Procedure

Procedure Name	***Responsible Use of Artificial Intelligence***		
Procedure #	IT 4.6	Parent Policy	IT 4.0 Digital Security Policy
Policy Owner	Vice President Administration & CFO	Effective Date	January 16, 2025
Procedure Owner	AVP Information Technology & CIO	Next Review Date	January 2030
Approved by	AVP Information Technology & CIO	Approval Date	January 16, 2025

1.0 Purpose/ Background

NAIT recognizes the transformative potential of artificial intelligence (AI) to enhance the Institute's operations, products, and services. This procedure provides a framework for engagement with AI and outlines NAIT's commitment to responsible, ethical, and secure use of artificial intelligence for administrative use within NAIT.

NAIT recognizes that decisions involving artificial intelligence, and the data used therein are nuanced and can change depending on context and time and that assessing the responsible use of AI and data is an ongoing process.

2.0 Definitions

Term	Definition
Artificial Intelligence (AI)	A branch of computer science focused on creating systems or machines that can perform tasks that typically require human intelligence.
Generative AI	A type of artificial intelligence capable of creating new content, such as text, images, music, and other forms of media.
Confidential Data	Any sensitive data intended for use only by specific groups of employees. Unauthorized disclosure, alteration, loss, or destruction of this data would seriously impact NAIT's reputation and possibly undermine public trust in the Institute. This includes personally identifiable information not publicly available.
Data	Information in a specific representation, usually as a sequence of symbols that have meaning.
Hallucination	An instance where an artificial intelligence system generates false or misleading information.
Need-to-know	The need-to-know principle (or the principle of least privilege) states that a user shall only have access to the data required for their job function, regardless of their leadership level.
Protected Data	Data available to staff, contractors, subcontractors, agents, and students at the Institute with a need-to-know for business operations.
Public Data	Data available to the public, as well as staff, contractors, subcontractors, agents, or students at the Institute.

Restricted Data	Any extremely sensitive data whose access is restricted to a limited set of named individuals. Explicit approval of the data trustee is required to release this information, even to those with a need-to-know. Unauthorized disclosure, alteration, loss, or destruction of this data could risk the health, safety, privacy, or reputation of an individual, members of the public, or NAIT students or staff
Sanitized Data	Data that has been processed to remove or obfuscate sensitive, personal, confidential, or NAIT proprietary information

3.0 Procedures

3.1 Generative AI may be used if NAIT's procedures and guidelines for data classification, data sharing, and data quality are followed.

3.2 Employees may only input data classified as public into AI systems which are available for general use over the Internet.

3.3 Data classified as protected may be used in public AI systems only if the data has been sanitized.

3.4 Any data classified as confidential or restricted may be used in public AI systems after formal approval from the data trustee. Before granting approval, the data trustee should ensure that such use will not violate the terms of any agreements to which NAIT is a party or any applicable laws, including privacy laws. General Counsel Services should be consulted when there is uncertainty regarding legal compliance.

3.5 Use of generative AI systems for NAIT business must be lawful and not jeopardize NAIT's professional reputation or brand.

3.6 Individuals are accountable for issues that arise from their elective use of generative AI in business processes. This includes copyright violations, exposure of unsanitized protected data, confidential or restricted data, poor data quality, and any bias or discrimination in outputs.

3.7 Employees must not violate privacy or data protection regulations or legislation when using generative AI systems.

3.8 NAIT will transparently communicate the use of AI in internal operations if AI systems support processes or decision-making.

3.9 Data used to train a NAIT-developed AI model must be classified as restricted and encrypted when stored or in transit to protect it from being stolen by an individual(s) with bad intentions.

3.10 Specific knowledge and details about how a NAIT-developed AI model has been trained and how it works must be kept strictly confidential, with access to such information being granted on a need-to-know basis.

3.11 All suspected or confirmed cases of compromised data confidentiality involving an AI system must be reported to IT Security using the channels defined in IT 4.4 Digital Security Incident Response Procedure.

3.12 Only AI tools that protect NAIT's ownership of data input and output are allowed, ensuring NAIT data is not used to train external AI models or shared outside the organization.

3.13 All AI-generated outputs used for NAIT business are subject to human oversight to mitigate potential biases related to equity, diversity, and inclusion (EDI), or AI-generated inaccuracies such as hallucinations.

4.0 Exceptions to the Procedure

Exceptions to this procedure must be documented and formally approved by the Procedure Owner.

Procedure exceptions must include:

- The nature of the exception
- A reasonable explanation for why the procedure exception is required
- Confirmation that the exception aligns with the general principles
- Any risks created by the procedure exception and how they will be managed.

5.0 Related Documentation

- NIST AI 100-1 – Artificial Intelligence Risk Management Framework 1.0
- NIST AI Risk Management Playbook
- Privacy Act / Personal Information Protection and Electronic Documents Act (PIPEDA)
- Freedom of Information and Protection of Privacy Act
- Copyright Act of Canada

Document History

Date	*Action/ Change*