IT Generative Artificial Intelligence

Generative Artificial Intelligence Policy			
Effective Date	August 5, 2025	Policy Type	Administrative
Responsibility	Director, IT	Related Policies	IT Governance IT Acceptable Use IT Security Privacy Disclosure Records Management Data Governance
Approval Authority	Executive Council	Review Schedule	5 Years

1. Policy Statement:

Northwestern Polytechnic (NWP or institution) is committed to ensuring that Artificial Intelligence (AI) is used in a secure, legal and ethical manner. This policy outlines our approach to managing risk associated with the use of Generative Artificial Intelligence.

2. Scope:

This policy applies to all members of the NWP community that will be using Generative Artificial Intelligence, including but not limited to, faculty, staff, contractors, and vendors. Industry-tailored generative AI tools, system-integrated generative AI tools and tools that are not publicly accessible are not in scope of this policy.

3. Reason for Policy:

NWP welcomes innovative and reliable uses of generative AI that respect human rights and democratic values. While the institution adopts technologies that support our operations, we understand that there are risks and limitations of generative AI and want to ensure responsible use. The following principles guide our approach to generative AI adoption and use: compliance with legal and regulatory requirements, protection of data privacy and security, ethical use, and employing human oversight when using generative AI.

4. Definitions:

4.1 Artificial Intelligence: a broad term used to describe an engineered system where machines learn from experience, adjusting to new inputs, and potentially performing tasks previously done by humans. More specifically, it is a field of computer science dedicated to simulating intelligent behavior in computers.

4.2 Confidential Information: Applies to data and information that, if compromised, could cause serious harm to an individual, organization or government.

4.3 Generative Artificial Intelligence: A field of AI that uses machine learning models trained on large data sets to create new content, such as written text, code, images, audio, simulations, and videos. These models can generate novel outputs based on input data or user prompts.

4.4 Generative Artificial Intelligence Tool: An AI tool is a software application that uses machine learning models trained on large data sets to create new content, such as written text, code, images, audio, simulations, and videos.

4.5 Industry-Tailored Generative Artificial Intelligence: Third-party vendor products that incorporate large language model products into an application, software, or content product, like Scite or Casetext's CoCounsel.

4.6 Input / Output: A general term for the equipment that is used to communicate with a computer as well as the data involved in the communications.

4.7 Protected Information: Applies to data and information that, if compromised, could cause injury to an individual, organization or government.

4.8 Publicly Available Generative Artificial Intelligence: Publicly available, large language model products, like OpenAI's ChatGPT or DALL-E.

4.9 Public Information: Applies to data and information that, if compromised, will not result in injury to individuals, governments, or to private sector institutions. Classifying data or information as Public does not require that it be made available to the public.

4.10 Restricted Information: Applies to data and information that, if compromised, could cause extremely grave injury to an individual, organization or government.

4.11 System-Integrated Generative Artificial Intelligence: Open-source of proprietary, licensable language model technology which requires information technology support to integrate it into enterprise systems.

5. The Policy:

5.1 Acceptable Use of Generative AI for Employees and Contractors

5.1.1 According to the institution's Data Classification Standard, employees must only enter information that is classified as public when using publicly accessible generative AI tools. Public information examples include published annual reports, news releases, business contact details, institution policies, published research, job postings, and publicly shared newsletters.

5.1.2 Generative AI tool use at NWP, if it meets the requirements as set by this policy, may include the following: natural language processing (e.g., creating, searching for, summarizing, classifying, extracting or translating text); computer vision (e.g., creating, classifying audio or video or images) or software engineering (e.g., creating or analyzing code).

5.1.3 All generative AI tools must be reviewed by the institution to ensure that the software meets all necessary security, privacy, and accessibility requirements: this applies to downloadable software, software as a service, web-based services, browser plug-ins, and smartphone apps. Plainly, to use a generative AI tool, it must have passed through the institution's software acquisition process.

Notwithstanding the above, use of generative AI tools that are incorporated into publicly available products that do not require the user to form an account, like internet search engines, are not required to go through the software acquisition process.

5.1.4 When producing work products with generative AI tools, NWP's email addresses, credentials, and phone numbers must be used when forming an account with that tool.

5.1.5 It is essential to have human oversight when AI generates content, as AI results may include inaccuracies or biases from the data they were trained on, which may not align with NWP's commitment to equity, diversity, and inclusion. Generative AI tools may produce errors or favor specific groups. Therefore, employees or contractors must carefully review AI-generated content for accuracy, appropriateness, and bias before using it for work purposes.

Generative AI outputs should not be assumed true, reliable, or ethical. They should not be used verbatim, treated as the sole source, issued as official statements, solely relied on for making final decisions, or used to impersonate individuals or organizations.

5.1.6 Content created with generative AI must be attributed and cited properly, following an appropriate style guide like APA.

5.1.7 NWP will ensure that contractors disclose in their contracts the use of generative AI tools. The institution may prohibit contractors from using NWP protected, confidential, or restricted data in generative AI tools.

5.1.8 Vendors must disclose the use of generative AI when used to produce intellectual property for the institution.

5.1.9 In all cases, use should be consistent with the IT Acceptable Use Policy.

5.2 Prohibited Use

5.2.1 Employees shall not enter protected, confidential, or restricted information of the institution into generative AI tools.

NWP strives to respect the rights of content creators and copyright owners. If entering content into a generative AI tool would violate the copyright owner's rights and the Canadian Copyright Act, then that content must not be entered into the generative AI tool. Employees should contact the Copyright Officer if they need help determining what material is copyright protected.

5.2.2 As per the Data Classification Standard, the institution's protected, confidential, and restricted information shall not be input into any generative AI tools. This includes but is not limited to, identifying student information subject to the Freedom of Information and Protection of Privacy Act, identifying health information, and trade secret information.

5.2.3 Similarly, generative AI tools must not be used to generate outputs that are considered non-public. Examples include but are not limited to generating legal analysis or advice, recruitment, personnel, or disciplinary decision-making.

5.2.4 Generative AI outputs may be used to support a decision made by a Northwestern Polytechnic employee. However, generative AI outputs shall not be used to make the decision for the employee. Generative AI tools will not replace the judgement required from human decision-makers.

5.3 Compliance and Accountability

Employees must be aware of and uphold their obligations under this policy, and any associated policies and procedures, standards, or guidelines. Non-compliance with this policy may result in disciplinary action from the institution.

Stakeholder	Responsibilities
Executive Council	• Approve and formally support the Policy.
Vice-President, Administration	• Review and formally support the Policy. • Ensure alignment of this policy to the Organizational Strategic Plan
IT Director	• Develop and maintain the Policy. • Align the Policy to the IT Strategic Plan and IT procedures
IT Management	• Maintain IT procedures
IT Team Members	• Implement the IT procedures

Stakeholder	Responsibilities
Users	• Contact the IT Help Desk for any problem, issue or needs related to the technology. When a problem, issue or needs cannot be addressed by the IT Help Desk, they contact their supervisor or representative. • Contact their supervisor or manager for any request related to access rights and privileges or needs for IT equipment. • Contact their supervisor or manager with any request to change the existing technology. • Backup their personal files stored locally on computers and mobile devices.

5.1. Exceptions to this policy must be approved by the Director, Information Technology

6. Revision History

6.1. Approved by Executive Council August 2025