Selkirk College

Policies and Procedures

Effective: 10.01.2021
Next Review: 10.01.2023

Policy 6555: Management of Privacy Breaches

1. PURPOSE

The collection and management of personal information at Selkirk College is governed by the BC Freedom of Information and Protection of Privacy Act[1] (FOIPPA). In the event of a conflict between this policy and FOIPPA, FOIPPA shall prevail.

The purpose of this document is to provide guidance to managing a privacy breach. A privacy breach is the unauthorized access to personal information or the unauthorized collection, use, disclosure, or disposal of personal information.

2. SCOPE / LIMITS

This policy applies to all personal data collected and maintained by Selkirk College, including both digital and physical records. The Act defines personal information as "recorded information about an identifiable individual other than contact information".

3. POLICY

a. An employee, officer or director of Selkirk College, or an employee or associate of a service provider, who knows that there has been an unauthorized disclosure of personal information ("privacy breach" or "breach") that is in the custody or under the control of Selkirk College must:
   i) Immediately notify the College's Privacy Officer.
   ii) As appropriate, take steps to prevent further disclosures
   iii) Protect evidence of the breach
   iv) Participate in an investigation of the breach as requested
   v) Implement applicable recommendations that may be a result of the breach investigation as directed

b. The College's Privacy Officer, when notified of an unauthorized disclosure of personal information must:
   i) Notify the College Executive and President
   ii) Confirm that appropriate steps have been taken to prevent further breaches and that evidence of the breach has been protected
   iii) Investigate of the breach
   iv) Within 14 days of being notified of the breach, deliver a breach investigation report, to appropriate stakeholders including recommendations, to the College President when possible.
   v) Monitor the implementation of investigation recommendations

[1] https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00

c. The College President or delegate where applicable will notify as per FOIPPA of an unauthorized disclosure of personal information within a reasonable time frame.
   i) Notify the Ministry of Advanced Education and Skills Training, the Office of the Privacy Commissioner and the College's Board of Directors of the breach
   ii) Ensure that impacted individuals are notified
   iii) Ensure that an investigation of the breach is conducted and that recommendations are implemented

4. PROCEDURE

There are four key steps in responding to a privacy breach which are as follows, it is important to respond immediately to a breach. These steps should be done simultaneously or in quick succession, the final step is to provide recommendation for a long-term solution and prevention of future breaches. The procedure will be conducted through the use of a standardized template and checklist, see link below.

1. Contain the breach
2. Evaluate the risks
3. Notification
4. Prevention

1. Contain the Breach

Take immediate steps to contain the breach for example by stopping the unauthorized practice, recovering the records or shutting down the system that was breached, revoking or changing computer access codes or correcting weakness in physical or digital security.

Immediately contact the Privacy Office at privacy@selkirk.ca and Executive Director of Human Resources. Determine any others who need to be made aware of the incident and whether a response team needs to be put in place. Notify the police if the breach involved theft.

2. Evaluate the risks

Assess what elements have been breached. Evaluate the level of information that was exposed and if it was personal which considered more sensitive. Also consider if it was a combination of personal information rather than a single piece. Depending on the type of information the level of breach investigation will be determined.

3. Notification

Notification can be an important mitigation strategy, a key consideration is whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used of disclosed. Notification will be aligned with FOIPPA legislation.

4. Prevention

After immediate steps are taken, an investigation of how the breach should take place, policies should be reviewed and information provided. As a result of a breach the necessary tools should be improved or developed to further long-term safeguards against further breaches. Ongoing training may be required to ensure that staff can be aware of how to avoid future breaches if necessary.

5. RESOURCES

Process and Procedure Document	Link to be added
BC FOIPPA Legislation	www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00
BC Government FOIPPA Policy & Procedures Manual	https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual
OIPC – BC Privacy Breach Reporting	www.oipc.bc.ca/resources/report-a-privacy-breach/

Responsibility, Recommendation and Approval Dates

Executive Responsibility: Vice President College Services/CFO
Administrative Responsibility: Executive Director Human Resource
Recommended by Policy Review Committee: N/A
Recommended/Approved by Education Council: N/A
Approved by President: 2021-09-22
Linkage to Board Policy: