SAIT

Southern Alberta Institute of Technology

Privacy Management Program

(PMP)

A framework of policies, procedures, responsibilities and roles ensuring SAIT's compliance with Alberta's Protection of Privacy Act (POPA).

June 2026

Table of Contents

Purpose

The Southern Alberta Institute of Technology's Privacy Management Program (PMP) establishes the framework of policies, procedures, responsibilities and roles that ensure SAIT's compliance with Alberta's *Protection of Privacy Act (POPA).* The development of this PMP ensures the privacy protection of personal information that is in SAIT's custody or under SAIT's control. SAIT's polices and procedures are publicly available on its website at sait.ca and are listed at the end of this PMP.

Commitment to Privacy Protection

SAIT protects the privacy of students, employees (which includes all persons whom SAIT engages to carry out its operations – staff, contractors and volunteers) and individuals whose personal information SAIT collects, uses, shares, and retains. It expects all employees to follow responsible information management practices to ensure SAIT fully complies with its obligations under the *POPA* and other applicable laws. SAIT's Access and Privacy Officer will annually review this PMP to ensure it remains effective and compliant with the *POPA*.

Accountability

SAIT's President and CEO is the head of SAIT for the purposes of the Protection of Privacy Act and the Access to Information Act and is responsible for the overall implementation of the PMP. Under this legislation, SAIT's head may designate other SAIT employees to carry out specific functions and duties. SAIT's Access and Privacy Officer has been designated to manage the overall implementation of the PMP and for serving as a liaison for privacy concerns. Contact information for SAIT's Access and Privacy Officer is provided at the end of this PMP.

Expectations of SAIT Employees

SAIT employees are responsible for:

- Familiarizing themselves with the requirements of the *POPA*, including participating in mandatory privacy training initiatives:
  - New employees must complete mandatory privacy training as part of their formal onboarding at SAIT, offered internally by SAIT's Human Resources Department
  - Current employees must complete mandatory privacy training on an annual basis, offered internally by SAIT's Human Resources Department
- Following responsible information management practices to ensure SAIT collects, uses, and discloses personal information in compliance with the *POPA* and other applicable laws.
- Following SAIT procedures to facilitate the appropriate release of records within its custody or control in response to access to information requests that SAIT receives under the *ATIA.*
- Protecting personal information against unauthorized collection, use, access, and disclosure. This includes, for instance, limiting the sharing of sensitive personal information on a need-to-know basis.
- Reporting privacy incidents in accordance with SAIT's procedures.

Key Takeaway

Every SAIT employee – staff, contractor, or volunteer – shares responsibility for protecting personal information and complying with the POPA.

SAIT's Collection, Use, Retention and Reporting of Personal Information

What is personal information?

Personal information is recorded information about an identifiable individual. It includes many different types of information, including but not limited to an individual's:

- Age or date of birth
- Educational, financial, employment, or criminal history
- Fingerprints, blood type, genetic or biometric information, physical or mental health care information or history
- Gender identity, sex, sexual orientation, marital or family status
- Identifying number (e.g. Social Insurance Number, SAIT student number), symbol (e.g. signature)
- Name, phone number, address, or business phone and address
- Personal views or opinions, unless about someone else
- Photograph, image, or audio recording of their voice
- Race, national or ethnic origin, colour
- Religious or political beliefs or associations

This list is illustrative, not exhaustive. If information identifies, or could, identify an individual - treat it as personal information.

Why does SAIT collect students' personal information?

In the course of carrying out its programs and activities, SAIT collects personal information of its students for many purposes, including, for instance:

- Accommodating students with special needs
- Communicating with students and responding to inquiries or complaints
- Ensuring compliance with applicable bylaws, policies, and other laws
- Investigating and responding to accidents, safety events, academic or non-academic student misconduct or similar incidents
- Making required reports and filings to the Government of Alberta's Ministry of Advanced Education
- Preparing and providing assessments of student performance
- Providing and delivering educational programs and services
- Registering, enrolling and transferring students
- Supervising and ensuring the safety of students
- Other purposes as set out in SAIT's procedures or as required under applicable laws and regulations.

