Checklist on Guidelines for the Use of Generative AI by Employees

PCPD
H K

PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Introduction

In light of the rapid development of generative artificial intelligence (Gen AI), the Office of the Privacy Commissioner for Personal Data (PCPD) has formulated this checklist. The checklist aims to help organisations develop internal policies or guidelines for the use of Gen AI by employees at work while complying with the requirements of the Personal Data (Privacy) Ordinance in relation to the handling of personal data, with a view to facilitating the safe and healthy development of artificial intelligence (AI) in Hong Kong. As a matter of good practice, organisations should devise their own policies or guidelines in alignment with their values and mission and should regularly review and update the relevant policies or guidelines as required to accommodate operational and technical changes.

In this checklist, "information" mainly refers to personal data, but it may also refer to general information or data, depending on the nature of the information processed by and the needs of the organisation in question.

Examples of Gen AI Tools

Organisations in Hong Kong commonly use Gen AI tools such as:

- Chatbots;
- Optical character recognition;
- Text/image/video/voice generators;
- Document/presentation generators; and
- Speech-to-text tools, etc.

Employees' access to these Gen AI tools differs depending on how they are utilised by organisations. For example, these tools can be installed and run on employees' computers (with or without an Internet connection), hosted on the organisation's servers (e.g., intranets), accessed via an application programme interface or via the Internet (e.g., web-based tools).

Recommended Coverage of Policies or Guidelines on the Use of Gen AI by Employees

Scope

☑ **Permitted tools:** Clearly specify the Gen AI tools and applications that are permitted within the organisation. These may include:

- Publicly available Gen AI tools or applications; and/or
- Internally developed Gen AI tools or applications.

Data Protection Tip💡: For publicly available Gen AI tools or applications, commercially licensed versions may offer more personal data privacy and security safeguards. For internally developed Gen AI tools, hosting the tools within the organisations' own premises generally allows for greater control over data security (e.g., requiring the input and output data to remain on employees' devices or on the organisations' servers) than hosting on a third-party cloud. However, the organisations should assess whether they have the necessary expertise and resources to securely operate and protect an on-premises system.

☑ **Permissible use:** Clearly specify the tasks or activities for which employees can use Gen AI tools, for example:

- Drafting;
- Summarising information; and/or
- Creating textual, audio and/or visual content.

☑ **Policy applicability:** Specify if the policy applies to:

- The whole organisation;
- Specific departments;
- Specific ranks; and/or
- Specific employees.

Protection of Personal Data Privacy

☑ **Permissible types and amounts of input information:** Provide clear instructions on the types and amounts of information that can be inputted into Gen AI tools and the types of information that cannot be inputted (e.g., personal[1], confidential, proprietary or copyrighted data)[2].

Data Protection Tip💡: If personal data is permitted for input into Gen AI tools, it is recommended that organisations instruct employees to anonymise the personal data (where possible and appropriate) and provide clear instructions on how personal data should be anonymised or cleansed before input.

☑ **Permissible use of output information:** Provide clear instructions on the permissible purposes[3] for using the information (including personal data) generated by Gen AI tools, and whether, when and how such personal data should be anonymised before further use.

☑ **Permissible storage of output information:** Require that the information generated by Gen AI tools, including any information used by employees, be stored according to the organisation's information management policy and deleted according to its data retention policy.

☑ **Compliance with other relevant internal policies:** Ensure that the policy on the use of Gen AI is aligned with the organisation's other relevant internal policies, including those on personal data handling and information security.

1 Data Protection Principle 3 of the Personal Data (Privacy) Ordinance stipulates that personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than the purpose for which the data was collected.

2 When considering the permissible types and amounts of information for input, organisations should take into account the level of security safeguards and privacy protections that the permitted Gen AI tools offer.

3 See Footnote 1.

Lawful and Ethical Use and Prevention of Bias

- ☑ Specify that employees shall not use Gen AI tools for unlawful or harmful activities.
- ☑ Emphasise the importance of employees acting as human reviewers to ensure that AI-generated output aligns with the ethical values and standards of the organisation.
  - **Accuracy and verification:** Emphasise the need for employees to verify the information provided by AI, including proofreading and fact-checking, to ensure that the information is accurate and up-to-date.
  - **Prevention of bias and discrimination:** Alert employees to the possibility that AI-generated output can be biased and discriminatory and set out the correction and reporting mechanisms to be followed.
  - **Watermarking/labelling:** Provide clear instructions on when and how AI-generated output should be watermarked or labelled.

Data Security

- ☑ **Permitted devices:** Specify the devices on which employees are permitted to access Gen AI tools, for example:
  - Office computers;
  - Work mobile phones; and/or
  - Tablets.

Data Protection Tip💡: Organisations are recommended to require employees to solely use Gen AI tools for work-related purposes on work devices.

- ☑ **Permitted users:** Specify the permitted users of Gen AI tools, such as employees who have operational needs and have received relevant training, and whether permission is necessary before use.
- ☑ **Robust user credentials:** Require employees to use unique and strong passwords along with multi-factor authentication.
- ☑ **Security settings:** Require employees to maintain stringent security settings in Gen AI tools for work-related input.

Data Protection Tip💡: Disallowing saving functions and disabling the sharing of prompts with Gen AI tool providers can help to minimise the risk of data security incidents and the behavioural profiling of employees.

- ☑ **Response to AI incident and data breach incident:** Require employees to report AI incidents according to the organisation's AI Incident Response Plan, including the following:
  - Data breach incidents involving the use of AI;
  - Unauthorised input of personal data into Gen AI tools;
  - Abnormal output results; and/or
  - Output results that may breach the law.

Data Protection Tip💡: Organisations can refer to the PCPD's "Guidance on Data Security Measures for Information and Communications Technology"[4] and "Guidance on Data Breach Handling and Data Breach Notifications"[5] for more tips on enhancing data security and handling data breach incidents.

4 Available at https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_datasecurity_e.pdf

5 Available at https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_note_dbn_e.pdf

Violations of the policies or guidelines

- Specify the possible consequences of employees' violation of the policies or guidelines on the use of Gen AI.

Data Protection Tip💡: Organisations can refer to the PCPD's "Artificial Intelligence: Model Personal Data Protection Framework"[6] for recommendations on establishing Gen AI governance structure and measures (e.g., measures for the management and continuous monitoring of the use of Gen AI tools by employees).

Practical Tips on Supporting Employees in Using Gen AI Tools

- **Transparency:** Regularly communicate the policies or guidelines to employees to ensure that they clearly understand whether they are permitted to use Gen AI tools and how to use them, and keep employees informed of updates to the policies or guidelines.
- **Training and resources:** Educate employees on how to use Gen AI tools effectively and responsibly, for example by:
  - Explaining the capabilities and limitations of AI tools;
  - Providing practical tips and examples of appropriate and secure uses of AI tools at work; and/or
  - Encouraging employees to read the privacy policy, terms of use and other data handling policies covering AI tools to understand how personal data will be collected, stored, used and shared.

Data Protection Tip💡: Organisations can encourage employees to read the "10 TIPS for Users of AI Chatbots"[7] published by the PCPD.

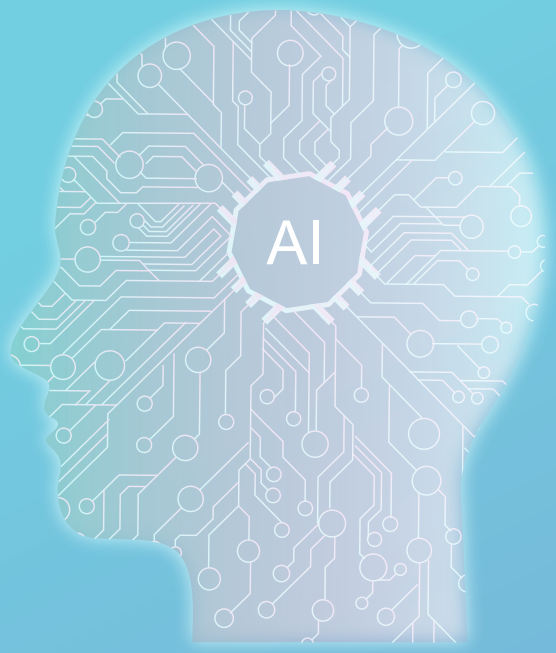
- **Provision of support team:** Set up a designated support team to assist employees to use Gen AI tools in their work. In addition to technical assistance, the support team should also be able to address any concerns that the employees have in relation to the policies or guidelines.

Data Protection Tip💡: The support team can include personnel responsible for the organisation's compliance with data protection laws (e.g., a Data Protection Officer) and for the organisation's AI governance (e.g., members of the AI Governance Committee or similar body).

- **Feedback mechanism:** Establish channels for employees to provide feedback on their experience using Gen AI tools in their work, which can help the organisation to identify areas for improvement and tailor internal policies or guidelines to the circumstances.

6 Available at https://www.pcpd.org.hk/english/resources_centre/publications/files/ai_protection_framework.pdf

7 Available at https://www.pcpd.org.hk/english/resources_centre/publications/files/ai_chatbot_leaflet.pdf



PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Tel : **2827 2827**
Fax : **2877 7026**
Address : **Unit 1303, 13/F., Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong**
E-mail : **communications@pcpd.org.hk**

PCPD Website: pcpd.org.hk

Download this Publication

Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law and do not constitute legal or other professional advice. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

March 2025