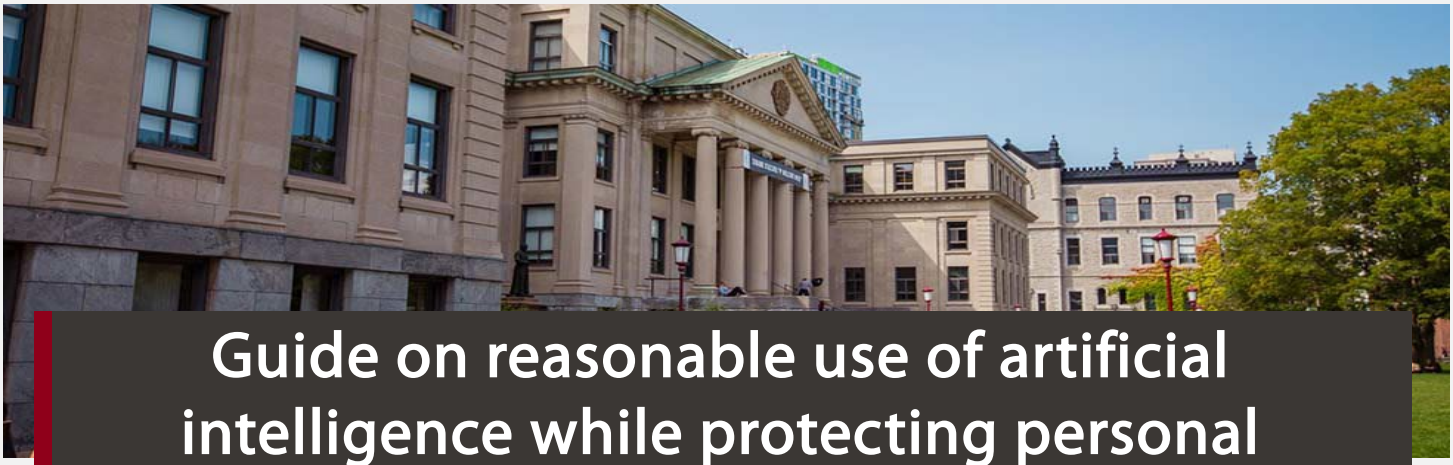

Guide on reasonable use of artificial intelligence while protecting personal information

Introduction

The Access to Information and Privacy Office (AIPO) has created this guide to advise University staff on using artificial intelligence (AI) at work. We wish to provide direction for your decisions on AI use and help you make the right choices, so that the University meets its privacy requirements.

PLEASE NOTE: AI systems are changing rapidly. Our office could therefore revisit our position on their use. You should regularly review this document, which will be modified as necessary.

What is AI?

Artificial intelligence, or AI, is technology that enables computers and machines to simulate human intelligence and problem-solving capabilities. For example, it can write and translate documents, analyze images and automate some administrative tasks. AI is based on algorithms and deep learning building on vast quantities of data.[1]

Today, AI can be found in many areas. We all use it, sometimes without realizing it. For example, it can be found in machine translation tools like DeepL, Google Translate or Grammarly, in conversational AI applications like ChatGPT or Microsoft Copilot, or in Teams through agents that can take meeting notes and create transcriptions.

[1] "What is AI?", IBM

Access to Information and Privacy Office

Tabaret Hall, M407
550 Cumberland Street, Ottawa, ON
K1N 6N5

Tel.: 613-562-5800 ext.1851
aipo@uOttawa.ca

uOttawa

University privacy obligations

Under Ontario's *Freedom of Information and Protection of Privacy Act* and the University's Policy 90 — Access to Information and Protection of Privacy:

- The University is responsible for information under its custody or control and must meet its obligations and protect the integrity of information.
- Persons affected must be kept informed of use of their information when it is collected. Collection of personal information is subject to a Notice of Collection or express consent.
- Personal information collected by the University is not used or disclosed other than for the purposes indicated in the Notice of Collection or to which the individual has consented or for lawful purposes.
- The University must ensure that the information it holds is correct and up to date.

Unauthorized use of personal information through AI systems can breach both privacy and the law.

- Such use fails to meet the University's obligations.
- Including personal information in query can constitute a privacy breach. You don't know how the queried information is then stored and used. It could be used to train AI and be illegally disclosed.
- Malicious individuals could also retrieve this information.

PLEASE NOTE: As this guide deals primarily with protection of personal information, the above list of risks is not exhaustive. There are many risks in other areas that we must consider when we use AI (e.g., regarding vulnerable groups, truthfulness of content produced and intellectual property).

Recommendations

On January 24, 2024, at a public event in celebration of Data Privacy Day organized by the Information and Privacy Commissioner of Ontario, experts highlighted the importance of transparency, caution and responsibility when using AI. To uphold the University's privacy obligation, we make the following recommendations:

The no-go zone

- Don't use AI for any activity that involves personally identifiable information and sensitive data.
- Never include names, SINs, email addresses and telephone numbers, and avoid other potentially identifiable information. For example, if you want to create a document that discusses a position filled by only one person, simply mentioning the position will allow the person to be identified. People can be easily identifiable even if their names don't appear in the document.

General advice on AI use

- Ask your manager about your sector's best practices.
- Use AI for low-risk activities where you can control the result and only if you have sufficient expertise to confirm whether the content produced is truthful.
- Ideally, use University-approved platforms and create as few accounts as possible on AI platforms not approved or offered by the University (see below).
- Consult with IT on the available tools and to choose the most appropriate tool for you needs.
- Learn about platforms' protection of personal information policies.
- If the AI system uses query data for its own learning, check if it has a opt-out function. If so, enable it.

In your query:

- Use anonymized information.
- Make sure the information you enter is up to date, accurate and necessary for your results. The less information you include in the query, the less risk of a privacy breach.

Use of final AI document or product

- Re-read and edit the AI-produced texts or documents. Make sure they meet expectations and that there are no errors in the information provided.
- Be transparent: Let the recipients of your work know that you've used AI.
- **Remember that information generated by AI tools in the custody and control of the University could be disclosed as part of a freedom of information request under the *Freedom of Information and Protection of Privacy Act*.**

A ChatGPT alternative

Recently, Microsoft launch its artificial intelligence tool, Copilot (formerly Bing Chat Enterprise). The tool, similar to ChatGPT, is covered by the University's Microsoft licences, thus ensuring that we meet our privacy obligations. While we still recommend not including personally identifiable information, this is a more secure solution than other systems.

[Discover Microsoft Copilot]

Log in using your uoAccess account. If you see your icon in the top right corner, you're logged in.

For more, see this video on Bing Enterprise Chat (now Copilot) (1 min).

Other resources on the use of AI

⇒ Principles for responsible, trustworthy and privacy-protective generative AI technologies

⇒ Guide on the use of generative AI

⇒ Training on AI functions and use