Protection of Privacy Procedure

Parent policy
Protection of Privacy Policy

Purpose
This procedure describes how Bow Valley College manages and protects personal information throughout its life cycle.

Scope
This procedure applies to all members of the college community including its Board of Governors, Executive Team, employees, contractors and volunteers. It also applies to all personal information in the college's custody and control.

Procedure
Bow Valley College will manage personal information throughout its life cycle as follows:

1. **Collecting personal information and providing notice**
   a. Before collecting personal information, the responsible department must confirm that the collection is authorized by the Protection of Privacy Act, Alberta (POPA) or another provincial or federal law and that the collection is directly related to and necessary for a college program or activity.
   b. The responsible department must limit the collection to what is strictly necessary for the identified purposes.
   c. Where personal information is collected directly from an individual, the responsible department must provide a notice at or before the time of collection. The notice must state the purpose of collection, the legal authority for collection, and the title, business address, and business telephone number of a college employee who can answer questions about the collection. The notice must also state whether the personal information will be inputted into an automated system to generate content or make decisions, recommendations, or predictions.
   d. Employees and departments must use and disclose personal information only for the purpose for which it was collected or compiled, or as otherwise authorized by POPA or another applicable law.
   e. Where the college relies on consent to use or disclose personal information, the responsible department must obtain consent before the information is used or disclosed. Consent may be provided by written or electronic signature, provided any electronic signature complies with the Electronic Signature Policy.

2. **Handling access and correction requests**
   Employees who receive a request to access or correct personal information must promptly forward the request to the Access and Privacy Officer. These requests will be handled in accordance with the Information Access and Correction Procedure.

3. **Maintaining the personal information bank directory**
   Cybersecurity and Compliance will maintain a directory of the Bow Valley College's personal information banks. Departments must work with Cybersecurity and Compliance to create, review, and update directory entries. Each entry will identify the title and location of the bank, describe the type of personal information and categories of individuals included, state the

authority for collection, and describe the purposes for which the information is collected, used, or disclosed.

4. **Training and employee responsibilities**
   a. **Training**
   Bow Valley College will provide privacy training for all employees. Employees must complete the required privacy training, refresher training, and any additional role-specific training assigned based on their duties, responsibilities, or access to personal information at the frequency prescribed by the college.

   b. **Employee obligations**
   Employees must:
      i. Comply with the college's privacy management program.
      ii. Use personal information only for the purpose for which it was collected or for another use authorized by law.
      iii. Not disclose personal information to any individual or organization unless the disclosure is authorized by POPA or other applicable law.
      iv. Access personal information only as authorized by the college and only as necessary to perform assigned duties. Curiosity-based access, access for personal reasons, unauthorized disclosure, and unauthorized retention are prohibited.
      v. Protect personal information, data derived from personal information, and non-personal data from unauthorized access, collection, use, disclosure or destruction.
      vi. Comply with all applicable administrative, technical, and physical safeguards established by the college.
      vii. Complete all required privacy training.
      viii. Immediately report any suspected or actual unauthorized access, use, disclosure, loss, or other privacy incident in accordance with the Privacy Incident Response Procedure.
      ix. When involved in procuring, managing, or overseeing service providers, ensure that privacy requirements are addressed in any contract involving personal information.

5. **Completing privacy impact assessments**
   a. Before implementing a new program, service, system, project, administrative practice, or substantial change that involves the collection, use, or disclosure of personal information, the responsible department must contact Cybersecurity and Compliance and the Access and Privacy Officer to determine whether a privacy impact assessment is required.
   b. Where a Privacy Impact Assessment (PIA) is required, the responsible department must collaborate with Cybersecurity and Compliance, the Access and Privacy Officer, and other relevant stakeholders to complete the prescribed PIA form. The PIA must describe the proposed activity, identify privacy risks, and document measures to eliminate or mitigate those risks before implementation.
   c. The Chief Information Security Officer must submit a PIA to the Commissioner where:
      i. a practice, program, project or service will collect, use or disclose personal information deemed to be of high sensitivity;
      ii. a practice, program, project or service will involve the personal information of a significant percentage of the population the public body serves;
      iii. a practice, program, project or service will involve data matching between two (2) or more public bodies;
      iv. a practice, program, project or service is part of a common or integrated program or service;
      v. a practice, program, project or service involves the development or use of innovative technology;

vi. the Office of the Information and Privacy Commissioner of Alberta (OIPC) requests a copy of a PIA.

d. The responsible department will collaborate with Cybersecurity and Compliance to update the PIA when there are material changes to the program, service, system, project, or administrative practice.
e. The Chief Information Security Officer shall be responsible for responding to inquiries from the Commissioner about a PIA submitted by the college.

6. **Classifying and safeguarding personal information**
The college will maintain a security classification system for records containing personal information. The classification assigned along with systems governance will determine the security safeguards, access controls, transmission methods, and disposal measures that will apply to the information.

