SAIT

	AD.1.1.1 **PERSONAL INFORMATION**
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:	December 8, 2006
Revision:	September 1, 2016 (reformatted); April 10, 2024; May 21, 2026

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

Artificial intelligence (AI) Artificial intelligence is the ability of machines, particularly computer systems, to perform tasks that typically require human intelligence. This includes the ability to reason, discover meaning, generalize or learn from past experiences. AI encompasses a range of technologies and methods, including machine learning, neural networks, deep learning, natural language processing and robotics, enabling machines to understand and process language, recognize patterns, solve problems, make decisions, communicate with other AI technologies and to perform physical tasks like navigating environments.

Automated system Any system, software, or process that uses computation as whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or otherwise interact with individuals and/or

	communities. Automated systems include but are not limited to systems derived from machine learning, statistics, or other data processing or artificial intelligence techniques, and exclude passive computing infrastructure.
Contractor	An individual or company contracted by SAIT to perform services or work for SAIT.
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.
Employee	A person employed on SAIT's payroll, whether paid by annual salary or hourly wage and contractors.
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.
Personal information bank	A collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

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.
Record	Information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business. A record may be in any form. This includes notes, images, audio-visual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records.
Student	A person who has a SAIT ID number and a student record.

GOVERNING PRINCIPLES

1. SAIT is committed to protecting the confidentiality and privacy of the personal information within the custody or under the control of SAIT.

2. This procedure applies to all recorded personal information that is necessary for the conduct of SAIT's operating programs or activities, regardless of medium or format.

3. All employees, regardless of work location, are responsible for protecting the privacy of personal information and confidential records by complying with policy AD.1.1 Privacy and its accompanying procedures.

4. Contractors must either adopt this procedure or implement their own privacy policies that meet or exceed its standards for themselves and their subcontractors while performing work on SAIT's behalf or at any SAIT campus or workplace.

5. The right to access and correct personal information is governed by the *Access to Information Act* (ATIA) and must comply with policy AD.3.4 Access to Information and its accompanying procedures.

6. The release of personal information to third parties is prohibited without the consent of the individual, unless otherwise stated in SAIT policy or procedure, or as required by law.

PROCEDURE

SAIT

PROCEDURE

A. General Guidelines

1. SAIT recognizes various types of personally identifiable information (PII) and personal data may be collectively referred to as personal information.

2. SAIT will implement reasonable security arrangements and access controls for personal information, data derived from personal information and non-personal data, appropriate to the security classification level of that information, recognizing that any unauthorized collection, use or disclosure of high-sensitivity information carries the potential risk of significant harm to individuals. Where personal information fits into more than one classification and/or when the sensitivity of the information is uncertain, the highest security classification level must be applied. Refer to Schedule C Security Classification Guideline, an Associated Document to this procedure for more information.

3. All collection, use and disclosure of personal information shall satisfy the requirements of the *Protection of Privacy Act (POPA)*, the *Access to Information Act* (ATIA) and must comply with the following:

    a) All use will be consistent with the stated purpose of collection or with consent of the individual;

    b) Disclosure shall be controlled and limited in accordance with the *POPA* and *ATIA*; and must comply with policy AD.3.4 Access to Information and its associated procedures.

    c) Personal information should only be used and/or disclosed within SAIT to those authorized and who need the information to carry out their duties or functions.

B. Collection and Use of Personal Information

1. Collection of personal information shall satisfy the requirements of the *Protection of Privacy Act* (POPA) and shall be limited to collection that is necessary for the operating program or activity of SAIT, the collection of information is authorized by an enactment under Alberta or Canada, or as otherwise prescribed by the *POPA.*

2. A collection notice is required whenever personal information is collected from an individual on behalf of SAIT, regardless of the collection method used. The notice may be delivered verbally or in writing, must be communicated in clear, plain language and

PROCEDURE

provided at or before the time of collection. Ensuring transparency is essential so that individuals are fully informed about how SAIT will use their personal information. If employees are uncertain about whether a collection notice is necessary, they are encouraged to contact access.privacy@sait.ca for further guidance.

