AI 方案，遵從《私隱條例》的相關規定，同時採取適當及足夠的保安措施。計劃為參加者、AI 方案供應商、私隱專員公署、數字辦、數碼港及生產力局提供一個協作平台，冀在促進創新的同時，協助參加者遵守《私隱條例》，並負責任地採用 AI 科技。沙盒將聚焦於教育界的 AI 科技應用，並支援學校探索和採用 AI 方案。

具體而言，沙盒旨在：

- 在推廣創新的同時確保學校負責任及安全地使用 AI：鼓勵在尊重私隱並堅守 AI 道德的前提下，以有利學校及教育界的方式採用 AI 科技；
- 展現 AI 的潛力：展示 AI 能如何為學校優化營運、提升效率並推動創新之餘，促進保障個人資料私隱和遵從《私隱條例》，包括六項保障資料原則；
- 推動協作：營造互相支持的環境，讓參加者及 AI 方案供應商可以分享專業知識並參與協作；及

- **加強機構對監管的理解**：讓參加者更充分理解《私隱條例》的相關規定，以促使其在使用 AI 時遵從該等規定，同時讓私隱專員公署及數字辦更深入地了解不同參加者如何採用和實施 AI。

一般原則

➤ **監管及技術指引**

在參與沙盒的整段期間，私隱專員公署、數字辦、數碼港及生產力局將擔當中立的促進角色，就任何可能會及實際上實施的 AI 方案提供監管或技術指引及／或最佳行事常規的建議。當中，私隱專員公署的指引是在不影響私隱專員公署日後可能根據《私隱條例》作出的任何決定或行動（包括任何執法行動）的情況下提供。

沙盒同時充當平台，讓參加者及 AI 方案供應商可以互相聯繫，並探索有關實施 AI 方案的潛在合夥及協作機會。

➤ **遵從《私隱條例》**

雖然私隱專員公署會就遵守《私隱條例》提供指引，但沙盒的參加者仍須對其是否符合所有適用法律及監管規定（包括但不限於《私隱條例》）負責。參加者獲選參與沙盒並不表示私隱專員公署或數字辦認可由參加者提議的 AI 方案的任何部分或其實際運作。

➤ **沙盒持續期**

沙盒以先導計劃形式推出，首階段為期 6 個月，經私隱專員公署及數字辦批准後可續期 6 個月，私隱專員公署及數字辦對評估參加者的續期申請有絕對酌情權。

➤ 使用場景

沙盒主要為可供使用於教與學的現成 AI 方案的實際應用而設，沙盒並不適用於開發中方案的試驗。

申請者應在申請表上表明其擬採用 AI 方案的範疇及/或種類。以下提供可能涉及處理個人資料的使用場景以作說明，並不涵蓋所有情況：

- 聊天機械人；
- 個人化及自適應學習；
- 寫作及創作內容；
- 管理及處理文件；
- 數據分析及預測；
- 資訊圖表、音訊及影片製作；及
- 行政自動化。

➤ 費用

申請參加沙盒毋須繳付任何費用。私隱專員公署會提供監管指引及研討會名額，而數碼港及生產力局則會向參加者提供技術諮詢服務，費用全免。然而，參加者須自行負責及承擔因參加沙盒而產生的或與之相關的成本，包括但不限於準備申請及實施 AI 方案的成本。

私隱專員公署、數字辦、數碼港或生產力局均不會就參加者因參加沙盒而產生的或與之相關的任何財務風險或債務承擔任何責任。參加者在沙盒內的運作獨立於私隱專員公署、數字辦、數碼港及生產力局，而所有相關風險及責任均由參加者獨自承擔。

益處

沙盒可向參加者提供眾多益處，包括：

- **與不同供應商接觸**：透過在有效運用 AI 方面具備良好服務紀錄的供應商所提供的 AI 服務方案，推動貴校進行改革。
- **監管方面的意見**：受惠於私隱專員公署就遵守《私隱條例》而提供的監管指引，以及私隱專員公署及數字辦發布的 AI 相關指引資料中建議的最佳行事常規。
- **參與私隱專員公署提供的活動**：獲得免費名額參加由香港國際數據私隱學院舉辦，有關 AI 及數據安全的講座，並有機會與私隱專員公署就保障數據的議題互動交流。
- **獲得數碼港及生產力局的技術諮詢服務**：就實施 AI 方案獲得數碼港及生產力局提供的技術意見支援。
- **協作學習**：以誠信及合規為核心促進創新，並與其他學校分享以尊重個人資料私隱的方式採用 AI 的最佳行事常規。

申請資格

沙盒接受根據《教育條例》（《香港法例》第 279 章）註冊並獲公帑資助的小學及中學申請。私隱專員公署及數字辦保留在諮詢由私隱專員公署及數字辦的代表、外部專家及資訊科技界成員組成的遴選委員會（「**遴選委員會**」）後，選擇申請者的絕對權利。

評審準則

私隱專員公署及數字辦經諮詢遴選委員會後，將選出合共 15 位申請者。評審將會按下列因素（並非所有因素）把合資格申請者列入候選名單：

- 對實施 AI 是否準備就緒；

- 是否致力保障個人資料私隱並達致穩健的 AI 治理；
- 對為受眾提供切實可行及可持續的應用方案，顯示出實在潛力；及
- 對採用 AI 會令申請者及教育界均受惠，並有助解決學校面對的共通挑戰，顯示出實在潛力。

