Freedom of Information and Protection of Privacy

Policy No:	6700
Version:	4
Category:	Information Management
Approving Body:	Board of Governors
Executive Sponsor:	Vice President, Human Resources & People Development
Department Responsible:	Information Access and Privacy
Directory of Records Class:	0650-15
Approval Date:	2021 May 26

Policy Statement

As a public body, BCIT is subject to the British Columbia *Freedom of Information and Protection of Privacy Act* (the "Act" or "FIPPA"), which both establishes processes for permitting access to records within its custody and control and regulates the collection, use, disclosure and protection of personal information by BCIT.

BCIT is committed to ensuring its compliance with FIPPA by protecting the privacy of its staff, students and members of the community and by maintaining appropriate transparency and accountability within the community.

BCIT seeks to maintain and foster a culture of respect for individual privacy and supports best practices and standards for privacy protection.

Purpose of Policy

This policy seeks to describe how BCIT complies with its obligations under FIPPA, including setting out the responsibilities of employees, service providers and volunteers regarding the right of access to records and information, and the protection of personal information.

Table of Contents

Application and Scope of this Policy

This policy applies to all BCIT employees, service providers and volunteers who have access to records and information in BCIT's custody and control.

Related Documents and Legislation

Legislation – Provincial

College and Institute Act, RSBC 1996, c 52

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165
Personal Information Protection Act, SBC 2003, c 63

Legislation – Federal

Canadian Anti-Spam Legislation[1], SC 2010, c 23

Legislation – Outside Canada

General Data Protection Regulation, (EU) 2016/679

Industry Standards

Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*, December 2018 (TCPS2 2018)

Standards Council of Canada, *Model Code for the Protection of Personal Information* (Can/CSA-Q830-03) (R2014)

BCIT Policies

1100, Whistleblower
1500, Code of Conduct
1504, Standards of Conduct and Conflict of Interest Policy
2501, Contracts
3501, Acceptable Use of Information Technology
3502, Information Security
4113, Convocation
4501, Accommodation for Students with Disabilities
5102, Student Code of Conduct (Non-Academic)
5201, Recording in the Classroom
5900, Educational Technology Policy
6500, Research Ethics for Human Participants
6701, Records Management
7000, Gift Acceptance
7103, Sexual Violence and Misconduct
7110, Emergency Management
7507, Harassment and Discrimination

Definitions

The following definitions apply to this policy and its associated procedures:

access: refers to the process for accessing records in the custody or control of BCIT under the Act.

Act or "**FIPPA**"**:** means the *Freedom of Information and Protection of Privacy Act,* including regulations.

Administrative Authority: means an employee, department, administrative body or committee of BCIT with responsibility or accountability for directing or overseeing a distinct BCIT activity, program, unit, office or department.

business contact information: has the same meaning as "contact information" in the Act, i.e. information to enable an individual at a place of business to be contacted and includes the name,

[1] Full title omitted for brevity

position name or title, business telephone number, business address, business email or business fax number of the individual.

Contracts Manager: means the position with the same title described in Policy 2501 - Contracts, who is responsible for providing services and guidance within BCIT relating to the identification, qualification, and execution of external business opportunities.

Director, Cyber Security: means the position with the same title described in Policy 3502 - Information Security, who is responsible for overseeing all aspects of cyber security.

Directory of Records: means the records classification and retention schedule established under Policy 6701 - Records Management.

disposition: has the same meaning as in Policy 6701 - Records Management.

employee: has the same meaning as in the Act, i.e. in relation to BCIT, includes a volunteer and a service provider, and the service provider's associates.

head: for the purposes of the Act means the President of BCIT.

Information Access and Privacy Office or **"IAPO":** means the BCIT office under Human Resources that is tasked with the administration of the Act.

Information Owner: has the same meaning as in Policy 3502 - Information Security, i.e. the BCIT employee who has been assigned responsibility for overseeing the lifecycle of one or more sets of information including responsibility for classifying and protecting information according to the information security classifications.

information security: has the same meaning as in Policy 3502 - Information Security.

information security classifications: has the same meaning as Policy 3502 - Information Security.

Institute: means BCIT, the British Columbia Institute of Technology.

OIPC: means the Office of the Information & Privacy Commissioner for British Columbia.

personal information: has the same meaning as in the Act, i.e. recorded information about an identifiable individual other than business contact information.

personal information bank: has the same meaning as in the Act, i.e. a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

privacy breach: means a confirmed case of unauthorized access, collection, storage, retention, disposition, use or disclosure of personal information to which the Act applies. Such activity is unauthorized if it occurs in contravention of FIPPA.

privacy incident: means an actual, possible, or pending privacy breach.

Privacy Impact Assessment or "**PIA**"**:** has the same meaning as in the Act, i.e. an assessment that is conducted by BCIT to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 of the Act.