7. **Applying reasonable security safeguards**
Employees and departments must apply security safeguards that are appropriate and proportionate to the sensitivity of personal information such as:

i. **Administrative safeguards** which include documented policies, procedures, standards, and processes governing the collection, use, disclosure, access, retention, destruction, and handling of personal information, data derived from personal information, and non-personal data. These safeguards include role-based access and accountability for information handling, documented lawful authority for collection, use and disclosure, privacy impact assessments where required, privacy-by-design review, data classification and sensitivity labelling, mandatory privacy and security training, periodic access and compliance reviews, privacy incident response procedures, breach escalation processes, disciplinary consequences for non-compliance, service-provider oversight, privacy-protective contractual provisions, clean desk expectations, retention and destruction requirements, and documented governance for data matching, derived data, non-personal data, automated systems, and re-identification risk.

ii. **Technical safeguards** which include controls that limit system access to authorized users on a need-to-know and least-privilege basis; authentication measures such as strong passwords, multi-factor authentication, privileged access controls, and periodic access reviews; audit logging and monitoring of access to systems containing personal information; encryption of information at rest and in transit; secure transmission and storage of electronic records; secure configuration baselines; vulnerability management; timely security patches and software updates; endpoint protection; data loss prevention; network and application security controls; backup and recovery controls; secure printing measures; secure application programming interface (API) and integration controls; and safeguards for automated or artificial intelligence (AI) enabled systems, including validation, logging, monitoring, human oversight, and controls to reduce unauthorized disclosure, data leakage, prompt injection, misuse, or re-identification risk.

iii. **Physical safeguards** which include secure office spaces, restricted-access work areas, visitor sign-in and escort requirements, employee identification cards, secure records storage, locked filing cabinets, locked storage rooms, secure front-desk controls, controls to prevent unauthorized viewing, copying, photographing, or removal of records, screen privacy measures where appropriate, secure printing and mailroom controls, document shredders, locked shredding bins, secure records transport, documented chain of custody for sensitive physical records, secure destruction processes for records

containing personal information, secure storage of portable media or devices, and environmental protections for physical records and information assets.

iv. **AI and automated-system safeguards** which include governance, transparency, validation, monitoring, and human oversight controls for AI systems, automated systems, agentic AI, autonomous workflows, decision-support tools, predictive systems, and generative AI systems that collect, use, disclose, infer, generate, transform, or act on personal information, data derived from personal information, or non-personal data. These safeguards include documented lawful authority and approved purpose, notice and transparency where automated systems are used to generate content or make decisions, recommendations, or predictions, human oversight and override mechanisms, assigned accountability, data minimization, restrictions on entering sensitive information into unapproved AI systems, output validation, bias and data quality review, decision traceability, logging and monitoring where appropriate, controls for prompt injection and model misuse, guardrails for agentic or autonomous workflows, re-identification risk assessment, material change reassessment, incident escalation, and testing or validation before and during operational use.

v. **Third-party safeguards** which include privacy, security, contractual, and oversight controls for vendors, contractors, service providers, researchers, partners, public bodies, and other external parties that collect, access, use, process, disclose, transmit, retain, or destroy personal information, data derived from personal information, or non-personal data on behalf of the college. These safeguards include pre-contract privacy and security review, written agreements, purpose limitation, restrictions on secondary use and disclosure, prohibitions on unauthorized re-identification, restrictions on AI model training or product improvement using college data, subcontractor controls, breach notification requirements, audit or assurance rights, data residency and processing location transparency, confidentiality requirements, secure return or destruction obligations, retention limits, and requirements to notify the college of material changes to systems, sub-processors, safeguards, or data use.

8. **Service provider management**
To support the third-party safeguards described above, the responsible department must ensure that privacy and security requirements are clearly documented in any contract with a service provider that will collect, use, disclose, access, store, process, or otherwise manage personal information on behalf of the college.

9. **Retaining and destroying personal information**
Departments must retain and destroy personal information in accordance with the *Data Governance Policy* and associated retention guidelines. Personal information must not be retained longer than required to satisfy legal, operational, administrative, or archival requirements. When personal information is no longer required, departments must securely destroy it in accordance with the applicable retention schedule.

10. **Handling privacy complaints**
Employees who receive a privacy complaint must forward the complaint to the Access and Privacy Officer. Privacy complaints must be assessed, investigated, responded to, and documented in accordance with the Privacy Complaint Procedure.

11. **Responding to privacy incidents**
The college must maintain and follow documented privacy incident response procedures for suspected or actual loss of, unauthorized access to, or unauthorized disclosure of personal

information. Incidents must be handled in accordance with the Privacy Incident Response Procedure and Information Security Breach Procedure. These procedures support prompt internal reporting, containment, evaluation of whether there is a real risk of significant harm to an individual, notification to affected individuals, the Commissioner, and the Minister where required by law, and post-incident review.

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, and expulsion for students.

Definitions

Commissioner:
The Information and Privacy Commissioner of Alberta

Personal information:
Recorded information about an identifiable individual as defined by POPA and includes data derived from personal information and non-personal data.

Privacy management program:
The college's documented framework of policies, procedures, roles, safeguards and review processes established to support compliance with POPA.

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

Associated policies and procedures
300-2-21 Data Governance Policy
300-2-17 Electronic Signature Policy
300-2-22 Information Access and Correction Policy
300-2-22 Information Access and Correction and Procedure
300-2-11 Information Security Breach Procedure
300-2-23 Privacy Complaint Procedure
300-2-23 Privacy Incident Response Procedure

Related legislation
Access to Information Act (Alberta)
Protection of Privacy Act (Alberta)
Protection of Privacy (Ministerial) Regulation
Protection of Privacy Regulation