

Guidelines: Generative AI Tools

Overview

This document provides guidelines when using generative artificial intelligence (AI) tools, including but not limited to ChatGPT, Copilot, Claude, and DALL-E. These guidelines detail the acceptable use of public, paid and unpaid 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
- Course delivery uses by instructors.
- Employee use in business contexts
- Research Use
- Use of Local models (for example: models run on Selkirk College provisioned hardware such as servers, laptops, or desktops).

These guidelines work in conjunction with other college policies including Policy 6550: Protection of Privacy (<https://policies.selkirk.ca/policy/6550/>).

These guidelines are adapted from work by the University of British Columbia (2026) for Selkirk College.

Navigating Registration and Prompt Interactions

Only low-risk information should be used into Generative AI tools.

Low Risk Information typically includes:

- Publicly available information (for example: posted on websites, public directories)
- General business information that is not confidential
- Non-sensitive operational data
- Anonymous or de-identified data with no personal identifiers
- General inquiries or questions without specific details tied to a real, identifiable person, group, or incident.
- Public research findings already published.

- Publicly listed contact information (public phone numbers, published email addresses)

Low Risk Information does NOT include:

- Personal information and identifiers (Any information that can directly or indirectly identify a person, such as student name, student number, employee number, SINS, birth dates, addresses, phone numbers, personal emails, or any combination of data points that could reasonably identify an individual.)
- Student records or grades
- Employee HR information (salaries, performance reviews, medical info)
- Financial data (credit cards, banking info, budgets)
- Proprietary or confidential business information
- Research data that has not been published or that is protected by ethics procedures.
- Any information the college is required to protect under privacy legislation (FIPPA), including personal and confidential institutional records.
- Authentication credentials (passwords, security questions)

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 Selkirk College collection of personal information. However, if generative AI tools are explicitly integrated into course delivery and assessments, instructors should inform students how they used AI and discuss responsible use, as outlined in these guidelines and other college-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 sometimes additional personal details is required. 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 your Selkirk College credentials for that account. Always use a unique password for every account.
- Employees must confirm their authority to execute clickthrough agreements with third-party vendors, to prevent unauthorized commitment to third party Terms of Use.

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

- Ensure only low risk information is inputted and avoid any sharing of personal or sensitive data.
- In the default settings of most AI tools, any input data may be used to improve or train AI models. It is recommended to turn off training functions, as this reduces long-term exposure risk and keeps your inputs from being further redistributed.
- Assume all inputs will become public information. Do not disclose any information that should not be made public.

Selkirk College is conducting pilot programs with publicly available models tailored to specific use cases. Licensed versions typically offer enhanced information management capabilities. At present, the institution is piloting licenses for Microsoft CoPilot, Anthropic Claude, and Perplexity.

Classroom Uses by Instructors

Instructors, as employees of the college, should review the business use and student 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:

- Selkirk College instructors should be transparent about their own use of AI including developing course content and assessments.
- Selkirk College recommends against requiring students to use AI tools over which Selkirk College has no contractual control, due to the inherent privacy risks.
- 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 name, email address, or other personal identifiers.
 - Alternate options should be available to reach teaching outcomes when personal information is required.

Research Use

When incorporating AI tools into research activities at Selkirk College, researchers must consider the information being used. Generative AI platforms may use any data inputted to improve or train these models. It is strongly recommended to turn off model training functions whenever possible, as these are typically enabled by default. All data shared with AI tools should be assumed public, and confidential or sensitive information must not be disclosed.

Any information that would exceed a low-risk designation would require a privacy assessment to be completed.

Before using AI in research, consult the Selkirk College Information Security Standards to determine the risk level of the information being processed. Usage of high or very high risk data, or deploying open-source AI models locally, requires a Privacy Impact Assessment (PIA) and a security review.

For medium risk information—such as proprietary third-party data, restricted library journals, or non-personal research data—assume public exposure and exercise caution.

Researchers are encouraged to contact the Research Ethics Board or IT Services for guidance on appropriate privacy protocols and risk assessments. Adhering to these directions helps protect both individual and institutional privacy, while supporting responsible innovation in academic research.

When is a PIA required

Not Required

- 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 college. (see Required below)
- 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 is not necessary. However, if you are concerned about your use-case, please contact the privacy officer or AI Steering Committee

Required

- When AI tool is required for course or credential completion
 - If the college is compelling students to disclose personal information to a third party.
- Externally hosted AI model or GenAI service: If information exceeds low-risk information interactions with AI tools.
- Local use of open-source AI models: If you are running a downloaded AI model locally, a PIA is required if information exceeds low risk or if:
 - The application/model will be used by or on behalf of the Selkirk College to make a decision that directly affects an individual.
 - The application/model is connected to or shares data with an external 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.

Additional Resources

- Selkirk College Policies
 - Cheating and Plagiarism
 - <https://policies.selkirk.ca/policy/8618/>
 - Acceptable Use of Electronic Resources
 - <https://policies.selkirk.ca/policy/7110/>
 - Protection of Privacy
 - <https://policies.selkirk.ca/policy/6550/>
 - [policies.selkirk.ca policy.](https://policies.selkirk.ca/policy/)
- Teaching and Learning with AI Resources

- Generative AI Guidelines & Resources | Selkirk College
 - <https://selkirk.ca/student-life-support/student-supports/learning-supports/academic-integrity/generative-ai-guidelines-resources>

For questions about the information contained in these guidelines or the PIA Process, or to initiate a PIA Request or PIA Inquiry, please contact privacy@selkirk.ca

References

University of British Columbia (2026). UBC Guidance, UBC Privacy Matters PIA Guidelines. Retrieved from https://privacymatters.ubc.ca/sites/default/files/2024-09/PIA_Guidelines_GenAI.pdf