Privacy Officer: means the Associate Director, Privacy, Information Access and Policy Management.

program: means formally recognized activities and functions designed to deliver specific services that are related to a specific subject matter or topic.

record: refers to "record" as that term is defined in the Act, and includes any information created by or received by an employee that is evidence of a business transaction or activity, regardless of format or source, and includes the same meaning in the Act, i.e. 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 as defined under the Act.

Records Manager: has the same meaning as in Policy 6701 - Records Management.

service provider: has the same meaning as in the Act, i.e. a person retained under a contract to perform services for BCIT.

third party: has the same meaning as in the Act, i.e. in relation to a request for access to a record or for correction of personal information, means any person, group of persons or organization other than the person who made the request, or a public body.

unauthorized disclosure: means the disclosure of, production of or the provision of access to personal information to which FIPPA applies, if that disclosure, production, or access is not authorized under FIPPA.

Guiding Principles

BCIT complies with the following personal information protection principles. This policy and its associated procedures shall be interpreted and applied consistently with the following principles and objectives:

1 General

1.1 BCIT will manage all personal information in compliance with the Act and shall seek to do so in accordance with best practices and standards for protecting personal information.

1.2 BCIT will limit collection, access, use, disclosure, and retention of personal information to what is directly related to and necessary for its operations except as otherwise authorized or required by the Act or other applicable laws.

1.3 BCIT will make every reasonable effort to ensure the accuracy and protection of personal information in its custody or control.

1.4 BCIT will evaluate suspected privacy incidents, and will manage and respond to them in an effective and timely manner in accordance with the Act.

1.5 If there is a conflict between another policy or procedure and this policy or its associated procedures, including assigned duties and responsibilities, this policy and its procedures prevail to the extent of the conflict.

2 Collection of Personal Information

2.1 BCIT provides notice to affected individuals of the purposes for which it collects personal information, except where otherwise authorized or required by the Act or other applicable laws.

2.2 BCIT limits the collection of personal information to the minimum amount necessary to carry out the Institute's programs or activities , except as authorized by the Act or other applicable laws.

3 Use and Disclosure of Personal Information

3.1 BCIT will use and disclose personal information only:

a. for the purpose for which that personal information was obtained or compiled or for other uses or purposes that are consistent with those original purposes for collection;

b. with notice to and the written consent of the individual the personal information is about;

c. for any other purpose permitted or required under the Act and other applicable laws.

3.2 Personal information at BCIT is shared internally on a need-to-know basis. Access by employees to personal information will only be granted in order to allow employees to carry out their duties or for other BCIT authorized purposes.

3.3 BCIT will only disclose personal information in its custody or control to external third parties where permitted by the Act or required by applicable laws.

3.4 Any employee who is aware or who suspects a privacy incident has occurred or is likely to occur must immediately notify the Privacy Officer.

4 Retention and Disposition of Personal Information

4.1 If BCIT uses an individual's personal information to make a decision that directly affects the individual, then it will retain that personal information for at least one year from the date of the decision so that the affected individual has a reasonable opportunity to obtain access to that personal information.

4.2 BCIT disposes of personal information in accordance with the Directory of Records. BCIT supports the destruction of records containing personal information when such information is no longer needed for business, legal or operational purposes.

5 Accuracy and Correction of Personal Information

5.1 BCIT will make every reasonable effort to ensure the personal information in its custody or control is complete and accurate.

5.2 BCIT will, where appropriate correct or annotate the personal information of an individual upon request by that individual with supporting evidence that is satisfactory to the Institute and in accordance with the Act.

6 Protection of Personal Information

6.1 BCIT will protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposition.

6.2 All employees shall ensure that the protection of personal information is appropriately considered in the course of planning, implementing, maintaining, and revising systems, projects, programs, and activities that involve the processing of personal information.

7 Storage of Personal Information

7.1 BCIT will only access or store personal information in its custody or control inside Canada, unless the individual the information is about has consented to access or storage outside Canada or unless the access or storage is otherwise permitted under the Act.

Duties and Responsibilities

President

The President is the head of the Institute under the Act and has authority to delegate the statutory duties, powers and functions of the head. The President may delegate their powers under the Act by written instrument.

Vice-President Human Resources and People Development

Subject to the terms of any written delegation by the President, the Vice-President Human Resources and People Development exercises the delegated powers of the head of the Institute for purposes of administering BCIT's compliance with the Act.

Privacy Officer and IAPO

The IAPO is responsible for the design, delivery and coordination of BCIT's information access and privacy compliance initiatives, and the Privacy Officer is responsible for overseeing the operations of this office. The Privacy Officer also exercises delegated powers from the President, as head of the public body.

