
Access to Information & Privacy Management Program
[DRAFT; renamed]

Policy No: 6700
Version: 5
Category: Administrative
Approval Body: Board of Governors
Executive Sponsor: Vice President, People, Culture & Inclusion
Entity Responsible: Information Access and Privacy Office (IAPO)
Directory of Records: 0650-15
Classification: Information Management
Approval Date: 2026 Mmm dd [tbd – pending]

Background

BCIT is committed to protecting Personal Information and supporting Access to Records in accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA). As a public post-secondary institution, BCIT has legal obligations to provide access to information in its Custody or Control, protect Personal Information throughout its lifecycle, and demonstrate accountability for its information management practices.

This Policy is intended to promote transparency and respect for individual privacy while supporting BCIT's educational mandate, research, and administration. It reinforces BCIT's commitment to responsible information stewardship and accessible information practices that align with Institute values and BCIT's *IDEAS Lens* (Indigenous, Inclusion, Diversity, Equity, Access, Sustainability, and Student Wellbeing).

Purpose

This Policy establishes BCIT's Access to Information and Privacy Management Program and provides a framework for managing information access and privacy responsibilities across the Institute.

The Program promotes a culture of respect for privacy by ensuring that Personal Information is collected, used, disclosed, accessed, stored, retained, and disposed of appropriately throughout its lifecycle. It supports the identification and mitigation of privacy risks, Privacy by Design practices, employee awareness and training, effective Privacy Incident response, and continuous improvement of privacy and information access practices.

Application

This Policy applies to all BCIT Employees, as defined.

Scope

This Policy applies to all Personal Information in BCIT's Custody or under its Control. It governs the collection, use, disclosure, access, storage, retention, disposal, and protection of Personal Information, as well as BCIT's administration of access to Personal Information requests under FIPPA. The Policy applies to Records in any format and is supported by Associated Procedures and Standards.

Related Documents and Legislation

Provincial Legislation

College and Institute Act, RSBC 1996, c 52

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165

Freedom of Information and Protection of Privacy Regulation, B.C. Reg. 155/20121

BCIT Policies

1500 Code of Conduct

3501 Acceptable Use of Information Technology

3502 Cyber Security

Related References

Office of the Information and Privacy Commissioner for British Columbia. (2023). *Accountable Privacy Management in BC's Public Sector*. (Guidance Document 1468)

British Columbia Ministry of Citizens' Services. (2022). *Privacy Management Program Direction* (Ministerial direction 02/2022).

Definitions

The following definitions apply to this Policy and its Associated Procedures:

Access and Privacy Management Program (or "Program") means the framework established by the Head of a public body as mandated by FIPPA to ensure that privacy obligations are understood and upheld across the Institute and that Personal Information is protected throughout its lifecycle.

Access to Information (or "Access" or "FOI" or "Freedom of Information") means the right granted by FIPPA and other applicable legislation for any person to obtain access to a Record held in BCIT's Custody or under its Control.

Access Request (or "FOI Request" or "Freedom of Information Request") means a person's right to access Records that may, depending on the context, involve Personal Information. Access Requests are administered within the Program.

Business Owner means the Program Head, Department Head, Associate Dean, Dean, or other designated leader responsible for the governance of information within their academic or administrative unit. The Business Owner is accountable for ensuring that Personal Information is

managed, accessed, used, disclosed, retained, and protected in accordance with BCIT policies and applicable legal requirements, including FIPPA.

Contact Information means information enabling contact with an individual at a place of business and includes their name, position name or title, business telephone number, business address, business email or business fax number (see also Personal Information).

Control means the power or authority to manage a Record throughout its lifecycle, including restricting, regulating, and administering its use or disclosure.

Custody means the physical possession of a Record by BCIT, whether the Record is held directly by BCIT or by a third party on its behalf. A Record is in BCIT's Custody when BCIT has responsibility for its care, storage, security, or maintenance, even if BCIT does not have authority to decide the Record's use, access, storage, retention, disposition, or disclosure.

Employee in relation to BCIT has the same meaning as in FIPPA and includes volunteers and Service Providers.

FOI Request (see Access Request).

Head is the person having statutory authority and accountability for decisions made under FIPPA for a given public body.

