SAIT

AD.1.1.2
PRIVACY IMPACT ASSESSMENT

Section:	Administration (AD)
Subject:	Organization of the Institution
Legislation:	*Access to Information Act (*RSA 2024, c A-1.4); *Post-Secondary Learning Act* (SA 2003 cP-19.5); *Protection of Privacy Act* (SA 2024, c P-28.5); *Protection of Privacy (Ministerial) Regulation (143/2025).*
Effective:	May 21, 2026
Revision:	

PROCEDURE

APPROVED: _____

President and CEO

POLICY

The policy of the Board of Governors is to comply with the *Protection of Privacy Act* (POPA) and the *Access to Information Act* (ATIA).

PROCEDURE

DEFINITIONS

Data matching — Refers to the linking of personal information across two or more databases, or other electronic data sources, to generate data derived from personal information. Such data identifies any individual whose personal information was utilized in the data matching process.

High-sensitivity information — Personal information related to biometric information, financial information, or personal information respecting a minor, senior or vulnerable individual.

Non-personal data — Data, including data derived from personal information, that has been generated, modified or anonymized so that it does not identify any individual, and includes synthetic data and any other type of non-personal data identified in the *Protection of Privacy (Ministerial) Regulation*.

Personal information	Recorded information about an identifiable individual and includes, but is not limited to, name, residential address and phone number, personal email address, sex (sex assigned at birth), age, gender identity, title, pronouns, sexual orientation, marital or family status, religious affiliation, Indigeneity, ethnicity, disability status, languages spoken, immigration status, identification number, education and employment history, health information including documentation of approved accommodations for physical or mental disability, an individual's personal views or opinions and information about an individual's financial matters.
Privacy impact assessment	A document used for information systems, administrative practices and policy proposals that helps to identify and address potential privacy risks that relate to the collection, use or disclosure of individually identifying personal or health information.

GOVERNING PRINCIPLES

1. SAIT collects, uses and discloses personal information and non-personal data only where it relates directly to and is necessary for an operating program or activity.

2. SAIT shall conduct privacy impact assessments (PIA) to ensure that personal information and non-personal data is managed in compliance with the *Protection of Privacy Act* (POPA) and *POPA Ministerial Regulation*. Refer to AD.1.1.1 Schedule D Non-Personal Data and Data Matching Guidelines (under development), and Associated Document to procedure AD.1.1.1 Personal Information, for more information.

3. SAIT is committed to safeguarding personal information in its custody or control by taking all reasonable precautions and security measures to mitigate against such risks such as unauthorized access, disclosure, disposal or destruction.

PROCEDURE

A. Risk Review and Coordination

1. Schools/departments are responsible for identifying initiatives and projects that may require a privacy impact assessment (PIA) based on the type of information or data that will be accessed and/or utilized, including personal information and non-personal

data, as outlined in section B of this procedure. SAIT employees involved in such initiatives and projects (requestors) are responsible for initiating the required privacy review and/or PIA request through SAIT's official request and workflow system (ServiceNOW). Privacy review informs decision-making however; the completion of a privacy review and/or PIA does not constitute approval of the initiative.

2. The PIA intake process is embedded within the Third-Party Risk and Privacy Assessment Request form, in coordination with SAIT's established technology vendor and procurement workflows. Refer to procedures AD.2.10.2 Technology Vendor Risk Assessment and FN.7.1.3 Procurement for more information. All PIA requests and related questions must be submitted in accordance with these procedures and tracked through ServiceNOW.

3. The Access and Privacy Unit, Office of General Counsel, shall conduct a PIA as required by the *POPA*, which may include but is not limited to, when the school/department is implementing a new system or application or planning a substantial change to an existing system/application.

4. Third-party technology risk reviews are managed by the Information Security Office, Information Technology Services, with privacy risks reviewed by the Access and Privacy Unit, Office of General Counsel.

B. Assessment

1. The Access and Privacy Unit, Office of General Counsel will assess Third-Party Risk and Privacy Assessment requests and, if necessary, prepare and submit a PIA to the Information and Privacy Commissioner (OIPC) for the following types of initiatives and projects:

   a) A practice, program, project or service that will collect, use or disclose personal information considered to be of high sensitivity;

   b) A practice, program, project or service that will involve data matching between 2 or more public bodies;

   c) A practice, program, project or service that will involve the development or use of innovative technology.

   d) A practice, program, project or service that will involve the personal information of a significant percentage of the SAIT community; or

PROCEDURE

e) A practice, program, project or service which is part of a common or integrated program or service.

2. Initiatives and projects involving the creation of non-personal data may be evaluated for privacy risks, where the data is de-identified, anonymized or otherwise does not contain personal information, in accordance with AD.1.1.1 Schedule D Non-Personal Data and Data Matching Guidelines (under development), and Associated Document to procedure AD.1.1.1 Personal Information,

3. In some cases, SAIT may conduct a proactive PIA where the *POPA* does not require regulatory filing with the OIPC.

C. Implementation and Ongoing Review

1. Requestors will implement approved mitigation measures and a PIA may be revisited or amended, if the scope changes or if new data elements are introduced. The school/department responsible for the initial PIA must notify the Access and Privacy Unit, Office of General Counsel, when such changes occur. A new Third Party Risk and Privacy Assessment Request form submission may be required.

2. The PIA process supports risk identification and SAIT's Privacy Incident Response through identifying privacy risks and safeguards. Refer to procedure AD.1.1.3 Privacy Incident Response.

D. Non-compliance

1. Failure to comply may result in disciplinary hearings under procedure HR.4.4.1 Corrective and Disciplinary Action and/or legal or regulatory penalties under the *Protection of Privacy Act* (POPA).

POLICY/PROCEDURE REFERENCE

AD.1.1	Privacy policy
AD.1.1.1	Personal Information procedure
AD.1.1.3	Privacy Incident Response procedure
AD.1.1.4	Privacy Complaints procedure

PROCEDURE