PIA Guidelines: Artificial Intelligence Solutions

Overview

This document provides Privacy Impact Assessment (PIA) guidance for the expected use of Artificial Intelligence (AI) solutions at UBC. This guidance helps ensure compliance with the British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA) and UBC Information Security Standards (ISS), clarifying when a PIA is required. The document is also designed to help guide University constituents to relevant support and highlights applicable UBC Policies and generative AI (GenAI) principles.

Before reading further, it is recommended that you first familiarize yourself with the available AI solutions at UBC that have undergone a PIA as well as UBC's Principles for the Use of Generative AI Tools.

Guidance around AI use varies based on your affiliation with UBC and the use case you are considering. Are you a student, faculty member, researcher, or administrative staff? Consider your role and AI use case when reviewing these guidelines.

**Be sure to check out the linked resources below as well as other use case focused PIA Guidelines, such as Meeting Recording, Transcription and Meeting Assistant Tools.*

Categorization of AI Solutions

These guidelines categorize AI solutions into four distinct types, to address guidance more effectively for a diverse and general set of AI applications/models:

1. **Individual AI**: Standalone AI solutions used by individuals for a wide variety of purposes, ranging from administrative to academic, research, and personal use. Examples include general purpose large language models like ChatGPT, Microsoft 365 Copilot, and meeting assistants like Otter.ai, or note taking tools like Glean.co. A PIA is required when the solution would be used for administrative purposes and will handle personal information, High or Very High Risk Information (as defined by UBC ISS U1). Using these solutions for purposes involving Low Risk Information does not require a PIA.
2. **Embedded AI**: AI functionalities embedded within existing UBC Systems, applications or devices. Examples include Workday Assistant and Salesforce Marketing Cloud. These solutions may require a PIA depending on the nature of use and data handled within the existing system. It is important to understand what data embedded solutions have access to and why this access is necessary. A PIA is required if these solutions access personal information, High or Very High Risk Information.
3. **Platform AI**: Refers to integrated collections of technologies used to develop, train, and run AI models. Solutions developed on these platforms that handle personal information, High or Very High Risk Information, will require a PIA.
4. **Bespoke AI**: These solutions are often custom-developed to address requirements specific to UBC, possibly leveraging platform AI solutions but may also involve developing the model from scratch. They require the University to assume significant development and management responsibilities than third-party tools but can offer unique benefits. A PIA is required if these solutions will handle personal information, High or Very High Risk Information.

For additional information, reference the "When is a PIA Generally Required?" section of this document.

Privacy Considerations for Individual AI Solutions by Affiliation

Navigating Registration and Prompt Interactions for Publicly Available Individual Solutions

Most freely available Individual AI tools should only be used with Low Risk Information (as defined by UBC ISS U1). Be mindful that information is consumed by these solutions in the following ways:

- **Registration:** Name, contact details, and password.
- **Prompts/forms**: The place where users ask questions or submit information/documents.
- **User-authorized sources**: These may allow models to access the user's microphone, camera, files, screen contents, or other applications to deliver context-driven responses.
- **Restricted Services**: Avoid use of DeepSeek or other software/services identified in UBC ISS U12.

Employee Use in Administrative Contexts

Keep data safe during registration: When users sign up for GenAI tools, their email address and phone number are 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 the UBC ISS is a mandated practice for ensuring the secure and compliant use of GenAI 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.
- Review the product's privacy policy and terms of service prior to use. Seek to understand the privacy/security protections offered through different licensing tiers. Submit a PIA Inquiry if you require support in understanding the potential risks for a particular tool.

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

- Ensure only Low Risk Information is entered. Avoid any sharing of personal information or sensitive data.
- If Medium Risk Information is to be entered, ensure your use case and the data to be used has been discussed and permitted by your Administrative Head of Unit when executing the Clickthrough Agreement.
- 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 at UBC should review the administrative-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 the following:

- Students' use of publicly available GenAI tools should be optional if it involves the submission of students' personal information. Using an alias is a common way to mitigate aspects of associated privacy risks.
- Avoid making it mandatory for students to use tools that UBC does not have a contract with, as this could pose privacy risks.
- Offer alternative sign-up options that do not require personal data, such as using aliases, if the tool's Terms of Use allow it.

Student Academic Use

Students' personal use of GenAI tools does not involve the collection of personal information by UBC and therefore does not require a PIA. 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).

When is a PIA Generally Required?

PIA NOT REQUIRED (in any of the following situations)	• **Student use**: During account creation, students enter a direct contractual relationship with the AI tool's vendor. Student-created records are outside the custody or control of the University. • **Research use:** Researchers should contact the Office of Research Ethics or Research Cybersecurity Compliance for further information about the use of AI tools in academic research contexts. • **Administrative use:** PIAs are not required for use cases involving Low or Medium Risk Information (as defined by UBC ISS U1), or if the platform and use case have already been reviewed as part of the PIA process. See GenAI – Privacy and Risk for more guidance. • **Other considerations (Research and Administrative Use):** ○ Use cases involving new solutions should first ensure there is appropriate authority to execute a Clickthrough Agreement. ○ Consult with your local IT department or Client Service Manager before implementing a new solution. Note: If using Medium Risk Information during interactions with GenAI tools—examples 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 it is disclosed to the tool. **Do not disclose information that should not be made public**.
PIA REQUIRED (in any of the following situations)	A PIA is required if using High or Very High Risk Information that is not incidental*. Further indicators that a PIA is required include: • 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. The above are referenced because they are strong indicators of collection, use or disclosure of personal information in an AI context. They do not supersede the primary guidance around High or Very High Risk Information. ****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

GenAI Tools and Privacy Impact Assessment