



SASKATCHEWAN INDIAN INSTITUTE OF TECHNOLOGIES

Privacy Policy

<p>Policy Title: Privacy Policy</p>	<p>Related Policies: Document Retention & Destruction</p>	<p>Personnel: All Personnel</p>
<p>Approvals: This Policy is the responsibility of Privacy Committee and will be reviewed annually.</p>	<p>Forms:</p>	<p>Effective Date:</p>

1. Policy Statement

The Saskatchewan Indian Institute of Technologies (SIIT) assumes full accountability for the personal information of its employees, clients, stakeholders and students in accordance with OCAP™ and privacy legislation. Each staff member must abide by SIIT’s procedures and practices when handling any type of personal information.

2. Definitions

OCAP™ – OCAP™ represents First Nations principles that protect individual privacy rights and the collective community. The principles of OCAP™ originated with the First Nations Information Governance Centre (FNIGC) and represent: Ownership, Control, Access and Possession. (<http://fnigc.ca/ocap.html>)

Personal Information Privacy and Electronic Document Act (PIPEDA) – Establishes rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. PIPEDA applies to federally regulated organizations, undertakings, or businesses and it came into effect January 1, 2004. Additionally PIPEDA applies to customers, clients, stakeholders, suppliers and students of provincially regulated organizations with respect to personal information that is collected, used or disclosed in the course of “commercial activities”.

Personal Information - According to PIPEDA, personal information is information about an identifiable individual that includes any personal information, recorded or not, in any form, including digital or paper format and includes:

- Name, address, telephone number, race, ethnic origin, religion, marital status or educational level (but see exception below regarding employees)
- Age, height, weight, medical records, blood type, DNA code, fingerprints, voiceprint
- Identification numbers such as social insurance numbers
- Credit records, loan records, existence of a dispute between a consumer and a merchant, and intentions to acquire goods or services

Under PIPEDA, personal information does not include the name, business title, business address or business telephone number of any employee (e.g. information found on a business card).

Real Risk: Requires consideration of the sensitivity of the information, the probability of misuse, and any other prescribed factor.

Significant Harm: PIPEDA defines significant harm as including, among other harms, humiliation, damage to reputation or relationships and identity theft.

Stakeholder – Refers to business partners, The SIIT Board of Directors, customers, vendors and applicable entities involved in any dealings with SIIT.

3. Policy Specifics

(i) Guidelines:

Guiding Principle: The Saskatchewan Indian Institute of Technologies (SIIT) is committed to respecting and protecting the privacy of the personal information it obtains about its students, clients, employees and stakeholders in the course of their employment, studies and business at SIIT.

The personal information of SIIT employees, clients, stakeholders and students must be managed so as to meet OCAP™ and legislative requirements. SIIT commits to the following statements:

- All personal information in SIIT possession or custody is protected as per the SIIT Document Retention and Destruction Policy;
- The forms of personal information being collected and the rationale for the collection of these forms of personal information will be identified and communicated to the individual;
- In obtaining consent, SIIT will ensure that the individual is advised of the identified purpose for which the personal information will be used:
 - Consent occurs and is obtained when an individual signs an application form which requests the release of personal information, or other form containing personal information thereby authorizing SIIT to collect, use, and disclose the individual's personal information for the purposes stated on the form;
 - Implied consent is granted by the individual when he/she signs the application or form. This allows SIIT to obtain or verify information from third parties (such as

banks, lenders, or insurance companies) in the process of assessing the eligibility of an individual, client, customer, student, job applicant or business partner;

- Written consent must be obtained prior to the collection of personal information; individuals have the right to withdraw their consent by submitting a written request to withdraw to the appropriate unit that was requesting consent to collect the information;
- The personal information collected is only collected for reasonable purposes as outlined on consent forms;
- Personal information is used only for the purposes for which it was collected;
- Personal information is retained only for the period of time that it is reasonably required as outlined in the SIIT Document Retention and Destruction Policy;
- Personal information is destroyed that is no longer required using a safe, secure and effective manner (e.g. shredding) as outlined in the SIIT Document Retention and Destruction Policy;
- All personal information collected is accurate as represented on the consent form;
- Individuals are permitted to gain access to their personal information through written requests, and to make corrections as appropriate;
- Appropriate security and safeguards are employed for the protection of personal information;
- Access to personal information is limited to authorized personnel that have a legitimate need to access the information;
- Written consent must be obtained from the employee, client, stakeholder, or student prior to the release of information to any third party;
- Individuals will be notified and consent will be obtained prior to the use of personal information for any reason(s) other than those provided at the time of collection; and
- Exceptions to any of the above will be limited to those set out in PIPEDA or as otherwise required by law.

