Selkirk College

Policies and Procedures

Effective: 2020/09/01
Next Review: 2023/04/01

Policy 6550: Protection of Privacy

A. PURPOSE

To provide guidance on the collection, usage, disclosure, retention, disposition, protection and management of personal information, within the custody and control of Selkirk College. Examples include the financial, employment, medical, academic, educational technology and legal records of employees and students. This policy ensures privacy protection at Selkirk College is in accordance with *The College and Institute Act* and the *Freedom of Information and Protection of Privacy Act (FIPPA)* and complies with applicable federal and provincial statutes and regulations. This policy outlines the principles guiding Selkirk College's privacy management and persons deemed responsible for managing information and the major elements of Selkirk's privacy program.

B. SCOPE OF POLICY / LIMITS

This policy applies to records at Selkirk College pertaining to students, employees, contractors, third parties and service providers.

C. PRINCIPLES

Selkirk College is committed to:

1. Ensuring the privacy of student and employee information.
2. Compliance with all federal and provincial statues and legislations governing privacy.
3. Best practice measures and procedures to ensure effective management of the information within the College's custody and control.
4. Collecting and using personal information only for the purposes of which it was initially collected; and if required for related purposes subsequent to this policy and requirements of the *College and Institution Act* and the *Freedom of Information and Protection of Privacy Act.*
5. Training those employees responsible for managing and securing personal information.

D. RESPONSIBILITY

The following outlines responsibilities for implementation and adherence to this policy:

1. The President and Selkirk College Leadership Team shall oversee privacy management, and delegate authority as required.
2. Employees handling personal information are responsible for maintaining confidentiality and keeping information in a secure environment. All employees are responsible for and adhering to the practices outlined in this policy and related policies.
3. Selkirk College will identify a Privacy Information Officer who will be a point of contact for all privacy-related questions and concerns.

4. Employees should consult the Selkirk College Privacy Information Officer about any concerns regarding the disclosure of confidential and personal information, including access-to-information requests.

5. Selkirk College's Privacy Task Force will be responsible for developing, implementing and ensuring that this policy is consistent with FIPPA. The task force will include representatives from all divisions within the College.

6. Members of the public may request access to their personal information or make inquires by contacting Selkirk College's Privacy Information Officer.

E. COLLECTION AND USE OF PERSONAL INFORMATION

Personal information is collected and used by Selkirk College to fulfill the educational, institutional and operational activities of the College, and Ministry of Advanced Education Skills and Training or as required by law. Information deemed unnecessary to these objectives is not collected. In most circumstances, personal information is collected directly from the individual. Indirect collection occurs in exceptional circumstances and is generally authorized by the explicit, written consent of the individual, unless required by law. Metadata, which is data that gives information about other data is collected for the purposes of analytics to improve our services as part of Selkirk College's online platforms. Selkirk College will make every reasonable effort to ensure the usage of personal information is accurate and complete.

F. ACCESS TO INFORMATION

Selkirk College supports public access to information and an individual's right to access their personal information and request changes. Selkirk College will provide routine access to information informally upon request, or actively disseminate information, using existing procedures. An individual has right of access to any record in the custody or control of Selkirk College that pertains to their personal information unless contrary to other procedures and policies of the College. The right of access does not extend to information excluded from disclosure under applicable sections as stated in FIPPA. However, if immaterial details can reasonably be severed from a record, an applicant has the right of access to the remainder of the record. The right of access to a record may be subject to a required fee under Section 75 of the Freedom of Information and Protection of Privacy Act (FIPPA). Individuals requesting Selkirk College to release their personal information to a third party must authorize this release in writing; students, through the Office of the Registrar, employees through Finance and Payroll and employees through the Human Resources Department.

G. RETENTION AND DISPOSAL OF INFORMATION

Selkirk College will retain, archive, and dispose of personal information under its custody and control in accordance with the records management policy. Selkirk College utilizes a records retention procedure that is customized by divisions (college services, education and students) and takes into account the length of time information is held and needs to be maintained as required by law.

H. DISCLOSURE OR ACCESS TO INFORMATION

Selkirk College treats personal information within its custody and control with the highest degree of confidentiality. Personal information will only be disclosed to the individual themselves, or in specific circumstances to a third party with the explicit authorization of the individual, or as required by law. Selkirk College does not sell, share, or disclose personal information to others for any type of mailing list. Selkirk College will not disclose personal information outside of Canada without explicit consent unless permitted

to do so by law. Disclosure of an individual's personal information is subject to the appropriate application of FIPPA. All requests for access for personal information will follow the information access procedure that will be overseen by the Privacy Information Officer.

I. PROTECTION OF INFORMATION

The security of personal information is paramount to Selkirk College. Selkirk College will protect personal information by making reasonable security arrangements to prevent the risk of unauthorized collection, access, use, disclosure or disposal of personal information, and measures will be taken to ensure personal information is secure at all times. Security measures include, but are not limited to: secure facilities, controlled areas, restricted user access, password protection, firewalls, encryption software, locked file cabinets, and best practices.