All collection occurs under the authority of the *Protection of Privacy Act* (POPA) and in accordance with SAIT's supporting policies and procedures.

Why does SAIT collect employees' personal information?

In the course of carrying out its employment activities, SAIT collects the personal information of prospective, current, and former employees for many purposes, including, for instance:

- Administering employment compensation/benefits
- Communicating with authorized union representatives
- Ensuring compliance with applicable bylaws, policies, and other laws
- Evaluating performance and managing disciplinary incidents
- Hiring and recruiting
- Investigating and responding to accidents, safety events, employee misconduct situations, or similar incidents
- Managing and administering employment relationships
- Supervising and ensuring the safety of SAIT's employees
- Other purposes as set out in SAIT's procedures or as required under applicable laws and regulations.

Employee means "all persons whom SAIT engages to carry out its operations – staff, contractors and volunteers".

Principles for collecting, using, retaining and disclosing personal information

- SAIT limits the personal information it collects to what is necessary in order for SAIT to carry out its programs and activities or for other purposes authorized by the *POPA*.
- SAIT collects personal information by fair, lawful and transparent means, including collecting personal information directly from the individual except where otherwise authorized by the *POPA*.
- SAIT informs individuals from whom it collects personal information about the purposes for which the information is being collected and the legal authority for collecting it and provides the contact information for a SAIT employee who can answer questions about the collection and use of that information. It does this at or before the time it collects the information (unless otherwise authorized by the *POPA*).
- SAIT only uses or discloses personal information for the purpose for which it was collected, except with the individual's written consent or as otherwise required or permitted by the *POPA* or other laws. Electronic consent, including the collection of an electronic signature , is a valid and acceptable form of consent for these purposes and shall be retained and authenticated in the same manner as written consent.
- SAIT only asks for oral consent to use or disclose personal information in extenuating circumstances, when it is unfeasible for SAIT to obtain written or electronic consent. SAIT will create a record of the date, time, and method that oral consent was obtained.
- SAIT ensures it has reasonable security safeguards (physical, organizational and electronic) in place to protect the personal information it collects and assigns a security classification to information appropriate to the sensitivity of that information.
- SAIT retains personal information only as long as necessary to meet SAIT's operational, instruction, financial and/or legal needs. It securely destroys personal information that it no longer needs to retain, in accordance with SAIT's record retention procedures.
- SAIT may use personal information already in its custody or control to create non-personal data in accordance with SAIT's procedures and generally accepted best practices.
- SAIT makes reasonable efforts to ensure the accuracy of personal information that it collects. Individuals have the right to request the correction of their personal information, and SAIT will respond to those requests in accordance with the *POPA.* Nothing in this section limits the ability of an individual to make an informal request to correct their personal information through a SAIT school or department that retains and manages that information.

Privacy Complaints

Privacy complaints about SAIT's personal information management practices should be directed to the Access and Privacy Advisor at access.privacy@sait.ca. SAIT will respond to all privacy complaints in writing, on a case-by-case basis.

Privacy Impact Assessments (PIA)

A PIA is a step-by-step review process that is required under the *POPA* and that helps a public body such as SAIT to identify and mitigate any privacy risks involved in a particular initiative. SAIT will complete a PIA when SAIT proposes to create a new administrative practice, program, project, service, or technology initiative or to make a substantial change to an existing administrative practice, program, project, service, or technology initiative involving the use or storage of personal information (including software, web-based tools, etc.).

A PIA is typically completed with the help of the individuals working on the initiative. Once a PIA is completed after an internal review, it will be stored in a central location accessible by employees. Should there be any changes to the technology initiative after the PIA is completed, a reassessment will be carried out to determine if any changes will need to be made. Note that in some situations, SAIT will submit a PIA to the Office of the Privacy and Information Commissioner for its review.

When is a PIA required?

New or substantially changed administrative practice, program, project, service, or technology initiative that uses or stores personal information.

