AFS Intercultural Exchanges — Guidelines on the Use of Artificial Intelligence

Published and Effective in December 2025

Table of Contents

1. Rationale and Purposes

1.1 AFS Intercultural Exchanges (hereinafter AFS HKG), one of the organizations of AFS Intercultural Programs (hereinafter AFS INT) located in Hong Kong, is committed to making all reasonable efforts to use artificial intelligence tools (hereinafter AI) responsibly.

1.2 Staff members and volunteers of AFS HKG (hereinafter staff and volunteers) bear responsibilities when using AI in connection with their work or voluntary work for AFS HKG. AFS HKG may lose the trust of stakeholders if staff and volunteers use AI irresponsibly.

1.3 It is noteworthy that while the use of AI offers great potential, and fosters creativity and productivity, it presents risks related to data privacy, intellectual property, accuracy, bias, and ethical considerations.[1]

1.4 This document sets out principles for the safe, responsible and ethical use of AI, to mitigate the risks brought by the improper use of AI. It should be read in conjunction with "Other Important Information" listed in paragraphs 6.1 and 6.2.

1.5 Staff and volunteers should make reference to this document and raise awareness about the risks when using AI in connection with their work or voluntary work for AFS HKG.

2. Definitions and Scopes

2.1 Artificial Intelligence

- According to the Office of the Privacy Commissioner for Personal Data, Hong Kong (hereinafter PCPD), AI refers to "a family of technologies that involve the use of computer programmes and machines to mimic the problem-solving and decision-making capabilities of human beings. Examples of AI applications include image recognition, speech recognition, chatbots, data analytics and automated decision-making or recommendation".[2]
- According to AFS INT, the emerging type of AI is Generative AI (hereinafter Gen AI). Gen AI "is a type of AI that can create new content, such as text, images, audio, and video. It works by learning patterns from existing data and then using this knowledge to generate new outputs that are similar in

[1] Please refer to this paper for more details: AFS INT's "AI Policy FAQs".
[2] Please refer to this paper for more details: PCPD's "Guidance on the Ethical Development and Use of Artificial Intelligence".

style and content. Generative AI tools can be used for a variety of purposes, including content creation, data augmentation, and research"[3].

2.2 Staff and volunteers should not input sensitive data of AFS (including AFS INT and AFS HKG; hereinafter AFS sensitive data) into AI tools (details will be provided in paragraphs 4.2 and 4.3). As defined by AFS INT[4]:

- AFS sensitive data is the collective term of personal data, confidential information and AFS proprietary information.
- Personal data is "any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier".
- Confidential information includes "any information that is not publicly known and is not intended to be shared outside the organization, such as business strategies, financial data, and internal communications".
- AFS proprietary information includes "any information that is owned by AFS and is not publicly known, such as intellectual property, trade secrets, internal processes, and confidential business information".

3. Regulations

3.1 When using AI, staff and volunteers should take account of the legal and regulatory framework of Hong Kong, including but not limited to laws relating to copyright, privacy, and anti-discrimination. They should also use AI in a manner consistent with the guidance and requirements provided by regulatory authorities, refraining from using AI for any illegal, non-compliant, or inappropriate purposes.[5]

3.2 Staff and volunteers should collect, hold, process and use personal data lawfully in accordance with the "Personal Data (Privacy) Ordinance (hereinafter PDPO)" when using AI, in particular the six data protection principles in Schedule 1 to the PDPO, which cover the entire life cycle of the handling of personal data from collection, retention, use to deletion (refer to Appendix for details).[6]

[3] Please refer to this paper for more details: AFS INT's "Network Policy on Artificial Intelligence".
[4] Please refer to these papers for more details: AFS INT's "Network Policy on Artificial Intelligence" and AFS INT's "AI Policy FAQs".
[5] Please refer to this paper for more details: Digital Policy Office's "Hong Kong Generative Artificial Intelligence Technical and Application Guideline".
[6] Please refer to this paper for more details: PCPD's "Guidance on the Ethical Development and Use of Artificial Intelligence".

