

Procedure Information	
Related to Policy No:	AD-CO-4.14
Approved by:	Executive Committee
Approval Date:	May 11, 2022
Executive Responsible:	VP Finance & Corporate Services
Administrator Responsible:	Director, Policy, Planning & Strategy
Date of Next Review:	May 2027

## FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY PROCEDURES

### Definitions

The following definitions apply to this policy and procedures:

#### **Access**

Refers to the process for viewing or using records in the custody or control of CNC under the Act.

#### **Act or "FIPPA"**

The BC Freedom of Information and Protection of Privacy Act, including regulations.

#### **Administrator**

A CNC employee with responsibility or accountability for directing or overseeing a distinct program area, campus, or department.

#### **Business Contact Information**

Contact information for an individual at a place of business including the individual's name, position or title, business telephone number, business address, business email or business fax number.

#### **Privacy Office**

The area within the College that is tasked with the administration of the Act.

#### **Personal Information**

Recorded information about an identifiable individual other than business contact information, as defined in the Act.

#### **Personal Information Bank (PIB)**

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, disclosure, or theft of personal information to which the Act applies.

#### **Privacy Incident**

Means an actual, possible, or pending privacy breach.

#### **Privacy Impact Assessment (PIA)**

A review conducted by CNC to assess the privacy implications of a current or proposed system, project, program, or activity.

#### **Public Body**

A ministry of the government of British Columbia; an agency, board, commission, corporation, office, or other body designated in Schedule 2 of FIPPA; or a local public

body including a local government body, a health care body, a social services body, an educational body, or a governing body of a profession or occupation designated in Schedule 3 of FIPPA.

**Record**

Any information recorded or stored by any means whether in hard copy or electronic format. This includes, but is not limited to documents, text messages, letters, emails, telephone records, written notes, maps, drawings, photographs, video, and papers.

**Service Provider**

A person or company retained under a contract or agreement to perform services for CNC.

**Unauthorized Disclosure**

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

**Procedures**

**1. Access to Information**

1.1. Routinely Released Information

1.1.1. This information can be released without a formal Freedom of Information Request. It may be released by the College proactively (for example, posting online, in publications, or in libraries) or made available by request by contacting the appropriate department. Information the College identifies as available by routine request may include reports, minutes, and other documents without personal information.

1.2. Freedom of Information (FOI) Requests

1.2.1. Information not available through routine channels can be requested through a formal FOI request by writing to the College's Privacy Office. If barriers exist, the request will also be accepted verbally.

1.3. A person may request access to any record in the custody or under the control of the College, including a record containing personal information about the applicant.

1.4. Some information is not able to be disclosed under Sections 12 to 22 of FIPPA, but if that information can reasonably be separated or redacted from a record, an applicant has the right of access to the remainder of the record.

1.5. Some requests may be subject to payment of a fee required according to College policy or practice for informal access requests and for a formal access request under Section 75 of FIPPA.

1.6. Members of the public may submit formal Freedom of Information requests by writing to the College Privacy Office at [foipp@cnc.bc.ca](mailto:foipp@cnc.bc.ca).

**2. Collection of Personal Information**

2.1. CNC will advise individuals of the purpose for the collection of their personal information, typically through a written notice at the time of collection. In some situations, notice may not be required where otherwise authorized by the Act or other applicable laws.

- 2.2. CNC will limit the collection of personal information to the minimum amount necessary to carry out the College's programs or activities, except as authorized by the Act or other applicable laws.

### **3. Use and Disclosure of Personal Information**

- 3.1. CNC will only use and disclose personal information:
  - 3.1.1. for the purpose the personal information was collected or for other uses consistent with the original purpose for collection;
  - 3.1.2. with the written consent of the individual the personal information is about; or
  - 3.1.3. for any other purpose permitted or required under the Act and other applicable laws.
- 3.2. Personal information will be shared internally on a need-to-know basis. Employees will only be granted access to personal information where necessary to carry out their duties or for other CNC authorized purposes.
- 3.3. Individuals wishing to allow CNC to disclose their personal information to an external third party must complete and sign a consent form.
- 3.4. Any employee who is aware or suspects a privacy incident has occurred or is likely to occur must immediately notify the Privacy Officer.

### **4. Retention and Disposal of Personal Information**

- 4.1. If CNC uses personal information to make a decision that directly affects an individual, that personal information will be retained for at least one year from the date of the decision.
- 4.2. CNC disposes of personal information in accordance with the Records Retention and Destruction Schedule.
- 4.3. CNC 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. CNC will make every reasonable effort to ensure the personal information in its custody or control is complete and accurate.
- 5.2. Individuals may request that their personal information be corrected or annotated as appropriate, with supporting evidence that is satisfactory to the College and in accordance with the Act.

