

Procedure Name:	FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY
Approved By:	Policy Review Committee
Approval Date:	January 12, 2026
Next Scheduled Renewal Date:	February 2027
Procedure Holder:	President's Council
Operational Lead:	Director, President's Office
Procedure Number:	ADM-003P



FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY PROCEDURE

1.00 PURPOSE

- 1.1 The purpose of this procedure is to outline the ways in which Coast Mountain College (the College) manages freedom of information (FOI) access requests, privacy impact assessments (PIAs), and privacy breaches in compliance with the [Freedom of Information and Protection of Privacy Act](#) (FOIPPA).

2.00 DEFINITIONS

- 2.1 **Access Request:** A written request made under FOIPPA for access to records under the College's custody or control.
- 2.2 **Applicant:** The individual or organization requesting access to records under the College's custody or control.
- 2.3 **Correction Request:** A request from an individual to correct their personal information that is held by the College.
- 2.4 **Employee:** A person who is employed by the College, including administrators, faculty members, staff, and students when employed by the College (e.g., as student assistants).
- 2.5 **Personal Information:** Recorded information about an identifiable individual, other than contact information used for business purposes.

Personal information includes, but is not limited to: an individual's name; home address and telephone number; age; sex; marital or family status; identifying numbers; race, national or ethnic origin; religious or political beliefs or associations; educational, medical, financial, or criminal history; anyone else's opinions about the individual; the individual's own personal views or opinions and the name, address, or telephone number of a parent, guardian, spouse, or next of kin.

- 2.6 **Privacy Breach:** Any unauthorized access, collection, use, disclosure, loss, or destruction of personal information.
- 2.7 **Privacy Impact Assessment (PIA):** A structured risk assessment conducted to ensure a program, activity, or system complies with FOIPPA and safeguards privacy.
- 2.8 **Privacy Officer:** The senior official designated to oversee and manage all privacy-related matters at the College

- 2.1 **Record:** Any recorded information, in any form, that is created, received, or maintained by the College.
A record includes books, documents, maps, drawings, photographs, letters, vouchers, papers, and all forms of electronic or digital information such as emails, text messages, audio recordings, video recordings, and photographs. A record also includes any other item on which information is recorded or stored by graphic, electronic, digital, mechanical, or other means.
A record does not include a computer program or any other mechanism that produces records.
- 2.2 **The College:** Coast Mountain College (CMTN).
- 2.3 **Third-Party Service Providers:** Individuals, companies, or organizations external to the College that are engaged to perform services or functions on behalf of Coast Mountain College and who may collect, access, use, disclose, store, or manage College records or personal information in the course of providing those services.
- 2.4 **Volunteer:** An individual who provides services to the College and who is not an employee, student, or contractor, but who may have access to College facilities, or personal information in the course of their assigned duties.

3.00 FREEDOM OF INFORMATION (FOI) ACCESS REQUESTS

- 3.1 The College is committed to openness and accountability and will respond to requests for access to records in accordance with the *Freedom of Information and Protection of Privacy Act* (FOIPPA)
- 3.2 Any individual may request access to records in the custody or under the control of the College.
 - a. Requests must be made in writing and submitted to foi@coastmountaincollege.ca.
 - b. Requests should clearly identify the records being sought, including subject matter, relevant dates, and any other details that may assist in locating the information.
 - c. The College encourages individuals seeking general or routine information (such as transcripts or certificates) to make an informal request through the appropriate department prior to submitting a formal FOI request.
- 3.3 When the request is unclear or incomplete, the Privacy Officer will contact the applicant for clarification before proceeding.
- 3.4 When a request becomes excessive, repetitive, frivolous, or otherwise unreasonable, the Privacy Officer may seek authorization from the Office of the Information and Privacy Commissioner to disregard the request.
- 3.5 The Privacy Officer will notify the applicable department(s) and provide direction on the collection and review of responsive records.
- 3.6 Employees must not destroy, conceal, alter, or withhold any record that may be relevant to an FOI access request.
- 3.7 Departments are responsible for maintaining confidentiality throughout the process and must not contact the applicant directly unless instructed by the Privacy Officer.

4.00 PROCESSING FOI REQUESTS

- 4.1 The Privacy Officer is responsible for managing the processing of all formal freedom of information (FOI) requests in accordance with the [Freedom of Information and Protection of Privacy Act](#) (FOIPPA).
- 4.2 The Privacy Officer will:
 - a. review the request to confirm its scope, validity, and applicability under FOIPPA
 - b. identify and coordinate the collection of all responsive records from relevant departments
 - c. examine all records to determine whether any statutory exemptions apply, including but not limited to third-party business information, law enforcement, or personal privacy
 - d. redact information that is exempt from disclosure using approved redaction tools and methods
 - e. prepare a complete response package and accompanying decision letter for issuance to the applicant. The decision letter will:
 - i. state whether access is granted in full, in part, or denied
 - ii. identify the specific sections of FOIPPA that authorize any redactions or refusals
 - iii. advise the applicant of their right to request an independent review by the [Office of the Information and Privacy Commissioner for British Columbia](#) (OIPC-BC).
- 4.3 Where permitted under FOIPPA Section 10, the Privacy Officer may extend the statutory response period.
 - a. The applicant will be notified in writing of the extension, the reason for it, and the anticipated completion date.
- 4.4 The Privacy Officer will maintain complete and accurate documentation of each request, including correspondence, records released, redacted materials, and decisions.

