PRINCIPLES FOR THE USE OF GENERATIVE AI TOOLS

BACKGROUND AND PURPOSE

Generative artificial intelligence (AI) is a type of artificial intelligence technology that can generate content at the request of a user, including audio, code, images, text, music and video based on data on which it has been trained. UBC recognizes the opportunities and transformative potential that generative AI tools represent - to foster innovation in all aspects of academic work, and to enable better experiences for students, staff and faculty, along with time-saving efficiencies in administration. UBC also recognizes that generative AI is a tool to assist in our tasks, not a replacement for human creativity and judgment.

UBC encourages experimentation and use ***within the boundaries of ethical and responsible use***. The Principles below provide direction for the UBC community on using generative AI responsibly for their administrative work. Additional guidelines apply for academic use. Using AI tools ethically and responsibly means being aware of, avoiding, and mitigating the risks.

These Principles outline the general risks of the use of generative AI tools and offer guidance for mitigation and avoidance. For cautions and strategies specific to research or teaching and learning, please visit academicintegrity.ubc.ca, the UBC Library at guides.library.ubc.ca/GenAI/learning-research or ai.ctlt.ubc.ca/ (from the CTL at UBCO and the CTLT at UBCV).

Generative AI is an evolving technology with unanswered questions about its reliability, accuracy, and best-use. There are also very significant ethical concerns about the ways in which AI may perpetuate existing biases that reinforce systemic inequities or may present new challenges and barriers to decolonization, accessibility, and equity & antiracism goals. Key rightsholder groups will be engaged to apply decolonization, accessibility, equity & anti-racism lenses to enhance and/or build on these Principles.

As such, these Principles will be regularly revisited, assessed, and maintained to ensure compliance with current and emerging regulatory standards and government advice, as well as emergent knowledge about the implications and impacts on marginalized communities.

RISKS ARISING FROM THE METHODS USED WITHIN GENERATIVE AI TOOLS TO STORE DATA

Most generative AI tools store and use any data that is entered by users, meaning anything that is entered into the tool may be inappropriately exposed to third parties, including any proprietary material entered (i.e., intellectual property or material deemed for internal use only), and any confidential or personal information entered about people. While it is possible and recommended to adjust the settings in some tools to disable the use of entered data to train the model, it is not certain that these measures mitigate the risks described above. There are currently no verifiable data privacy assurances or protections regarding confidential enterprise information associated with many of these tools unless they have been reviewed and verified as part of UBC's Privacy Impact Assessment process.

RISKS ARISING FROM THE RESULTS GENERATIVE AI TOOLS PRODUCE

Generative AI tools produce results based on complex statistical analysis of an enormous body of training data gathered from publicly available sources. These analyses, at present, may not correct for bias or check for correctness, or may overcorrect for bias, and they may seem extremely believable while being inaccurate. Anything generated by a generative AI tool is potentially duplicated from sources that were not intended or licensed for copying, which introduces a level of risk related to copyright infringement. There is also a general risk to data security that could leave UBC's systems vulnerable to security breaches (i.e., information security risk) if confidential information such as passwords, architectural configuration, or user data is entered, or even code generated that results in lower security.

PRINCIPLES FOR MITIGATING RISKS

- **Understanding and Remaining Current with Generative AI**: Prior to using generative AI, take steps to learn about the tool's strengths and limitations. Read all terms of use to understand privacy, security, and copyright implications. UBC's LinkedIn learning offers an array of free courses on how to best use generative AI. Generative AI is a rapidly evolving field, so if using these tools regularly, make sure you stay up to date on the latest advancements, use cases, and best practices in AI to harness its potential to the fullest. When in doubt, do not hesitate to ask for help or further clarification on the use of generative AI. We are all learning, and open dialogue will ensure we utilize the innovation of generative AI in a balanced and responsible manner.

- **Appropriate and Responsible Use:** Ensure it is appropriate to use generative AI tools in your administrative work and ensure that if you are using a tool for UBC purposes, that you undertake the necessary approvals, and security and privacy reviews via the Privacy Impact Assessment process if required.