3. The collection notice must clearly inform individuals of the following:

    a) The purpose for the collection of their personal information. The purpose needs to be clearly stated (for example, for the purpose of processing an application for admission).

    b) The legal authority for the collection. If applicable, list any other legislation or regulation that expressly authorizes the collection, including the name and relevant sections of that legislation/regulation. In accordance with *POPA*, the information being collected must relate directly to, and is necessary for, an operating program or activity of SAIT including a common or integrated program or service.

    c) Contact information for the school or department responsible for responding to inquiries regarding the collection or use of personal information must be provided, including an email address and phone number.

    d) If applicable, the intention, if any, at the time the information is collected to input that information into an automated system to generate content, make decisions, recommendations or predictions. Any statement pertaining to the use of an automated system should be limited to describing the functions performed by the system at the time the information is collected, such as generating automated responses, providing analytics, supporting service efficiency and similar activities.

    e) SAIT will collect personal information directly from the individual unless otherwise authorized under the *POPA.*

4. The use of personal information must be considered consistent with the purpose for which it was collected or compiled when the use has a reasonable and direct connection to the original purpose. Where a proposed secondary or subsequent use does not meet these conditions for a consistent purpose, SAIT will treat it as a new purpose or use and provide a new collection notice.

5. All collections of personal information must be documented in the SAIT personal information bank (PIB), which provides details of the purpose, legal authority, and categories of information collected. Access and Privacy Unit, Office of General Counsel, will maintain a PIB Directory.

C. Confidentiality of Student Information

1. The Office of the Registrar maintains student records and files, except for records and files related to academic or non-academic misconduct, which the Office of the Registrar has designated to be maintained by the Office of Community Conduct.

2. The Office of the Registrar, Associate Registrar and the Continuing Education and Professional Studies department are the SAIT authorities authorized to release a student's academic record or other personal information from their official file, unless the student has provided consent or a formal access to information request has been submitted to the Access and Privacy Unit, Office of General Counsel. Each authority will determine the legitimacy of all such requests. Urgent requests for student information based on an apparent emergency may also be handled by the Safety and Community Services department in consultation with a designated authority.

3. The student record and file consist of student personal and academic information relating to a student's education at SAIT. This permanent record includes personal information required in the administration of official student academic records and academic information such as grades, credential or transfer credit awarded and program withdrawal or expulsion. This information may also include assessments, correspondence and other information provided by the student.

4. Disclosure to other persons or agencies of any student personal information is prohibited, except as authorized elsewhere within this procedure, for the purposes provided under the *Protection of Privacy Act* (POPA) and/or with the written consent of the student. Please see Schedule A Student Information Waiver form, an Associated Document to this procedure. In particular, disclosure without statutory authority and/or consent is not permitted to:

    a) Commercial or credit agencies of any kind.

    b) Debt collectors (except as provided under *POPA*).

    c) Employers.

    d) Government or other agencies including sponsoring bodies.

    e) Legal agents (except by a court order or appropriate legislation).

    f) Other students.

    g) Parent or legal guardian, unless the student is a minor.

h) Representative of foreign states.

i) School boards, high schools and other academic institutions.

j) Any other third party not listed above.

5. Because of the relationship of those responsible for students who receive financial aid funding from the federal and provincial governments and banks, SAIT has, in specific identifiable situations, the responsibility to release information that the student would have submitted in support of an application for financial assistance to:

   a) Chartered banks with which a registered student negotiated government student loans (if specific authorization is part of the loan application documentation);

   b) Student Finance Board; and

   c) The Government of Alberta ministry responsible for post-secondary education.