Information Access and Privacy Office or **IAPO** means the BCIT office responsible for the administration of FIPPA and for overseeing the Program.

Initiative means a project, program, service, system, process, or activity supporting BCIT business that is being introduced, changed, expanded, or reviewed, and that may involve the collection, use, disclosure, retention, or protection of Personal Information.

Personal Information means recorded information about an identifiable individual other than Contact Information (see also Contact Information).

Personal Information Bank or "**PIB**" means a collection of Personal Information organized or retrievable by an individual's name or by an identifying number or other symbol assigned to an individual (see also Personal Information Directory).

Personal Information Directory or "**PID**" means a directory that lists and describes Personal Information Banks (PIBs) to assist in identifying the location of Personal Information held by BCIT (see also Personal Information Bank).

Privacy Breach means confirmed theft or loss, or the collection, use, or disclosure of Personal Information in the Custody or under the Control of a public body in contravention of Part 3 of FIPPA (see also Privacy Incident).

Privacy by Design means from the outset embedding privacy into the design specifications of technologies, business practices, and systems.

Privacy Concern means any reported Privacy Incident.

Privacy Incident means an event that has or could result in theft or loss or the unauthorized collection, use, or disclosure of Personal Information (see also Privacy Breach).

Privacy Risk Assessments means the tools used to identify and evaluate privacy and information security risks. The type and scope of review required depend on the nature of the Initiative and the level of risk.

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 means a service provider, contractor or consultant retained to perform services for BCIT.

Guiding Principles

Transparency and Access - BCIT supports timely, fair, and consistent access to Records in accordance with FIPPA, while balancing the protection of Personal Information and other information exempt or excepted from disclosure.

Privacy and Responsible Information Stewardship - Personal Information is collected, used, disclosed, retained, stored, and disposed of only where authorized by law and while respecting individual privacy, trust, and accountability.

Privacy by Design and Risk Management - Access and privacy considerations are integrated into Initiatives from the outset, with risks identified, assessed, and mitigated throughout the information lifecycle.

Inclusion, Equity, and Respect for Indigenous Data - BCIT applies its *IDEAS Lens* in Access and privacy decision-making and recognizes that information practices may affect individuals and communities differently. BCIT respects Indigenous data interests and supports engagement and approaches that align with Indigenous Data Sovereignty principles where appropriate.

Shared Accountability and Continuous Improvement - Access to information and privacy protection are shared responsibilities. BCIT monitors compliance, addresses issues and incidents, and continuously improves its Access and Privacy Management Program in response to evolving risks, legal requirements, and operational needs.

Policy Statements

Access to Information and Privacy Management Program

- BCIT maintains the Program to support compliance with FIPPA. The Program includes the designation of a Privacy Officer, Privacy Risk Assessments, information-sharing controls, privacy training, Privacy Incident management, and ongoing privacy compliance monitoring.
- BCIT expects all Employees to complete privacy training and make reasonable efforts to understand and comply with this Policy and Associated Procedures.

Collection, Use and Disclosure of Personal Information

- BCIT collects Personal Information transparently for defined purposes, provides notice of legal authority and contact information, and limits collection to what is necessary and authorized to support its programs, operations, and legal obligations.
- BCIT accesses, uses and discloses Personal Information only for authorized purposes, with consent or as permitted or required by FIPPA, and restricts internal access on a need-to-know basis.
- BCIT requires contractual agreements to be in place with Service Providers, public bodies, and other third parties handling Personal Information on BCIT's behalf.

Privacy Risk Assessments

- BCIT requires Privacy Risk Assessments for new or significantly revised Initiatives involving Personal Information, Institute data, technologies, systems, services, or business processes.
- The type and scope of review required depends on the nature of the Initiative and the level of risk identified by the Privacy Office and the Cyber Security Office.

Protection, Retention, and Disposal of Personal Information

- BCIT protects Personal Information using reasonable physical, technical, organizational, and contractual safeguards.
- BCIT retains, stores, and securely disposes of Personal Information in accordance with legal and operational requirements and stores Personal Information within Canada by default (whenever possible).

Privacy Incidents

- BCIT requires that all Privacy Incidents be reported promptly to IAPO and managed in accordance with protocols.