Privacy Incidents

A privacy incident involves the loss or unauthorized access of personal information, or the unauthorized disclosure of personal information. SAIT has processes in place to address a privacy incident, including providing written notices to affected individuals and, in situations involving a real risk of significant harm to affected individuals, reporting the incident to the Office of the Information and Privacy Commissioner and to the Alberta Government's Minister of Technology and Innovation. SAIT investigates each incident and implements measures to prevent future similar occurrences.

Information Security

SAIT utilizes end-point detection and response as well as security information and event management systems to proactively monitor and defend against external attempts to access personal information. Internal audit logging is also utilized, to the extent available, to protect personal information from unauthorized access, use, and disclosure. SAIT will endeavor to review and assess new ITS security technology as it becomes available to determine the feasibility of their integration into current practices to better defend SAITs networks and systems.

Artificial Intelligence and Automated Decision Making

SAIT may utilize automated systems and artificial intelligence to the extent allowable in accordance with SAIT's artificial intelligence and information technology policies and procedures. When an individual's personal information may be input into an automated system to generate content, make decisions, recommendations, or predictions, the individual must be made aware of this at the time of collection.

Formal Access to Information

SAIT supports appropriate transparency and accountability in its operations by making information available to the public as permitted or required under the *ATIA.* SAIT recognizes that individuals may make request for access to records – including a right to access their own personal information - within SAIT's custody or control and will respond to such requests in accordance with the *ATIA* and its own procedures. The Access and Privacy Advisor is responsible for processing formal requests made under the *ATIA.*

Policies and Procedures

Privacy

AD.1.1 Privacy Policy
AD.1.1.1 Personal Information Procedure
- Schedule A - Student Information Waiver
- Schedule B - Disclosure of Student Information in an Emergency
- Schedule C - Security Classification Guideline
- Schedule D - Non-Personal Data and Data Matching Guidelines *(under development)*

AD.1.1.2 Privacy Impact Assessment Procedure
AD.1.1.3 Privacy Incident Response Procedure
AD.1.1.4 Privacy Complaints Procedure

Access to Information

AD.3.4 Access to Information Policy
AD.3.4.1 Access to Information Procedure
- Schedule A - Access to Information Request Form

Anti-Spam

AD.2.12 Compliance with Canada's Anti-Spam Legislation Policy
AD.2.12.1 Compliance with Canada's Anti-Spam Legislation Procedure
- Schedule A - Applying Canada's Anti-Spam Legislation to SAIT Activities

Data Governance

AD.3.3 Data Governance Policy
AD.3.3.1 Data Governance Procedure
AD.3.3.2 Research Data Management

Information Security and Artificial Intelligence

AD.2.15 Acceptable Use of Computing and Information and Technology Resources
AD.2.15.1 Acceptable Use of Computing and Information and Technology Resources Procedure
AD.2.15.2 Student Digital Identity Management Procedure
AD.2.15.3 Use of Artificial Intelligence Technologies at SAIT Procedure
- Schedule A - Use of Artificial Intelligence in Teaching and Learning
- Schedule B - Artificial Intelligence Committee Terms of Reference

Records Management

AD.3.2 Records Management Policy
AD.3.2.1 Records Management Procedure
AD.3.2.2 Transitory Records Procedure
- Schedule A - Official vs. Transitory Records
- Schedule B - Transitory Records Destruction

AD.3.2.3 Retention and Disposition Schedule Procedure

For a full list of SAIT's policies and procedures refer to: SAIT.ca

Contact Information

For questions or inquiries regarding the PMP, please contact:

Jocelyn Baxter, Access and Privacy Advisor

Access & Privacy Unit

Office of General Counsel

Southern Alberta Institute of Technology (SAIT)

Telephone: 403.284.8777

Email: access.privacy@sait.ca

This Privacy Management Program is reviewed annually by SAIT's Access and Privacy Unit to ensure it remains effective and compliant with Alberta's Protection of Privacy Act.