J. INFORMATION STORAGE AND TECHNOLOGY

Selkirk College collects, retains, and stores personal data electronically (e.g., servers, databases) for the purposes of fulfilling its program and operational requirements. Regardless of the mode of data collection and storage or retention, Selkirk College will manage electronic personal information in accordance with procedures outlined at Selkirk College, and as required by the province and by law. Storage of electronic data will be consistent with geographic boundaries and limitations outlined in the FIPPA and defined policy and procedures.

K. USING SELKIRK COLLEGE WEBSITE

Selkirk College captures identification data from visitors to its website for security, statistical and reporting purposes. The consent to the use of cookies permits specific enquiries to be directed to, and managed by, appropriate information systems at Selkirk College. There is no disclosure of information about any particular website visitor to external organizations or individuals as outlined in FIPPA. Selkirk College website contains links to external third party websites, navigating to these links means that you are leaving Selkirk College's secure website and are no longer covered by our privacy policy.

L. EDUCATION AND AWARENESS

Employees must complete training relevant to their job on the appropriate collection, use, disclosure, storage, and destruction of personal information upon commencement of employment. Service providers and volunteers who collect personal information must demonstrate knowledge on privacy as it relates to the appropriate collection, use, disclosure, storage, and destruction of personal information. Selkirk College will recommend training prior to providing any service that involves personal information.

M. PRIVACY IMPACT ASSESSMENTS

When deemed appropriate, Privacy Impact Assessments (PIA) should be completed when developing or procuring any new technologies or systems that handle or collect personal information to ensure that privacy is fully understood and considered from the onset. Selkirk College's Privacy Information Officer must ensure that PIAs are completed where necessary. A PIA is not complete until it has been fully signed by all required parties as set out in the PIA Directions.

When deemed necessary, PIAs must be completed before the start of any new or updated or proposed changes to an enactment, system, project, program or activity and finalization of related procurement. Employees must conduct PIAs in accordance with the PIA Directions as issued by the Selkirk College's Privacy Information Officer. The College will maintain a site for the PIA program.

Policies and Procedures

N. DEFINITIONS

The terms below are those used in the FIPPA. The definitions use examples from the Selkirk College community to help illustrate their meaning. The following definitions describe the types of information which must not be disclosed to persons other than those who are authorized to have access:

Access: Includes both disclosure of records under FIPPA as a result of a request, and routine release of records that contain information that is available to the public or to an individual.

Selkirk College Leadership Team: Refers to senior administrators of Selkirk College who lead a specific division, school, or department at the College.

Personal Information: Recorded information about an identifiable individual other than contact information. Examples of personal information include, but are not limited to: ethnicity, gender, marital status, employment history, criminal history, grades, personal tax information and health-related information.

Privacy Impact Assessments: A process used to evaluate and manage privacy impacts and to ensure compliance with privacy protection rules and responsibilities.

Public Body: Includes a ministry of the government of British Columbia, an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2, of the FIPPA or a local public body (i.e. an educational body). Under the *College and Institute Act*, Selkirk College is an educational body, and therefore, a public body.

Record: Includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records;

Service Provider: A person or organization contracted by Selkirk College to perform services. Service providers may require access to personal information – either regularly or from time-to-time.

Information: Refers to personal information, unless otherwise specified.

Educational Records: Includes course grades, grade point average, academic status, graduation status, other institutions attended, admission status and course schedules and course registration status and all supporting documents.

Financial Records: Includes information about beneficiaries, insurance, benefits, debts, computer loans, deductions, maintenance enforcement and personal tax information.

Employment Records: Includes personal recommendations, evaluations, charter references or letters of discipline and reason for terminations.

Medical Records: Includes health care history related to medical, physical, psychiatric or psychological prognosis, treatments or evaluations.

Metadata: A set of data that describes and gives information about other data. Examples are date created, date modified, file size, images, video, webpages, spreadsheets.

Legal Records: Includes disciplinary investigations or proceeding that lead or could lead to a penalty or imposed sanction or policing.

O. RELATED POLICIES AND RESOURCES

British Columbia *Freedom of Information & Protection of Privacy Act* Office of the Information & Privacy Commissioner Guidelines
Public Sector Surveillance Guidelines
Privacy Impact Assessment Guidelines
Employee Code or Conduct and Conflict of Interest Policy

P. GOVERNMENT WEBSITES

http://www.bclaws.ca/civix/document/id/complete/statreg/96165_00
https://www.oipc.bc.ca/
http://www.bclaws.ca/civix/document/id/complete/statreg/96052_01

Note: the above list is not exhaustive. Statutes, regulations, policies, procedures, directives, practices, guidelines and other documents related directly or indirectly to freedom of information and protection of privacy will be updated and change over time.

Responsibility, Recommendation and Approval Dates

Executive Responsibility: President
Administrative Responsibility: Executive Director of Human Resources
Recommended by Policy Review Committee: 2020-09-16
Recommended/Approved by Education Council: N/A
Approved by President: 2020-10-02
Linkage to Board Policy: E30, E40, GP200