Interim PIA Guidelines: Generative AI Tools

Overview

This document outlines the Privacy Impact Assessment (PIA) guidelines applicable to artificial intelligence (AI) tools, including but not limited to generative AI (GenAI) tools such as Microsoft Copilot and DALL-E. These guidelines detail the acceptable use of publicly available GenAI tools from a privacy and information security standpoint, and will be updated as related AI concerns develop and new insights arise. This guidance addresses several primary use cases and extends to:

- Student academic use
- Employee use in business contexts
- Classroom use by instructors

Navigating Registration and Prompt Interactions

GenAI tools should only be used with Low-Risk Information (as defined by UBC Information Security Standard U1). Information is generally consumed by GenAI tools in the following ways:

- **Registration:** Name, contact details, and password.
- **Prompts/forms**: The place where users ask questions or submit information/documents.
- **Training data**: The data sets used to train the GenAI model on how to respond (this is only an option for information sharing if creating a large language model).
- **User authorized sources:** Provide models with access to use a user's microphone, camera, files, or screen contents to provide contextual answers.

Student Academic Use

Students' personal use of GenAI tools does not involve UBC collection of personal information. However, if GenAI tools are integrated into classroom instruction or assignments, instructors should inform students about responsible use, as outlined in these guidelines and other University-issued directives (see Additional Resources below).

Employee Use in Business Contexts

Keep data safe during registration: When users sign up for GenAI tools, their email address and phone number is usually required (and sometimes additional personal details). Be mindful of the following:

- Sharing this information can expose users to the risk of unauthorized data collection or misuse. Where possible, supply business contact information rather than personal information.
- If a tool requires creating an account password, do NOT reuse CWL credentials for that account. Always use a unique password for every account.
- Adhering to UBC Information Security Standards is a mandated practice for ensuring the secure and compliant use of generative AI within the University context.
- Employees must confirm their authority to execute a Clickthrough Agreement as per UBC Board of Governors Signing Resolution #26, to prevent unauthorized commitment to third party Terms of Use.

Be cautious with input/prompt information provided to GenAI tools (questions, documents, etc.):

- Ensure only Low Risk Information (as defined by UBC Information Security Standard U1) is inputted and avoid any sharing of personal information or sensitive data.
- Assume all inputs will become public information. Do not disclose any information that should not be made public.
- Know that any input data may be used to improve or train AI models. It is recommended to turn off the chat history or training functions.
- Review outputs for accuracy, before acting on the results.

Classroom Uses by Instructors

Instructors, as employees of the University, should review the business-use guidance above. In addition, instructors may need to provide guidance to students on how they should use GenAI tools, if used for teaching purposes. The PIA Team recommends:

- Against requiring students to use GenAI tools over which UBC has no contractual control, due to the inherent privacy risks.
- Making it optional for students to sign-up for a GenAI tool if that tool requires students to supply their personal information, such as an email address.
- Providing alternative sign-up options that do not require submitting personal data, such as using aliases (if permitted by the tool's Terms of Use).

When is a PIA Required?

PIA NOT REQUIRED (in any of the following situations)	• **Student use**: During account creation, students enter into a direct contractual relationship with the AI tool's vendor. Student-created records are outside of the custody or control of the University. • **Research use:** Researchers should contact the Office of Research Ethics or Advanced Research Computing (ARC) for further information about their use of AI tools in academic research contexts. Note: If using Medium Risk Information (as defined by UBC Information Security Standard U1) during interactions with AI tools—examples of which include proprietary information received from a third party under a non-disclosure agreement, restricted circulation library journals, and non-personal research information—assume this information will become public information if disclosing it to the tool. Do not disclose information that should not be made public. • **Administrative use:** There are many low-risk uses of AI Tools. If your use case is not identified in the "PIA Required" category, a PIA isn't necessary. However, if you are concerned about your use-case, please submit a PIA Inquiry for further guidance.

PIA REQUIRED (in any of the following situations)	• **Externally-hosted AI model or GenAI service:** If using High or Very High-Risk Information (as defined by UBC Information Security Standard U1) during interactions with AI tools, a PIA is required.
	• **Local use of open-source AI models:** If you are running a downloaded AI model locally, a PIA is required if High Risk or Very High-Risk information (that is not incidental*) is involved or if ANY of the following conditions are met:
	  ○ The application/model will be used by or on behalf of the University to make a decision that directly affects an individual.
	  ○ The application/model is connected to or shares data with a non-UBC party, including the authors, developers, or publishers of the application/model.
	  ○ The locally hosted application/model is intended to be made available as a service to internal or external parties.
	***Incidental**: Refers to unexpected and unnecessary submission of personal information. It does not include personal information intentionally present in structured data like spreadsheets.*

If you are uncertain whether your use-case meets the conditions noted above, please submit a PIA Inquiry.

Additional Resources

UBC CIO Generative AI Guidelines

UBC CIO Generative AI Website

CTLT AI in Teaching and Learning Website

UBC Academic Integrity Guidelines

For questions about the information contained in these guidelines, or to initiate a PIA Inquiry, visit Privacy Matters.