Principles and Guidelines for Use of Generative Artificial Intelligence

Topic:	Generative AI
Approval Authority:	VPFA
Approval Date:	
Effective Date:	Oct 1, 2024
Last Revised:	

1. Purpose

Generative Artificial Intelligence (GenAI) is a powerful and quickly evolving technology that has the potential to support and transform the way we work at York University.

York University supports responsible and ethical use of generative AI tools and solutions, but there are important considerations when using these tools, including information security, privacy, compliance, copyright, and other factors. These guidelines rely on York's current policies, procedures, and guidelines to support our use of Generative AI. These guidelines will continue to be updated as we develop the appropriate security features and governance structures to support our use of these innovative tools in University administrative and operational activities.

2. Scope and Application

These guidelines apply to staff, faculty, contractors, or third-party agents that use GenAI technologies in University administrative or operational activities.

3. Definitions

Generative AI (GenAI) refers to an artificial intelligence technology that derives new versions of text, audio, or visual imagery usually from large bodies of data in response to user prompts. GenAI can be used in stand-alone applications, such as OpenAI's ChatGPT, Google's Gemini, or incorporated into other applications, such as Microsoft Bing or Microsoft Office Suite.

4. Principles

All use of GenAI technologies in University administrative or operational activities should align with the principles of ethical use, transparency, accountability, sustainability, security, and privacy, as outlined below.

1. **Ethical Use**: Adhering to ethical standards, particularly in applications with significant social impact.
2. **Transparency**: Clear understanding and appropriate disclosure to others of how GenAI technology is incorporated into solutions, how it makes use of data, and decision-making processes along with potential impacts.
3. **Accountability**: Establishing responsibility for outcomes produced by the AI system. AI generated content can be factually inaccurate, misleading, or biased.
4. **Sustainability**: Consideration of the environmental impact of GenAI systems when weighing the appropriateness of a GenAI-based solution.
5. **Privacy and Intellectual Property Protection**: Safeguarding sensitive data and intellectual property from unauthorized access or misuse.
6. **Security**: Implementing robust measures to protect AI systems from cyber threats and data breaches.

5. Guidelines

1) **Use** - York supports staff using GenAI appropriately in University administrative or operational activities, subject to management approval. The responsible use of this technology introduces opportunities for increased productivity, insights and innovation.
2) **Disclosure** – Ensure that content generated by GenAI is appropriately identified as such in all outward-facing communication of generated content.
3) **Assessment** - Use of GenAI in University administrative or operational activities should be discussed with supervisor and is subject to approval of management – refer to use case assessment table below for further guidance. For use cases where oversight is required, conduct a review and assessment process prior to use, see assessment of use cases below.
4) **Human Oversight** - Ensure that decisions made by GenAI have adequate final review by a human who is accountable for the decision and can vet for errors, bias or discrimination. Understand that responsibility for decisions made by these tools ultimately lies with the person who opts to make use of the tool for that purpose.
5) **Bias** - Ensure output of GenAI are regularly reviewed for bias and discriminatory results. Vetting for bias and discrimination is a complex task and requires expertise – please refer to York's DEDI strategy and toolkit for additional information and guidance.
6) **Privacy & IP Protection**- Ensure that personal information and other confidential or regulated information is not provided to GenAI tools unless explicitly authorized for such data through York's assessment process. Refer to the guidance on the use of information within York University licensed GenAI tools on the UIT website (link). Ensure that only materials and information that you have intellectual property rights over are provided to GenAI.

7) **Cybersecurity** - Ensure that GenAI (including both inputs and outputs of GenAI) are designed with robust cybersecurity controls, and other related GenAI technical standards. Consult with and utilize assessment services from Information Security where appropriate.
8) **Compliance** - All existing York policies and procedures also apply to use of GenAI in University administrative or operational activities.

Assessment of Use Cases

The table below outlines use cases and examples to help guide judgement of what scenarios would or would not be permissible for use of GenAI in University administrative or operational activities. The University will continue to develop these use cases and assessment methods.

Category	Use Cases	Examples
Generally Permissible Use Cases	Uses that do not involve confidential or regulated information (including personal information) in accordance with the University's Information Classification Guidelines, and where output will not be used in major business decisions.	Conducting high-level background research into a non-sensitive topic. Automation tasks that do not involve sensitive or confidential information.
Use Cases That Require Oversight	Uses that involve outward-facing information or output. Uses that will be used in strategic decision-making. Generating code that will be used with University systems or data.	Text generated for websites or email communication. Chatbot-type assistance to help navigate University processes. Generating and summarizing meeting transcripts, email messages, and associated action items. Translation of business rules from code within legacy systems.
Not Permissible	Uses that provide expert or critical decision-making without human oversight. Uses that enable impersonation of a human or identifiable individuals. Any use of GenAI not in compliance with York University policies, procedures, standards, and guidelines.	Interpreting vendor contracts. Guidance related to business decisions or to create legal or policy documents. Assessment and decisions about individuals based on employee or student data.

For assistance with assessment of specific use cases, contact Information Security at infosec@yorku.ca to initiate an assessment process.

6. Information on Authorized Generative AI tools

For a current list of available GenAI tools that York University has authorized for use in University administrative or operational activities, see http://uit.yorku.ca/ai.

Related policies, procedures and guidelines:	Information Security Policy Information Classification Guidelines Data Governance Policy Records and Information Management (Policy)