5.00 IDENTITY VERIFICATION

- 5.1 Individuals requesting access to their personal information must provide valid government-issued photo identification before their records are released.
- 5.2 Verification may be completed in person or through secure electronic means when the applicant is unable to attend in person.
- 5.3 When access is requested on behalf of another individual, written authorization from that person must be provided.
 - a. The College reserves the right to confirm authenticity prior to release.

6.00 FEES

- 6.1 Fees may be charged for services related to the processing of freedom of information (FOI) access requests in accordance with Section 75 of the [Freedom of Information and Protection of Privacy Act](#) (FOIPPA).
- 6.2 The Privacy Officer is responsible for determining whether fees apply, preparing a written fee estimate, and providing the applicant with a detailed breakdown before proceeding with the request.

- a. Processing will be suspended until the required payment is received.
- 6.3 Fees may be assessed for the following prescribed services:
 - a. locating and retrieving the record
 - b. producing the record
 - c. preparing the record for disclosure, except for time spent severing information from the record
 - d. shipping and handling the record
 - e. providing a copy of the record.
- 6.4 The first three hours spent locating and retrieving records will be provided at no charge.
 - a. Fees will apply only for time that exceeds this initial three-hour allowance.
- 6.5 No fees will be charged for a request for the applicant's personal information.
- 6.6 The Privacy Officer will maintain documentation of all fee estimates, invoices, and payments.

7.00 PRIVACY IMPACT ASSESSMENTS (PIA)

- 7.1 A privacy impact assessment (PIA) must be conducted before implementing or substantially changing any system, program, or initiative that involves the collection, use, disclosure, or retention of personal information.
- 7.2 A PIA is required when an initiative:
 - a. introduces new information technologies, software, or surveillance tools
 - b. changes how personal information is collected, stored, shared, or disclosed
 - c. involves third-party service providers, contractors, or cloud-based services
 - d. consolidates or integrates multiple datasets containing personal information.
- 7.3 The Privacy Officer determines whether a PIA is required based on scope and risk.

8.00 PIA PROCESS

- 8.1 Departments must notify the Privacy Officer at the planning stage of any initiative that may involve personal information.
- 8.2 The Privacy Officer and Project Lead review the proposal to define the scope, identify risks, and confirm required documentation.
- 8.3 The responsible Employee completes the College's approved PIA template in consultation with the Privacy Officer.
- 8.4 The Privacy Officer reviews the PIA for completeness, accuracy, and compliance with FOIPPA.
 - a. Risk mitigation strategies are documented and, where necessary, coordinated with the Director of Information Technology and Chief Information Officer (CIO) or Legal Counsel.
- 8.5 The President & CEO or delegate reviews and approves the final PIA before the system, contract, or activity proceeds.

a. No initiative may move forward until approval has been granted.

8.6 The Privacy Officer retains approved PIAs and supporting documentation.

8.7 Departments are responsible for notifying the Privacy Officer of any material change that may require an updated PIA.

9.00 PRIVACY BREACHES

9.1 All employees, contractors, and volunteers must report any suspected or confirmed privacy breach immediately to their department manager and the Privacy Officer.

9.2 The Privacy Officer records the incident, initiates containment, and provides notification to the President & CEO and or Vice-President, Corporate Services and Chief Financial Officer (CFO).

9.3 The Privacy Officer leads the privacy investigation with the relevant departments, assess the scope and the cause of the breach, oversees containment, and coordinates any necessary technical or administrative controls.

9.4 When a breach presents a risk of significant harm, the Privacy Officer ensures that affected individuals and the [Office of the Information and Privacy Commissioner for British Columbia](#) (OIPC-BC) are notified in accordance with FOIPPA requirements.

9.5 Following each privacy incident, the Privacy Officer will:

a. submit a privacy incident report to OIPC-BC

b. retain a copy of the submitted report

c. identify required corrective and preventive measures

d. oversee the implementation of corrective and preventive measures

e. review the privacy management program and applicable security safeguards to determine whether updates or enhancements are required.

10.00 CORRECTION REQUESTS

10.1 Individuals have the right to request correction of their personal information that is held by the College when it is inaccurate or incomplete.

10.2 Requests submitted to the relevant department, identifying the record in question, and the correction sought will be responded to within 10 business days.

a. Where an individual believes that their request has not been satisfactorily resolved, the Privacy Officer may be consulted to support clarification and next steps.

10.3 The Relevant Department will:

a. review the request

b. provide a written response within 30 business days, either confirming the correction or explaining the reason for refusal.

10.4 Where a correction is refused, the individual will be informed of their right to request a review by the [Office of the Information and Privacy Commissioner for British Columbia](#) (OIPC-BC).

11.00 RELATED POLICIES, PROCEDURES, AND GUIDELINES

- 11.1 [ADM-003, Freedom of Information and Protection of Privacy Policy](#)
- 11.2 [ADM-011, Records Management Policy](#)
- 11.3 [ADM-011P, Records Management Procedure](#)
- 11.4 [HMR-001, Employee Code of Conduct Policy](#)
- 11.5 [INF-001, Acceptable Use of Information Resources Policy](#)
- 11.6 [INF-003, User Account Management Policy](#)
- 11.7 [INF-005, College Data Classification Policy](#)

12.00 OTHER SUPPORTING DOCUMENTS

- 12.1 [Freedom of Information and Protection of Privacy Act \(FOIPPA\)](#)

13.00 HISTORY

Created/Revised/ Reviewed	Approval Date	Author's Role	Approved By
Created	2017		Board of Governors
Revised	June 1, 2024	Director, President's Office	Board of Governors
Revised	January 12, 2026	Director, President's Office	Policy Review Committee