Safeguarding Personal Data AI Sandbox

Framework

Objectives

In October 2023, the Chinese Mainland issued the "Global AI Governance Initiative", which advocates *"a people-centred approach in developing AI, with the goal of increasing the wellbeing of humanity and on the premise of ensuring social security and respecting the rights and interests of humanity, so that AI always develops in a way that is beneficial to human civilisation"* and puts equal emphasis on development and security.

At the Paris Artificial Intelligence Action Summit in February 2025, over 60 countries, including China, and other international bodies published a joint statement on "Inclusive and Sustainable Artificial Intelligence for People and the Planet" which, among other things, calls for an approach that will *"enable AI to be human rights based, human-centric, ethical, safe, secure and trustworthy".*

The Office of the Privacy Commissioner for Personal Data ("PCPD") published the "Artificial Intelligence: Model Personal Data Protection Framework" ("Model Framework") in June 2024, to provide internationally well-recognised and practical recommendations and best practices to assist organisations in procuring, implementing and using artificial intelligence ("AI"), including generative AI ("GenAI"), in compliance with the relevant requirements of the Personal Data (Privacy) Ordinance ("PDPO"). The Model Framework seeks to facilitate organisations to harness the benefits of AI while safeguarding personal data privacy. In March 2025, the PCPD also published "Checklist on Guidelines for the Use of Generative AI by

Employees" ("GenAI Checklist Guidelines") to assist organisations in developing internal policies or guidelines on the use of GenAI by employees at work while complying with the requirements of the PDPO.

The Digital Policy Office ("DPO") has formulated the Ethical AI Framework to provide guideline to organisations on AI technology development and application projects, enabling them to identify and manage potential risks and matters of concern associated with AI application projects. The DPO has also issued the Hong Kong Generative Artificial Intelligence Technical and Application Guideline ("DPO Guideline") to establish a governance framework with local characteristics that is suitable for the Hong Kong context for all stakeholders in the AI ecosystem, with a view to balancing AI innovation development, application, and responsibility.

In active alignment with the guiding principle of ensuring both development and security under the National 15th Five-Year Plan, and to support the policy to develop AI+ in Hong Kong as set out in the Chief Executive's 2025 Policy Address, the PCPD and the DPO jointly launch the Safeguarding Personal Data AI Sandbox ("Sandbox"), with Hong Kong Cyberport ("Cyberport"), the Hong Kong Productivity Council ("HKPC"), the Association of I.T. Leaders in Education ("AiTLE") and the Hong Kong Association for Computer Education ("HKACE") acting as supporting organisations. The Sandbox aims to assist participating schools in adopting AI solutions ("Participants") in their operations in a safe and responsible manner, in compliance with the relevant requirements of the PDPO while adopting appropriate and adequate security measures. The programme provides a collaborative platform for Participants, AI solution suppliers, the PCPD, the DPO, the Cyberport and the HKPC, with a view to fostering innovation while facilitating compliance with the PDPO and promoting the

responsible adoption of AI technologies. The Sandbox will focus on the use of AI technologies in the education sector and support schools in exploring and adopting AI solutions.

Specifically, the Sandbox aims to:

- **Promote innovation while ensuring responsible and safe use of AI**: Encourage the adoption of AI technologies in ways that benefit schools and the education sector, and in a privacy-respecting manner that upholds AI ethics;
- **Showcase the potential of AI**: Demonstrate how AI can enhance operations, drive efficiency, and foster innovation for schools, while facilitating the protection of personal data privacy and compliance with the PDPO, including the six Data Protection Principles;
- **Foster collaboration:** Create a supportive environment where the Participants and AI solution suppliers can share expertise and engage in collaboration; and
- **Enhance regulatory understanding**: Enable the Participants to better understand the relevant requirements of the PDPO to facilitate compliance thereof when using AI, while allowing the PCPD and the DPO to gain deeper insights into the adoption and implementation of AI by different Participants.

General Propositions

➢ Regulatory and technical guidance

Throughout the participation in the Sandbox, the PCPD, the DPO, the Cyberport and the HKPC will act as neutral facilitators to provide regulatory or technical guidance and/or recommendations on best practices in potential and actual implementation of AI solutions. The guidance from the PCPD is given without

prejudice to any decision or action that the PCPD may take in the future, including any enforcement action, pursuant to the PDPO.

The Sandbox will also serve as a platform for the Participants and AI solution suppliers to connect and explore potential partnerships and collaboration on the implementation of AI solutions.