Information Access and Correction

- BCIT recognizes individuals' rights under FIPPA to request correction of their Personal Information and to access their own Personal Information and Institute records. BCIT will make reasonable efforts to provide access in a format that is accessible and responsive to the requester's communication and accessibility needs.

Duties and Responsibilities

Director, Privacy and Policy Management ("Privacy Officer")

The Privacy Officer is responsible for the administration and oversight of BCIT's Access to Information and Privacy Management Program, and for overseeing compliance with FIPPA and this Policy. In fulfilling these responsibilities, the Privacy Officer:

- Develops, implements and maintains the Program.
- Promotes, monitors, and reports on compliance with FIPPA and this Policy.
- Provides access to information, guidance and training.
- Maintains BCIT's Personal Information Bank and Personal Information Directory.
- Investigates and responds to Privacy Concerns and Privacy Incidents.
- Supports the review and completion of Privacy Risk Assessments.
- Provides guidance on and supports review and negotiation of privacy language in contracts.
- Recommends corrective actions in response to non-compliance with this Policy or FIPPA.
- Represents BCIT before the Office of the Information and Privacy Commissioner (OIPC).
- Delegates duties assigned under this Policy.

Information Access and Privacy Office

Under the direction of the Privacy Officer, IAPO is responsible for providing guidance, education, oversight, and operational support to facilitate compliance with FIPPA, this Policy, and Associated Procedures.

Business Owners

Within their areas of responsibility, Business Owners will:

- Promote and support compliance with FIPPA, this Policy, and Associated Procedures.
- Ensure Employees under their supervision are aware of and complete required privacy training and understand their privacy obligations.
- Ensure Personal Information is collected, accessed, used, disclosed, retained, secured, and disposed of in accordance with BCIT policies and security standards.
- Ensure Privacy Risk Assessments are completed in consultation with IAPO and the Privacy Officer for new or significantly revised Initiatives ("changed Initiatives") involving Personal Information, including programs, projects, systems, technologies that use AI, services, and business processes.
- Review and address privacy or information security risks and implement appropriate mitigation or corrections.
- Report promptly Privacy Incidents to the Privacy Office and cooperate in related

investigations and responses.

- Cooperate with Personal Information Access Requests, privacy investigations, audits, and compliance activities.
- Before responding to requests received directly from external parties, engage IAPO to ensure consistent handling and compliance.
- Ensure Service Providers handling Personal Information on behalf of BCIT comply with contractual privacy requirements.
- Seek guidance from the IAPO when privacy requirements, risks, or obligations are unclear.

Employees

All BCIT Employees are expected to:

- Familiarize themselves with and adhere to this Policy and Associated Procedures.
- Be aware of and complete required privacy training and understand their privacy obligations.
- Report all Privacy Incidents or Concerns without delay to the Privacy Office and cooperate in related investigations and responses.
- Offer full cooperation and participate in the processes described in this Policy and Associated Procedures.

Service Providers

Service Providers whose work involves access to, or the collection, use, disclosure, storage, retention, or destruction of Personal Information must adhere to this Policy, and to applicable contractual Privacy and Data Security Schedules, and FIPPA. Upon request they must provide BCIT with any relevant privacy and data security documentation. BCIT may require Service Providers to demonstrate that their systems and services for handling Personal Information support applicable accessibility, privacy, and human rights requirements.

Special Situations

None

Associated Procedures

6700-PR1 Information Access Procedure
6700-PR2 Privacy Incident Handling Procedure
6700-PR3 Privacy Risk Assessments Procedure

Associated Forms

See Associated Procedures

Appendix

None

Approval History

		<u>Approval Date</u>	<u>Status</u>
Created:	Policy 6700 version 1	2002 Nov 12	Replaced
Revised:	Policy 6700 version 2	2004 Aug 11	Replaced
Revised:	Policy 6700 version 3	2008 Sep 30	Replaced
Revised:	Policy 6700 version 4	2021 May 26	In Force
Revised:	Policy 6700 version 5	[2026] tbd	draft revision

Scheduled Review Date

2026 Month dd - *tbd upon approval*; however, the Policy's Executive Sponsor may initiate review at any time.

DRAFT