Subject to the terms of any written delegation by the President, the Privacy Officer and the IAPO are responsible for:

1. Overseeing how the Act is administered by the Institute to ensure compliance with the Act and that the purposes of the Act are achieved, including administration of the Information Access and Privacy Office. In doing so the Privacy Officer may provide advice and guidance to the BCIT community, conduct investigations, and make recommendations to Administrative Authorities, including concerning matters such as the suspension or termination of systems, projects, programs, or activities.
2. Consulting with the BCIT community with respect to initiatives involving the processing of personal information and supporting the completion of Privacy Impact Assessments (PIAs) for such initiatives.
3. Establishing and maintaining BCIT's privacy management framework.
4. Responding to requests, inquiries, complaints, information access requests, and privacy incidents, including liaising with the OIPC.
5. Maintaining BCIT's personal information directory in accordance with the Act.
6. Establishing, in consultation with the President and the Vice-President Human Resources and People Development, categories of records available to the public without a request in accordance with the Act.
7. Promoting privacy awareness in the BCIT community including education and training.

Employees (which includes service providers and volunteers)

All employees are responsible for:

1. Handling all personal information to which they receive access in accordance with the Act and this policy.
2. Accessing the minimum amount of personal information necessary for the performance of their duties.
3. Cooperating with the Privacy Officer in responding to access requests.
4. Immediately reporting to the Privacy Officer any circumstances where the employee suspects a privacy incident has occurred or is likely to occur.

5. Employees must cooperate with the Privacy Officer as required in the fulfillment of the Institute's obligations under this policy, related procedures, and applicable access and privacy legislation.

Administrative Authorities

Administrative Authorities have responsibility and authority for:

1. Assisting the Privacy Officer, including in responding to access requests by providing records and information, and taking action as needed to support compliance with the Act, including conducting searches and producing records in a timely manner.
2. Ensuring that the programs and activities for which they are responsible comply with the Act, this policy and its associated procedures.
3. Ensuring that any contract or agreement for which they are responsible complies with this policy.
4. Ensuring that policies and procedures over which they have authority are consistent with this policy and its associated procedures.
5. Consulting with the IAPO in respect of new BCIT initiatives that involve the processing of personal information.
6. Cooperating with the Privacy Officer on investigations regarding privacy risks and implementing any resulting recommendations.
7. Ensuring employees for whom they are responsible receive training on this policy and its procedures.

Contracts Manager

The Contracts Manager is an Administrative Authority with responsibility and authority for:

1. Fulfilling the general responsibilities assigned to Administrative Authorities above.
2. Consulting with the Privacy Officer to assess contracts for privacy risks and take action as necessary, including providing guidance or direction to other Administrative Authorities.

Director, Cyber Security

The Director, Cyber Security is an Administrative Authority with responsibility and authority for:

1. Fulfilling the general responsibilities assigned to Administrative Authorities above.
2. Working with the Privacy Officer to investigate privacy and security concerns.
3. Reviewing all PIAs for adequacy, consistency, and compliance with BCIT information security policies and standards.
4. Working with the Privacy Officer to provide privacy and information security training and awareness.

Director, Enterprise Risk and Internal Audit

The Director, Enterprise Risk and Internal Audit is an Administrative Authority with responsibility and authority for:

1. Fulfilling the general responsibilities assigned to Administrative Authorities above.
2. Working with the Privacy Officer to identify and mitigate privacy risks.

Director, Safety, Security and Emergency Management

The Director, Safety, Security and Emergency Management is an Administrative Authority with responsibility and authority for:

1. Fulfilling the general responsibilities assigned to Administrative Authorities above.
2. Working with the Privacy Officer to identify and mitigate privacy risks.
3. Working with the Privacy Officer to investigate privacy and security concerns.

Information Owners

Information Owners are Administrative Authorities with responsibility and authority for:

1. Fulfilling the general responsibilities assigned to Administrative Authorities above.
2. Classifying information for which they are responsible according to the information security classifications, and managing information in accordance with Policy 3502 - Information Security and this Policy.
3. Communicating the information classifications and safeguards to employees or third parties who handle that information.
4. Contacting the Privacy Officer prior to undertaking a new system, project, program or activity for which they are responsible, or making changes to an existing one, to determine whether a PIA is required.
5. Completing a PIA as identified by the Privacy Officer.
6. Incorporating PIA requirements into program development and project governance processes for which they are responsible, including:
    a. ensuring sufficient lead time and resources are available to carry out PIA requirements in relation to other project deadlines;
    b. abiding by the requirements of a completed PIA, including taking steps to correct or mitigate any identified privacy and information security risks prior to implementation if implementation would fail to comply with the Act, this policy, or associated procedures; and
    c. establishing protocols consistent with Policy 6701 - Records Management that authorize the disposition of records.

Records Manager

1. Fulfilling the general responsibilities assigned to Administrative Authorities above.
2. Working with the Privacy Officer to identify and mitigate privacy risks.
3. Ensuring BCIT's records and information programs and records management services comply with the Act.

Procedures Associated with This Policy

6700-PR1, Information Access (in development)
6700-PR2, Privacy Incident Response (in development)

Amendment History

		Approval Date	Status
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

Scheduled Review Date

2026 May 26