- **Adherence to the PDPO**

While the PCPD would provide guidance on compliance with the PDPO, the Participants in the Sandbox shall remain responsible for their compliance with all applicable legal and regulatory requirements, including but not limited to the PDPO. Admission to the Sandbox does not represent endorsement by the PCPD or the DPO on any part(s) of the AI solutions proposed by the Participants or on their actual implementation.

- **Duration**

The Sandbox is launched as a pilot project. The first phase of the Sandbox will be 6 months, with the possibility of renewal for another 6 months subject to the approval of the PCPD and the DPO, which shall have absolute discretion in assessing the application for renewal by the Participants.

- **Use cases**

The Sandbox focuses on practical applications of readily available AI solutions for teaching and learning, rather than being a testing ground for solutions still under development.

Applicants should indicate in the application form the area(s) and/or the type(s) of intended usage they are interested in pursuing. Non-exhaustive examples of

use cases that may involve the handling of personal data are provided below as illustration:

- Chatbots;
- Personalised and adaptive learning;
- Writing and content creation;
- Document management and processing;
- Data analysis and prediction;
- Infographic, audio and video creation; and
- Administrative automation.

➢ **Fees**

Application to participate in the Sandbox is free of charge. The PCPD will offer regulatory guidance and provide seminar quotas, whereas the Cyberport and the HKPC will provide technical enquiry services to the Participants at no cost. However, the Participants shall be solely responsible for and bear their own costs arising from or in connection with their participation in the Sandbox, including but not limited to the preparation of application and the implementation of the AI solution.

Neither the PCPD, the DPO, the Cyberport nor the HKPC undertake any responsibility for any financial risk or liability on the part of the Participants arising out of or in connection with their participation in the Sandbox. Participants shall operate independently of the PCPD, the DPO, the Cyberport and the HKPC within the Sandbox and all such risks and liabilities shall be borne solely by the Participants.

Benefits

The Sandbox offers the Participants with the opportunity to gain a diverse array of benefits:

- ***Access to suppliers****:* Drive transformation across your school with AI solutions delivered by suppliers with a proven track record in the deployment of AI services.
- ***Regulatory insights****:* Benefit from the PCPD's regulatory guidance on compliance with the PDPO together with the best practices recommended in the AI-related guidance materials published by the PCPD and the DPO.
- ***Access to resources from the PCPD****:* Enjoy access to complimentary quotas for attending seminars on AI and data security organised by the Hong Kong International Data Privacy Academy, alongside opportunities to engage with the PCPD on data protection issues.
- ***Access to technical enquiry services from the Cyberport and the HKPC****:* Receive technical advisory support from the Cyberport and the HKPC on the implementation of AI solutions.
- ***Collaborative learning****:* Enable innovation with integrity and compliance at its core with a view to sharing with other schools best practices in AI adoption that respect personal data privacy.

Eligibility Criteria

The Sandbox is open for application from publicly-funded primary and secondary schools registered under the Education Ordinance (Cap. 279 of the Laws of Hong Kong). The PCPD and the DPO reserve the absolute right to select applicants after consulting a selection committee comprising officers of the PCPD and the DPO, external experts and members from the IT sector ("**Selection Committee**").

Evaluation Criteria

A total of 15 applicants will be selected by the PCPD and the DPO in consultation with the Selection Committee. Eligible applicants may be shortlisted based on the following non-exhaustive factors:

- Readiness to implement AI;
- Commitment to personal data privacy protection and sound AI governance;
- Demonstration of strong potential for a viable and sustainable application that is suitable for beneficiaries; and
- Demonstration of strong potential that adopting AI can benefit both the applicant and the education sector as well as resolve common challenges across schools.

In addition to the factors listed above, the PCPD and the DPO may select the applicants with a view to achieving a diverse spectrum of AI use cases.

Application and Selection Process

➢ Call for applications

The Sandbox is open for applications until **30 October 2026**.

➢ Application form

Applicants must complete the online application form at https://eform.cefs.gov.hk/form/dpo034/en/.

➢ Briefing session

A briefing session will be held on **28 August 2026** to provide an overview of the Sandbox, including its objectives, scope, application requirements and evaluation criteria, for interested schools. Details of the briefing session will be announced in due course.

➢ **Result announcement**

Successful applicants will be informed of the result within three months from the application deadline. Unsuccessful applicants may be placed on a waiting list for future consideration. The decisions of the PCPD and the DPO shall be final and absolute.