SIIT protects the privacy and confidentiality of personal information by maintaining and storing it in secure locations that are not accessible to others without the express permission of the Director of Human Resources.

As required by federal legislation under Section 10.1 of PIPEDA, SIIT will notify individuals and report all data breaches where it is believed that the data breach creates a real risk of “significance harm” to the individual.

(ii) **Employees:**

The personal information of SIIT employees includes information found in employee personnel files such as dates of birth and home addresses, employee phone numbers, salary and benefits information, performance ratings and appraisals, internal investigation files, medical diagnoses or assessments, and complaints filed against an employee.

SIIT shall use some or all of the personal information obtained from employees for the purpose of interviewing applicants and offering employment, maintaining personnel files, providing benefits to employees, assisting employees in obtaining other forms of benefits or compensation, conducting performance evaluations, determining compensation in compliance

with other policies, investigating potential policy violations, determining discipline and conducting or participating in any processes or procedures relating to employee issues.

With prior consent, SIIT may disclose employee personal information to outside third parties. SIIT shall ensure that all third party providers employ a comparable level of protection for personal information as SIIT except where disclosure by SIIT or the third party provider is required by law. Where possible, SIIT will utilize privacy agreements/contracts with third party providers to protect the confidentiality and security of personal information.

(iii) **Students**

The personal information of students at SIIT includes all information found in student record files including student names, dates of birth and home addresses, student numbers, financial records, disciplinary matters, CPICS (where applicable) and medical diagnoses and assessments.

With prior consent, SIIT may disclose the personal information of students to outside third parties. SIIT shall ensure that all third party providers employ a comparable level of protection of personal information as SIIT except where disclosure by SIIT or the third party provider is required by law. Where possible, SIIT will utilize privacy agreements/contracts with third party providers to protect the confidentiality and security of personal information.

A student at SIIT who would like to know what personal information SIIT has collected about him/her should direct the inquiry to the Registrar's Office who will respond to the inquiry as quickly as possible and, in any event, not later than thirty (30) days after receiving the request. If the thirty day timeframe cannot be made and an extension is required, written notice will be provided to the individual outlining the expected date of response.

Any student who has a question or complaint about the content, administration or application of this policy should direct the inquiry to the Registrar's Office. The Registrar's Office will investigate the complaint and notify the student of the outcome of the investigation, including any action(s) taken as a result.

(iv) **Administration**

SIIT has appointed a Privacy Committee to be responsible for the administration of this privacy policy and compliance with OCAP™ principles and privacy legislation. If there is a conflict between OCAP™ and privacy legislation, OCAP™ will be the governing principles. SIIT's Privacy Policy shall be reviewed annually.

The Privacy Committee shall be responsible for:

- Developing and implementing policies and practices under SIIT's Privacy Policy including:
 - Procedures that address the collection, use, retention, destruction and management of personal information
 - Procedures for protecting personal information, complaints and inquiries
 - Staff training on privacy obligations
 - Procedures for establishing Privacy Policy committee members
- Reviewing policies, practices and procedures on an annual basis, or as needed, making appropriate revisions

- Ensuring appropriate measures are taken for breach of confidentiality regarding student, employee and stakeholder's personal information. Please refer to the SIIT Human Resource Policy manual Section B for further information.

(v) **Requests and Complaints**

An employee, client, or stakeholder of SIIT who would like to know what personal information SIIT has collected about him/her should direct the inquiry to the Director of Human Resources who will respond to the inquiry as quickly as possible and, in any event, not later than thirty (30) days after receiving the request. If the thirty day timeframe cannot be made and an extension is required, written notice will be provided to the individual outlining the expected date of response.

In accordance with PIPEDA, SIIT also reserves the right to deny an employee, client, stakeholder or student access to personal information if the record would reveal personal information about another individual.

Any employee, client or stakeholder who has a question or complaint about the content, administration or application of this policy should direct the inquiry to the Director of Human Resources. The Director of Human Resources will investigate the complaint and notify the employee of the outcome of the investigation, including any action(s) taken as a result.