PRIVACY MATTERS @ UBC

Interim PIA Guidelines: Generative AI Tools

Overview

This document outlines the Privacy Impact Assessment (PIA) guidelines applicable to generative artificial intelligence (AI) tools, including but not limited to *ChatGPT*, *GitHub Copilot*, and *DALL-E*. These guidelines detail the acceptable use of publicly available generative AI tools from a privacy and information security standpoint and will evolve as related concerns and understanding develop. This guidance addresses several basic use cases and extends to:

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

Navigating Registration and Prompt Interactions

Generative AI tools should only be used with Low Risk Information (as defined by UBC Information Security Standard U1). Users submit information at three points:

1. **Registration:** Name, contact details and password.
2. **Prompts/forms**: The place where users ask questions or submit information/documents.
3. **Training data**: The vast data sets used to train the AI on how to respond (this is only an option for information sharing if creating a large language model).

Student Academic Use

Students' personal use of generative AI tools does not involve UBC collection of personal information. However, if generative AI 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 it safe during registration: When users sign up for generative AI 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.
- Adhering to UBC Information Security Standards is a mandated practice for ensuring the secure and compliant use of generative AI within the University context.
- If a tool requires creating an account password, do NOT reuse CWL credentials for that account. Always use a unique password for every account.
- Employees must confirm their authority to execute a Clickthrough AgreementUBC Board of Governors Signing Resolution #26, to prevent unauthorized commitment to third party Terms of Use.

Be cautious with input/prompt information provided to 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 or sensitive data.
- Any input data may be used to improve or train AI models. It is recommended to turn off the chat history or training functions.
- Assume all inputs will become public information. Do not disclose any information that should not be made public.

PRIVACY MATTERS @ UBC

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 generative AI tools, if used for teaching purposes. The following applies:

- The PIA team recommends against requiring students to use AI tools over which UBC has no contractual control, due to the inherent privacy risks[1].
- Make sure it is optional for students to sign up for an AI tool if that tool requires students to supply their personal information, such as email address.
- Provide 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 REQUIRED	PIA NOT REQUIRED
Use including High or Very High Risk information: If using High or Very High Risk Information (as defined by UBC Information Security Standard U1) during interactions with generative AI tools, a PIA is required.	**Student use**: During account creation, students enter a direct contractual relationship with the AI tool's vendor. Student-created records are outside of the custody or control of the University.
Local use of open-source AI models: If running a downloaded AI model locally, a PIA and security assessment is required.	**Research use:** Researchers should contact the Office of Research Ethics or Advanced Research Computing (ARC) for further information about their use of generative AI tools in academic research contexts. Note: If using Medium Risk Information (as defined by UBC Information Security Standard U1) during interactions with generative 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.

Additional Resources

UBC CIO Generative AI Guidelines (coming soon)

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 the PIA Process, or to initiate a PIA Request or PIA Inquiry, visit Privacy Matters

[1] As of October 2023, Microsoft has activated Bing Chat Enterprise for all licensed users within the UBC community. Initiate a PIA Inquiry via the Privacy Matters website for clarification and support on your use-case of Bing.