### **6. Storage of Personal Information**

- 6.1. Whenever possible, CNC will only store and disclose personal information inside Canada.
- 6.2. Where storage and/or disclosure outside of Canada is necessary, CNC will complete a Privacy Impact Assessment (PIA) to fully assess and mitigate any risks prior to proceeding with the initiative.

### **7. Duties and Responsibilities**

- 7.1. Subject to the terms of any written delegation of duties by the President, the Privacy Officer and the Privacy Office are responsible for:

- 7.1.1. Overseeing the College's administration of the Act.
  - 7.1.2. Establishing and maintaining CNC's Privacy Management Program.
  - 7.1.3. Providing advice and guidance to the CNC community, conducting investigations, and make privacy recommendations.
  - 7.1.4. Consulting with the CNC community about initiatives involving the use of personal information and supporting the completion of PIAs for such initiatives.
  - 7.1.5. Responding to requests, inquiries, complaints, information access requests, and privacy incidents, including liaising with the Office of the Information and Privacy Commissioner (OIPC).
  - 7.1.6. Maintaining CNC's PIB directory.
  - 7.1.7. Establishing, in consultation with the President and Executive Committee, categories of records available to the public through routine request.
  - 7.1.8. Promoting privacy awareness in the CNC community including offering education and training.
- 7.2. Employees (which includes service providers and volunteers) are responsible for:
- 7.2.1. Handling all personal information in accordance with the Act and this policy. Accessing the minimum amount of personal information necessary for the performance of their duties.
  - 7.2.2. Cooperating with the Privacy Officer in responding to access requests.
  - 7.2.3. Immediately reporting to the Privacy Officer any circumstances where the employee suspects a privacy incident has occurred or is likely to occur.
  - 7.2.4. Cooperating with the Privacy Officer as required in the fulfillment of the College's obligations under this policy and the Act.
  - 7.2.5. Participating in College privacy and access training.
- 7.3. Administrators have responsibility and authority for:
- 7.3.1. Assisting the Privacy Officer, including in responding to access requests by providing records and information, conducting searches, and producing records in a timely manner, and taking action as needed to support compliance with the Act.
  - 7.3.2. Ensuring the programs and activities under their responsibility comply with the Act and this policy.
  - 7.3.3. Ensuring any contract or agreement under their responsibility complies with this policy.
  - 7.3.4. Ensuring policies and procedures under their responsibility are consistent with this policy.
  - 7.3.5. Contacting the Privacy Officer prior to undertaking a new system, project, program, or activity that involves the use of personal information, or making changes to an existing one, to determine whether a PIA is required.
  - 7.3.6. Completing a PIA as identified by the Privacy Officer.
  - 7.3.7. Incorporating PIA requirements into program development and project governance processes under their responsibility.

- 7.3.8. Cooperating with the Privacy Officer on investigations into privacy risks or breaches and implementing any resulting recommendations.
- 7.3.9. Ensuring direct report employees receive training on this policy and the Act.

7.4. The Director Procurement and Ancillary Services has responsibility and authority for:

- 7.4.1. Fulfilling the general responsibilities assigned to Administrators above.
- 7.4.2. Consulting with the Privacy Officer to assess contracts for privacy risks and taking action as necessary, including providing guidance or direction to other Administrators.

7.5. The Chief Information Officer (CIO) has responsibility and authority for:

- 7.5.1. Fulfilling the general responsibilities assigned to Administrators above.
- 7.5.2. Working with the Privacy Officer to investigate privacy and security concerns.
- 7.5.3. Reviewing PIAs for adequacy, consistency, and compliance with CNC information security policies and standards.
- 7.5.4. Working with the Privacy Officer to provide privacy and information security training and awareness.

7.6. The Director, Safety and Security has responsibility and authority for:

- 7.6.1. Fulfilling the general responsibilities assigned to Administrators above.
- 7.6.2. Working with the Privacy Officer to identify and mitigate privacy risks.
- 7.6.3. Working with the Privacy Officer to investigate privacy and security concerns.

**Links to Other Related Policies, Documents, and Websites**

- Freedom of Information and Protection of Privacy Policy #AD-CO-4.14
- Standards of Ethical Conduct Policy #AD-HR-1.05
- Acceptable Use of CNC Information Technology Policy #AD-IT-6.02
- Information Cybersecurity Policy #AD-IT-6.03
- CNC Access and Privacy Webpage
- Records Retention and Destruction Schedule (under review)
- Breach Response Procedures (in development)
- Surveillance of Public Areas Policy (in development)

**Procedure Amendment Log**

Amendment Number:	Date:
0	May 2022
1	
2	