AI Writing Series

AI and Your Unpublished Writing:

Risks of Using Large Language Models

By Jodie Salter, PhD, Writing Specialist, University of Guelph

Inputting unpublished writing and data into large language models (LLMs) like ChatGPT carries numerous risks.

Potential risks can be grouped into 4 main areas of concern: **privacy, intellectual property, data security, and reputational concerns.**

Risks:

- If unpublished research is unintentionally incorporated into a model's future outputs, your work could resurface without attribution, thus leading to potential **accusations of plagiarism**.
- If you input unpublished ideas, research, and/or data into an LLM, you could **compromise your ability to retain full intellectual property rights**.
- If sensitive or confidential material is input into an LLM, this could **violate internal institutional data governance policies.**
- If data contains sensitive or personally identifiable information (PII), uploading it to a third-party LLM service (e.g., OpenAI) could **violate privacy laws**, such as Freedom of Information and Protection of Privacy Act (FIPPA) Manual | ontario.ca
- LLM providers may be operating in jurisdictions with different data protection laws, potentially compromising the privacy of your data, leading to **legal complications**.
- If you are developing cutting-edge or proprietary research, using LLMs that store data (even temporarily) may lead to **unintentional early disclosures** and **undermine patent eligibility** and enable other independent developments.

Mitigation Strategies:

Before using any generative AI tool...

1. Read the Terms of Use and Privacy Policy to understand how input data is used and who owns the generated data. Questions can be directed to the UG Information Security Team at infosec@uoguelph.ca and CCS at ithelp@uoguelph.ca.
2. Know the university's (and collaborators, if applicable) organizational research data management and AI-use policies and follow them.
   - Safeguarding Research | Office of Research
   - Research Data Classification
   - Data Storage Guidelines
   - Acceptable Use Policy (AUP): The University reserves the right to audit AI tool usage with appropriate approval where there are reasonable grounds to suspect a violation of any law or University policy.
   - Information Security Guidelines for the Use of Generative Artificial Intelligence (PDF): This document provides "guidelines for the responsible use of generative AI tools by University staff and faculty in a way that protects the confidentiality, integrity, and availability of University information assets and complies with applicable policies, laws, and regulations."
3. Know which providers store and use data for training, and do not use them.
   - (see below "Comparison Table: AI Providers, Training and Data Storage Options")
4. Obtain appropriate approvals from the data owner (and/or sponsors) to use AI tools, and comply with any terms and conditions that they specify.

If you plan to use AI tools...

The following information is excerpted from U of G's Information Security Guidelines for the Use of Generative Artificial Intelligence (PDF) under "Information Security Risks and Guidelines for Secure Usage":

1. Extra care should be exercised whenever sharing information in a private AI tool.
2. Remove any personally identifiable information (PII) and sensitive data before inputting into any LLMs.
   - Internal (S2), Confidential (S3) and Restricted (S4) University data should never be entered into a public AI tool (e.g., ChatGPT) or used in a generative AI prompt.
3. Obtain consent from data subjects if you plan to use an AI tool to collect, process, or disclose personal data.
   - Inform data subjects of the purpose, scope, potential risks, and provide an option to opt out.
4. Ensure system outputs are not identical or substantially similar to copyright protected material.
   - Remove problematic material to minimize the risk of intellectual property infringement.
5. Give proper attribution where appropriate.
   - Indicate explicitly and clearly that generative AI was used to develop content.