除上列因素外，私隱專員公署及數字辦可為達致 AI 使用場景多樣化而選擇申請者。

申請及遴選過程

➤ 接受申請

申請沙盒的截止日期為 **2026 年 10 月 30 日**。

➤ 申請表格

申請人必須透過 <https://eform.cefs.gov.hk/form/dpo034/tc/> 填妥網上申請表格。

➤ 簡介會

私隱專員公署及數字辦將於 **2026 年 8 月 28 日** 舉辦簡介會，為有意參加的學校簡介沙盒，包括其目標、範圍、申請要求及評審準則。簡介會的詳情將適時公布。

➤ 結果公布

獲選申請者將於申請限期屆滿後三個月內獲通知結果。落選申請者可能會被列入候補名單，以供日後考慮。私隱專員公署及數字辦的決定為最終及絕對決定。

沙盒的運作

➤ 啟動會議

為促進各方之間的溝通、傳達關鍵資訊並啟動合作夥伴關係的建立過程，獲選參加者將獲邀參與一場啟動會議。會議將介紹沙盒的相關詳情，包括其架構、運作預期與時間表，以及支援配套的實務安排等。該會議將匯聚獲選參加者、私隱專員公署、數字辦、數碼港及生產力局，並同時標誌為期六個月的沙盒正式開展。

➤ 私隱專員公署提供的監管指引

在獲選參加者考慮建立合夥關係及實施 AI 方案的可能性時，私隱專員公署可按要求提供監管指引，監管指引以《私隱條例》、《模範框架》、《生成式 AI 指引清單》及私隱專員公署不時可能發布的任何其他 AI 相關指引為依據。私隱專員公署可：

- 就實施 AI 方案，提供從《私隱條例》角度出發的觀察，尤其聚焦於六項保障資料原則。六項保障資料原則涵蓋由收集、保留、使用以至銷毀個人資料的整個處理周期；
- 按獲選參加者的需要，就保障資料最佳行事常規提供指引；
- 就參加者是否符合《模範框架》提供所需指引，涵蓋以下四個範疇：
(i) 制定 AI 策略及管治架構；(ii) 進行風險評估及人為監督；(iii) 實行 AI 模型的定製與 AI 系統的實施及管理；及 (iv) 促進與持份者的溝通及交流；及
- 就參加者是否符合《生成式 AI 指引清單》提供所需指引，涵蓋其內部生成式 AI 政策或指引中應包含的五個重點，包括 (i) 獲准使用生成式 AI 的範圍；(ii) 保障個人資料私隱；(iii) 合法及合乎道德的使用及預防偏見；(iv) 數據安全；及 (v) 違反政策或指引可能帶來的後果。

私隱專員公署將按要求在有需要的情況下，在為期 6 個月期間，向參加者提供**三輪監管指引**，指引將從《私隱條例》角度出發。指引可以面對面會面或書面形式提供，私隱專員公署對指引的提供方式有絕對酌情權。

此外，私隱專員公署將會向每位參加者提供**五個免費名額**¹，參加由香港國際數據私隱學院主辦的資料保障講座，包括專為使用 AI 而設的講座。

➤ 數字辦的指引

在獲選參加者考慮建立合夥關係及潛在採用 AI 方案進行探索時，數字辦可應要求根據《數字辦指引》及不時由其發布的其他相關 AI 指引文件提供指引。數字辦可：

- 就參加者在遵循《數字辦指引》方面提供適切指引，涵蓋針對生成式 AI 的技術開發者、服務提供者及服務使用者的實務指引。

指引可以面對面會面或以書面形式提供，數字辦對指引的提供方式有絕對酌情權。

請注意，任何有關 AI 方案的技術層面的查詢，應向相關供應商或獨立技術專家（包括數碼港及生產力局）提出。

➤ 期滿報告

為期 6 個月完結後，不論任何合夥進度如何，每名參加者均須提交期滿報告，報告內容應涵蓋但不限於在沙盒下實施 AI 方案的進度及成果（如有）、參加者在保障個人資料私隱方面所面對的挑戰、參加者對私隱專員公署所提供的指引的回饋，及參加者對沙盒的一般意見及／或評估。

¹ 一個名額僅供一位參加者的一名代表出席一場研討會。

➤ 項目分享會

參加者可能會獲邀在該 6 個月完結後，於私隱專員公署及數字辦舉辦的分享會上，分享其在探索和採用 AI 方案的整個過程中的經驗，並交流見解。分享會將為參加者提供寶貴平台，讓其分享所得的實務經驗及創新方法，維持開放的對話及協作，從而有助在採用 AI 方面達成具意義的成果。

查詢

如有查詢，請以電郵（AIsandbox@pcpd.org.hk）或致電 2827 2827 聯絡私隱專員公署的沙盒小組。

免責聲明

私隱專員公署或數字辦均不會成為參加者及 AI 方案供應商之間的任何商業談判、業務往來、商業交易或協議的一方，或涉及其中任何部分。任何因上文所提及的活動而產生的或與之相關的合夥、協議或債務的責任均由參加者獨自承擔。私隱專員公署或數字辦均不會認可任何供應商或其方案。私隱專員公署及數字辦並不保證供應商所提供的資料的準確性。

私隱專員公署及數字辦均不會就因參加沙盒而產生的或與之相關的，或任何因參加沙盒而作出的任何行動或決定而導致的任何後果、糾紛、損害或損失（包括但不限於業務虧損或利潤虧損所造成的損害）承擔法律責任。

私隱專員公署向參加者提供的監管指引屬一般性觀察，並在不影響私隱專員公署日後可能根據《私隱條例》作出的任何決定或行動（包括任何監管或執法行動）的情況下提供。參加者可按意願自行尋求獨立法律意見。

--- 完 ---