6. A waiver for release of information is usually incorporated in all government student loan documents, copies of which are maintained by the Canada Student Loans Administration and agency negotiating the loan. However, the waiver varies from form to form and may or may not include non-government agencies. Information shall only be released to agencies with the student's waiver. Please see Schedule A Student Information Waiver form, an Associated Document to this procedure.

7. Except as provided for under the *Post-secondary Learning Act*, government agencies have no legal right to further information or access to student files and records without the student's written authorization. Further information will be released only on court order or subpoena.

8. External agencies providing scholarships or other direct assistance to a student may require periodic reports of the student's progress as a condition of their grants. The student, however, shall be fully informed, preferably by the external agency itself, of all such requirements, the kind of information required and the manner in which it is to be reported. It is the student's responsibility to arrange to have this information forwarded as required.

9. Disclosure of student information from other official records:

a) Access to financial assistance, academic advising, counselling, student services and disciplinary files is limited to those officials responsible for those matters and may not be released to anyone except as otherwise stated in this procedure.

b) Information about student accommodation information and documentation is kept confidential. Refer to procedure AC.3.16.1 Accommodations for Students with Disabilities.

c) The Office of the Registrar shall make routine changes in statistical information.

d) Information gathered on a student may be used for research purposes only if the data is de-identified or anonymized in accordance with the *POPA* and is used solely for the purpose for which it was obtained or compiled. When personal information is converted into non-personal data, it must be done so in accordance with Schedule D Non-Personal Data and Data Matching Guidelines (under development), an Associated Document to this procedure. Should a research project require that a student's name be attached to the data, the student must give free and informed consent. Refer to procedures AC.4.4.2 Free and Informed Consent and AC.4.4.3 Privacy and Confidentiality.

D. Confidentiality of Employee Information

1. The Human Resources department maintains an employee's personnel file. This file contains information which is directly related to the employee's job duties, performance, salary and employment history. To ensure that confidentiality is strictly maintained, all requests for employee information, including an employee's request to examine their own employee file, must be directed to Human Resources.

2. Human Resources maintains other employment-related records separately from the employee's personnel file in accordance with legal requirements. These other records, include, for instance, payroll records, auxiliary medical files such as disability claim forms or workers' compensation documents and medical records or correspondence provided by the employee or Employee Family Assistance Program (EFAP) provider.

3. Original permanent employee records may not be removed from Human Resources except as required by order of a competent court or tribunal.

4. SAIT employees who have a legitimate interest in another employee's personnel file and have demonstrated a "need to know" will be permitted access to the records. The

associate vice president, human resources, or designate, will determine whether the need to have access to the record or file has been demonstrated.

5. Urgent requests for an employee's personal information, such as their address, telephone number or immediate whereabouts, based upon an apparent emergency, is handled by the associate vice president, human resources, or designate, unless the individual has expressly authorized the release of this information or as authorized elsewhere in this procedure.

6. Access to employee personal information, including but not limited to salary data and employment history, shall be limited to those officials responsible for those matters and may not be released to anyone except as otherwise stated in this procedure.

7. Human Resources shall make routine changes in statistical information.

8. An individual wishing to use information gathered on an employee for research purposes must comply with procedure AC.4.4.1 Research Requiring Ethics Review.

9. SAIT is required to annually disclose compensation information, including severance, for employees earning over a specified threshold amount as outlined in *Alberta's Public Sector Compensation Transparency Act*. If the disclosure threatens an employee's personal safety, the employee may apply directly to the Government of Alberta for an exemption from having their compensation disclosed.

10. Under the *Protection of Privacy Act* (POPA), SAIT is permitted to disclose employee information that is a type routinely disclosed in a business or professional context. The disclosure is limited to an individual's name and business contact information, including business title, address, telephone number, facsimile number, email address and does not reveal other personal information about the individual or personal information about another individual. An employee who has safety concerns regarding disclosure of their information related to employment responsibilities may refer to procedure H.S.1.2.1 Prevention of Violence for details about the reporting mechanism. The employee may also disclose safety concerns to the associate vice president, human resources.