- **Accountability for Results:** Ensuring the accuracy and appropriateness of generative AI results is the responsibility of the user. While AI can aid in generating content, the final communication should be reviewed for accuracy and remain in keeping with any relevant or applicable UBC policies and guidelines. Remember to attribute sources when appropriate (see Plagiarism Risk Mitigation).

- **Privacy Risk Mitigation:** Do not enter personal information into any generative AI tool that has not been through UBC's FIPPA compliance assessment (Privacy Impact Assessment or PIA), as to do so may be a breach of privacy. Personal information includes names, personal contact information, student numbers, academic history, etc. The guidance for personal information with respect to generative AI tools is the same as for any other toolset that has not undergone a PIA.

- **Confidentiality of UBC Data:** Do not enter any content into a generative AI tool that has not been assessed via UBC's PIA process or that you would not be able to place publicly on the internet for free use. This includes any content that is not intended for public release (e.g., research results before they are published), or content that was created by others including students (e.g., student essay submissions). Entering confidential content into a non-PIA assessed generative AI tool may expose that content to third parties who are not authorized to see or use it.

- **Ownership of Original, Generated Content:** Generative AI tools may have varying policies on ownership and licensing of generated content. Some tools might grant you full ownership, while others may retain certain rights. Before using a generative AI tool, read the terms of use, and fully understand how material that has been generated can be used for personal or enterprise use and where necessary ensure the appropriate licence is purchased, with approval as required.

- **Copyright Infringement Risk Mitigation**: Models may be trained on intellectual assets that are copyrighted and so may inadvertently generate content that infringes upon existing intellectual property rights. Though generative AI tools seem to be providing original responses, they may be quoting near directly from sources in their training set. Using or reproducing copyrighted outputs without a license presents a legal risk. Mitigation strategies include using proper attribution, checking for originality, or using copyright-compliant tools. Likewise, your own intellectual property may be compromised or used without your permission if entered into a tool. For example, entering your original writing into the tool may result in the tool using your writing as an original response for another user.

- **Plagiarism Risk Mitigation:** Plagiarism, an academic risk as opposed to legal risk, refers to the act of presenting someone else's work or ideas as one's own without proper attribution, regardless of whether the content is protected by copyright. It is recommended to adhere to guides.library.ubc.ca/GenAI/cite for citing generative AI use. Use citation/quotation practices as you would if you were referring to any online resource. Also consider searching for phrases from generated results to try to identify and credit original sources. If imagery has been created or modified using AI, it can be credited in much the same way as photo credits, for example, "Photo illustration: [insert name of tool/UBC]".

- **Information Security Risk Mitigation:** Ensure the use of generative AI complies with other UBC Policies such as Information Systems Policy SC 14: Acceptable Use and Security of UBC Electronic Information and Systems, including the Information Security Standards. If non-UBC systems are being used for UBC business, ensure compliance with the ISS: SC14 - *4.1 - To maintain the security of UBC electronic information, users intending to conduct University business using systems other than UBC systems must do so in accordance with the Information Security Standards*. The extent to which generative AI can be weaponized by threats and malicious exploits is unknown and there is a real and significant risk of increased cyber and fraud attacks, such as threat actors who use deep fakes for social engineering or exploiting personnel.

- **Mitigating the Risk of Reproducing Cultural Bias and Systemic Inequities:** Results produced by generative AI reflect society's gender, culture, and other biases present on the internet. Over-reliance on generated output may result in inappropriate differential treatment and serious consequences for groups of individuals and/or their human rights. A careful review of any results produced by generative AI for bias is necessary, before use. Consult the UBC Equity & Inclusion Office and/or the Indigenous Guiding Network as required.

- **Mitigating the Risk of Incorrectness:** Due to the statistical approach, generative AI tools may return results that are believable but are incorrect. Users should double check all results returned by generative AI tools for correctness. Similarly, if using generative AI tools to produce code, be sure to review the code carefully against your own tests, and test the code in a safe, quarantined environment, in case it invokes behaviours with unintended or problematic consequences.

- **Mitigating Ecological Impacts:** UBC is committed to sustainability. Generative AI tools use significant amounts of electricity. Users should consider choosing solutions and/or vendors that limit and/or reduce power consumption and leverage high-quality renewable energy to mitigate the impact on sustainability goals.