Sandbox Operation

➢ **Onboarding meeting**

To facilitate communications among all parties, convey key information and kick-start the partnership formation process, selected Participants will be invited to an onboarding meeting wherein details of the Sandbox such as the structure of the Sandbox, operational expectations and the timeline, practical logistics on access to support, etc will be discussed. The meeting will bring together the selected Participants, the PCPD, the DPO, Cyberport and the HKPC. It also serves as the commencement of the 6-month Sandbox period.

➢ **Regulatory guidance by the PCPD**

As the selected Participants explore partnership formation and possible implementation of AI solutions, the PCPD may, upon request, provide regulatory guidance based on the PDPO, the Model Framework, the GenAI Checklist Guidelines and any other relevant AI-related guidance materials that may be issued from the PCPD from time to time. The PCPD may offer:

- **Observations from the perspective of the PDPO in relation to the implementation of AI solutions**, with particular regard to the six Data Protection Principles covering the entire personal data handling cycle from collection, retention, use to destruction;
- **Guidance on best practices** for data protection tailored to the needs of the selected Participants;

- **Guidance on the Participants' adherence to the Model Framework**, as appropriate, covering the four areas of (i) Establishing AI Strategy and Governance; (ii) Conducting Risk Assessment and Human Oversight; (iii) Customisation of AI Models and Implementation and Management of AI Systems; and (iv) Communication and Engagement with Stakeholders; and
- **Guidance on Participants' adherence to the GenAI Checklist Guidelines**, as appropriate, covering the five key aspects to be covered in their internal GenAI policies or guidelines, including (i) Scope of permissible use of GenAI; (ii) Protection of personal data privacy; (iii) Lawful and ethical use and prevention of bias; (iv) Data security; and (v) Possible consequences of violation of policies or guidelines.

The PCPD will offer, where necessary and upon request, **three rounds of regulatory guidance** from the perspective of the PDPO to the Participants during the six-month period. Guidance may be provided through face-to-face meetings or written communication at the absolute discretion of the PCPD.

In addition, the PCPD will provide **five complimentary quotas [1] for the Participants to join the data protection seminars of the Hong Kong International Data Privacy Academy**, including those specifically tailored for AI use.

➢ **Guidance by the DPO**

As the selected Participants explore partnership formation and potential implementation of AI solutions, the DPO may, upon request, provide guidance based on the DPO Guideline and any other relevant AI-related guidance materials that may be issued by the DPO from time to time. The DPO may offer:

[1] One quota entitles one representative of a Participant to one seminar.

- **Guidance on the Participants' adherence to the DPO Guideline**, as appropriate, covering the Practical Guidelines for Technology Developers, Service Providers, and Service Users of Generative AI.

Guidance may be provided through face-to-face meetings or written communication at the absolute discretion of the DPO.

It should be noted that any enquiries relating to the technical aspect of AI solutions should be directed to the supplier(s) or independent technical experts including the Cyberport and the HKPC.

➢ **Completion report**

At the end of the 6-month period, regardless of the progress of any partnership, each Participant is required to submit a completion report which covers, amongst others, the progress and achievements (if any) from the implementation of the AI Solutions under the Sandbox; challenges they face in terms of personal data privacy protection; their feedback on the guidance provided by the PCPD; and their general comments and/or evaluation on the Sandbox.

➢ **Projects sharing session**

Participants may be invited to share their experience and exchange insights encountered throughout the journey of exploring and adopting AI solutions in a sharing session to be organised by the PCPD and the DPO after the end of the 6-month period. It will provide a valuable platform for the Participants to share the practical lessons and innovative approaches learnt, maintain open dialogue and collaboration, which will be conducive to driving meaningful outcomes in the adoption of AI.

Enquiries

Enquiries can be made to the PCPD's Sandbox Team at AIsandbox@pcpd.org.hk and 2827 2827.

Disclaimer

Neither the PCPD nor the DPO will be a party to or involved in any part of any commercial negotiation, business dealing, commercial transaction or agreement between the Participants and AI solution suppliers. Any partnership, agreement or liability arising from or in connection with the foregoing is solely the responsibilities of the Participants. Neither the PCPD nor the DPO endorses any supplier or its solution. The PCPD and the DPO do not guarantee the accuracy of the information provided by the suppliers.

The PCPD and the DPO will not be liable for any outcome, dispute, damage or loss (including but not limited to, damages for loss of business or loss of profits) howsoever arising from or in connection with the participation in the Sandbox or from any action or decision taken as a result of the participation in the Sandbox.

The PCPD's regulatory guidance provided to the Participants in the form of general observations is given without prejudice to any decision or action that the PCPD may take in the future, including any regulatory or enforcement action, pursuant to the PDPO. Participants are at liberty to seek their own independent legal advice.

--- End ---