

Privacy Incident Response Procedure

Parent Policy

300-2-23 Protection of Privacy Policy

Purpose

This procedure establishes Bow Valley College's process for responding when a privacy incident occurs. It supports timely containment, assessment, escalation, notification, mitigation and prevention in accordance with the *Protection of Privacy Act*, Alberta ("POPA").

Scope

This procedure applies to Bow Valley College Board of Governors, employees, volunteers, contractors, and service providers who collect, use, disclose, store, access, or otherwise handle personal information on behalf of the college. It applies to privacy incidents arising from the handling of personal information, including incidents involving unauthorized access or unauthorized disclosure of personal information. Some incidents may also involve the college's information technology systems, networks, devices, applications, or other information technology assets and may therefore constitute both a privacy incident under this procedure and an information security breach under the Information Security Breach Procedure. In those cases, both procedures must be engaged and coordinated.

Responsibilities

- Employees, contractors, volunteers, students, and service providers will immediately report privacy incidents and will cooperate with containment, investigation, and remediation efforts.
- The Access and Privacy Officer will conduct or oversee the investigation, determine whether the real risk of significant harm threshold is met, coordinate required notifications and lead post-incident review.
- College departments, including Cybersecurity and Compliance, Information Technology Services, People and Culture, and Communications, will provide subject-matter expertise as may be required.

Procedure

The college will respond to privacy incidents as follows:

1. Contain the Breach

Any person subject to this procedure who becomes aware of a suspected or actual privacy incident must immediately report it to their supervisor and the Access and Privacy Officer. If a contractor, volunteer, or service provider becomes aware of a privacy incident first, they must immediately report it to their primary college contact. If the incident also originates from, affects, or requires technical investigation or remediation of the college's information technology systems, networks, devices, applications, or other information technology assets, it must also be reported promptly in accordance with the Information Security Breach Procedure. In such cases, the incident will be managed as both a privacy incident and an information security breach through a coordinated response.

2. Initial Report

The initial report will capture, to the extent known at the time, what happened, when and how the incident occurred, the type of personal information involved, the individuals potentially affected, and what immediate steps have already been taken to limit further exposure.

Upon receiving a report, the responsible college department, the Access and Privacy Officer, with support from Cybersecurity and Compliance, Information Technology Services, or other relevant

college departments, will immediately take reasonable steps to contain the incident. Containment will include, as appropriate, retrieving records, and recalling or deleting misdirected communications.

3. Investigation

The Access and Privacy Officer will promptly assess the risks associated with the incident to determine if any further steps are required. The assessment will consider the type and sensitivity of the personal information involved, the number of affected individuals, the cause and extent of the incident, who obtained or could obtain access to the information, whether the information has been or is likely to be misused, and whether the information has been recovered. As part of this assessment, the Access and Privacy Officer will determine whether a reasonable person would consider that the incident creates a real risk of significant harm, considering the factors listed in the *Protection of Privacy (Ministerial) Regulation*. The analysis will be documented and will consider all relevant circumstances, including the sensitivity of the information and the probability of misuse.

4. Incident Notification and Reporting

If the college determines that the incident creates a real risk of significant harm, the college will provide notice without unreasonable delay to the affected individuals, the Commissioner, and the Minister of Technology and Innovation.. Notices will be in writing and include a description of the incident, the date or period during which the incident occurred, a general description of the personal information involved, the steps the college has taken to contain the incident, and the contact information for the Access and Privacy Officer or other designated college contact who can answer questions.

Where the real risk of significant harm threshold is not met, the college will still document the assessment, rationale, and any corrective or preventive actions.

The college will provide appropriate mitigation measures to affected individuals, which may include credit monitoring where financial information is involved.

Communications will manage public and external communications related to the incident.

5. Prevention

In consultation with relevant college departments, the Access and Privacy Officer will recommend measures to prevent or reduce the risk of a similar privacy incident recurring. These measures may include strengthening administrative, technical, or physical safeguards, improving business processes, and providing additional training.

6. Documentation

The Access and Privacy Officer will keep a record of all privacy incidents, including the initial report, containment measures, findings, the real risk of significant harm analysis, any notifications issued, and recommended preventive measures.

Compliance

Members of the college community must adhere to the policies, procedures, and standards established by the college. These policies are designed to foster a safe, respectful, and inclusive environment that supports learning, teaching, and professional integrity.

Non-compliance may create risk for the college and will be addressed accordingly through applicable college policies, procedures and contracts. This may result in disciplinary action, up to and including termination for employees.

Definitions

Commissioner:

The Information and Privacy Commissioner, Alberta.

Personal information:

Recorded information about an identifiable individual, including name; address or telephone number; race, national or ethnic origin, colour, religious or political beliefs or associations; age, sex, marital or family status; an identifying number, symbol, or other particular assigned to the individual; fingerprints, other biometric information, blood type, genetic information, or inheritable characteristics; health and health care history, including information about a physical or mental disability; educational, financial, employment, or criminal history, including criminal records where a pardon has been given; anyone else's opinions about the individual; and personal views or opinions, except if they are about someone else.

Privacy incident:

The loss of, unauthorized access or unauthorized disclosure of personal information.

Significant harm:

Includes the risk of identity theft, damage to reputation or relationships, humiliation, bodily harm, loss of employment or professional opportunity, negative effects to an individual's credit history, damage to or loss of property and other material adverse effects on an individual.

Data sheet

Accountable officer

Executive team member responsible for legal. function

Responsible officer

Access and Privacy Officer

Approval

President and CEO

Contact area

Campus Services

Relevant dates

Approved	Executive Team: EXT260714-04
Effective	July 14, 2026
Next review	July 13, 2029

Related policies and procedures

200-2-23 Protection of Privacy Policy

300-2-11 Information Security and Identity Management Policy

300-2-11 Information Security Breach Procedure

Related legislation

Protection of Privacy Act, Alberta (POPA), 2024

Access to Information Act, Alberta (ATIA), 2024