4. Principles

4.1 Below are some key principles listed in AFS INT's "Network Policy on Artificial Intelligence".[7] Staff and volunteers should keep these in mind when using AI in connection with their work or voluntary work for AFS HKG:

- Protect Privacy, Confidentiality and Proprietary Information
- Be Mindful of Copyright and Other Intellectual Property Issues
- Review for Inaccuracies
- AI Ethical Issues
- Security and Use

4.2 Protect Privacy, Confidentiality and Proprietary Information

- Do not refer to or enter into Chat GPT or any other AI chatbots or language models any AFS sensitive data unless for specific sub-sets of such type of data as authorized by AFS (including AFS INT and AFS HKG) for specific tools that ensure appropriate levels of security (typically tools available for a service fee).
- In all cases, take proper steps to "opt-out" from the AI tool's collection and further use of any uploaded information when possible.

4.3 Be Mindful of Copyright and Other Intellectual Property Issues

- Intellectual Property Rights: Respect and protect intellectual property rights, both internally and externally. Unauthorized use of copyrighted material or creation of content that infringes on the intellectual property of others is strictly prohibited.
- Responsible AI Usage: Ensure that the generated content produced using generative AI aligns with AFS's values, ethics, and quality standards.
- AI for Content Creation: Generative AI tools can be used for content creation, such as drafting documents, creating presentations, and generating marketing materials. However, it is important to ensure that the AI tools are not provided with content that contains AFS sensitive data.
- Output: Be mindful that staff and volunteers may own the output of Chat GPT or any other Generative AI chatbots or language models. Chat GPT Terms state that the user is assigned all its right, title and interest in and to the chat output. This would mean that users can use the generated content for any purposes. There is a risk, however, that the same content be generated for other users who ask the same or similar questions. Also, one would have to ensure that the AI is actually creating new original content to be able to get copyright. So be mindful that the question of who owns the written content generated by AI tools like Chat GPT is not entirely solved.

[7] Please refer to this paper for more details: AFS INT's "Network Policy on Artificial Intelligence".

4.4 Review for Inaccuracies

- Content produced by AI may be, and often is, inaccurate; therefore, always review and double-check the content, and use other reliable sources when needed.
- The generated content must not be used if it is inaccurate, misleading, harmful, offensive, or discriminatory.

4.5 AI Ethical Issues

- Be mindful that AI content may be biased as it may be the set of data used to train AI tools.

4.6 Security and Use

- Preferred Generative AI Tool: the preferred generative AI tool for the AFS Network is Google Gemini. It offers strong security measures and integrates well with the existing Google Workspace. Please assess with Angela Yung, Executive Director of AFS HKG and then contact privacy@afs.org to request access to the premium version of Gemini.
- Data Security:
  - Always be aware of the security risks involved in using AI tools.
  - Never input AFS sensitive data into any AI tool, including Gemini.
  - Follow organizational guidelines on data security and privacy when using AI tools.
- Appropriate Use of AI Tools:
  - Use AI tools responsibly and ethically.
  - Ensure that the use of AI tools aligns with AFS's values, mission, and code of conduct.
  - Be mindful of the potential biases present in AI-generated content.
- Unauthorized AI Tools:
  - The use of unauthorized AI tools that require access to AFS sensitive data is strictly prohibited.
- Questions or Concerns:
  - If staff and volunteers have any questions or concerns about the use of AI tools, discuss with Angela Yung, Executive Director of AFS HKG at angela.yung@afs.org, then contact the IT department and Data Protection team at privacy@afs.org.

4.7 In addition, staff and volunteers should make reference to the Hong Kong Government Digital Policy Office's recommendations when using AI services[8]:

- Maintain Independent Discretion
- Understand Responsibilities and Obligations
- Prudent Dissemination

[8] Please refer to this paper for more details: Digital Policy Office's "Hong Kong Generative Artificial Intelligence Technical and Application Guideline".

4.8 Maintain Independent Discretion: Generative AI serves as a tool, not a replacement for users. It should not be adopted without human verification and judgment. Staff and volunteers should possess a multifaceted awareness and knowledge capability in law, ethics, and risk management, so as to validate and review generated content and make independent information judgments.

4.9 Understand Responsibilities and Obligations: Before engaging with any generative AI services, staff and volunteers should thoroughly read and familiarise themselves with the terms of use of the relevant platforms or software to understand their responsibilities and obligations. These terms often encompass themes such as privacy, security, ethical standards, and legal compliance. For instance, it is explicitly stipulated that users may not instruct AI to generate content that contains hate speech, discrimination, defamation, or other immoral and illegal content, as well as protections for users' rights, such as restrictions on the sharing of personal data to prevent users from recording and disseminating users' personal information beyond the scope of consent.