E. Disclosure of Personal Information in an Emergency or to Law Enforcement

1. Under the *Protection of Privacy Act* (POPA), SAIT is authorized to collect emergency contact information, which may include personal information relating to someone other than the individual (i.e., the student or employee), for the purpose of responding to emergencies.

2. SAIT may disclose emergency contact information provided solely for the purpose of contacting the designated person(s). Disclosure is authorized for students by the Office of the Registrar or designate, the Environmental Health and Safety department and/or by the deans/directors of the relevant schools and departments. For employees, disclosure may be authorized only by the associate vice president, human resources or designate.

3. In accordance with the *POPA,* SAIT may disclose personal information to law enforcement agencies with the appropriate consent and:

   a) If an employee receives a formal request directly from a law enforcement agency, they must promptly forward the request, along with any accompanying documentation or attachments, to the manager of Security and Emergency Services, Environmental Health and Safety.

   b) If the request involves multiple individuals, the school/department may consult with the Access and Privacy Unit, Office of General Counsel, for additional guidance.

4. The Office of the Registrar may release additional student personal information to authorized individuals in the event of an emergency or urgent situation involving a SAIT student, in accordance with Schedule B Emergency Disclosure of Student Personal Information, an Associated Document to this procedure.

F. Protection of Personal Information

1. 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.

2. If an employee becomes aware of unauthorized access to or unauthorized collection, use, disclosure or disposal of personal information, they must immediately inform their supervisor and submit a privacy incident report providing the relevant details, as outlined in procedure AD.1.1.3 Privacy Incident Response.

3. SAIT will create, use, protect and disclose non-personal data (data derived from personal information) in accordance with the *Protection of Privacy Act* (POPA) and in compliance with Schedule D Non-Personal Data and Data Matching Guidelines (under development), an Associated Document to this procedure.

PROCEDURE

4. SAIT will conduct a third-party risk assessment whenever third parties will collect, access and/or use personal or protected health information. Refer to procedure AD.2.10.2 Technology Vendor Risk Assessment.

5. A privacy impact assessment (PIA) may be conducted when evaluating a new system/application and/or planning a substantial change to an existing system/application which collects, uses or retains personal information, to identify and mitigate privacy risks, as outlined in procedure AD.1.1.2 Privacy Impact Assessment.

6. Personal information must not be used with any publicly accessible systems or artificial intelligence (AI) technologies unless a third-party risk and privacy impact assessment has been completed. Personal Information that is classified as protected, confidential or restricted, under procedure AD.3.3.1 Data Governance, may only be used within AI technologies that are managed by SAIT and only where all required consents and privacy assessments have been obtained, in accordance with procedure AD.2.15.3 Use of Artificial Intelligence Technologies at SAIT.

G. Retention and Disposal of Personal Information

1. SAIT will retain personal information only for as long as necessary to fulfill the purposes for which it was collected, in compliance with the *Protection of Privacy Act* (POPA) and other applicable legislation.

2. Personal information that is no longer required will be securely disposed of, in a manner that protects privacy and prevents unauthorized access, use or disclosure. l Records containing personal information will follow SAIT's Classification Scheme and Records Retention Schedule (refer to procedure AD.3.2.3 Retention and Disposition Schedule).

3. Certain student records are maintained in perpetuity and in accordance with SAIT's Classification Scheme and Records Retention Schedule (refer to procedure AD.3.2.3 Retention and Disposition Schedule).

H. 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).

PROCEDURE

2. All suspected or confirmed incidents of non-compliance must be reported immediately in accordance with procedure AD.1.1.3 Privacy Incident Response.

ASSOCIATED DOCUMENTS

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)

POLICY/PROCEDURE REFERENCE

AD.1.1	Privacy policy
AD.1.1.2	Privacy Impact Assessment procedure
AD.1.1.3	Privacy Incident Response procedure
AD.1.1.4	Privacy Complaints procedure

PROCEDURE