4.10 Prudent Dissemination: Any content generated by generative AI systems and further disseminated, which may impact society, economy, or culture, ultimately holds the content disseminator responsible. This means that staff and volunteers need to assess and take responsibility for the potential misdirection or negative consequences of the content. Staff and volunteers should proactively verify the authenticity, legality, and appropriateness of generated content and seek professional advice or conduct secondary reviews when necessary to reduce potential risks.

5. AFS HKG's Obligations

5.1 AFS HKG will circulate this document to staff and volunteers.

5.2 AFS HKG will assign staff to relevant trainings.

5.3 AFS HKG will closely monitor the updated regulations and policies regarding the use of AI tools. Where appropriate, AFS HKG will revise this document and inform staff and volunteers accordingly.

6. Other Important Information

6.1 The below materials have been referenced in this document:

- AFS INT's "AI Policy FAQs"
- AFS INT's "Network Policy on Artificial Intelligence"

- Digital Policy Office's "Hong Kong Generative Artificial Intelligence Technical and Application Guideline"
- Office of the Privacy Commissioner for Personal Data, Hong Kong's "Guidance on the Ethical Development and Use of Artificial Intelligence"

6.2 The below materials have been quoted by AFS INT:

- AFS INT's "Network Policy on Data Protection"
- UNESCO's "Recommendation on the Ethics of Artificial Intelligence"
- EU's "Artificial Intelligence Act"

Appendix: Data Protection Principles under the Personal Data (Privacy) Ordinance

The Personal Data (Privacy) Ordinance (Cap. 486) (hereinafter PDPO) governs the collection, holding, processing and use of personal data by both private and public sectors. The PDPO is technology-neutral and principle-based. The Data Protection Principles (hereinafter DPP) in Schedule 1 to the PDPO represent the core requirements of the PDPO and cover the entire life cycle of the handling of personal data from collection to destruction.[9]

DPP 1 - PURPOSE AND MANNER OF COLLECTION

DPP 1 provides that personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user. The means of collection shall be lawful and fair. The data collected shall be necessary and adequate but not excessive for such purpose.

Data users shall also be transparent as regards the purpose of collection and the potential classes of persons to whom the personal data may be transferred, and the data subjects' right and means to request access to and correction of their personal data. Usually, the information is presented in a Personal Information Collection Statement.

DPP 2 - ACCURACY AND DURATION OF RETENTION

DPP 2 requires data users to take all practicable steps to ensure that personal data is accurate and is not kept longer than is necessary for the fulfilment of the purpose for which the data is used. Section 26 of the PDPO contains similar requirements for the erasure of personal data that is no longer required.

If a data user engages a data processor for handling personal data, the data user must then adopt contractual or other means to prevent the personal data from being kept longer than is necessary by the data processor.

DPP 3 - USE OF DATA

DPP 3 prohibits the use of personal data for any new purpose which is different from and unrelated to the original purpose of collection, unless express and voluntary consent has been obtained from the data subjects.

[9] Please refer to this paper for more details: PCPD's "Guidance on the Ethical Development and Use of Artificial Intelligence".

DPP 4 - DATA SECURITY

DPP 4 requires data users to take all practicable steps to protect the personal data they hold against unauthorised or accidental access, processing, erasure, loss or use.

If a data user engages a data processor in processing the personal data held, the data user must adopt contractual or other means to ensure that the data processor complies with the aforesaid data security requirement.

DPP 5 - OPENNESS AND TRANSPARENCY

DPP 5 obliges data users to take all practicable steps to ensure certain information, including their policies and practices in relation to personal data, the kind of personal data held and the main purposes for which the personal data is held, is generally available to the public.

DPP 6 - ACCESS AND CORRECTION

DPP 6 provides data subjects with the right to request access to and correction of their own personal data.

DPP 6 is supplemented by the detailed provisions in Part 5 of the PDPO which covers the manner and timeframe for compliance with data access requests and data correction requests, the circumstances in which a data user may refuse such requests, etc.