B - 14

CANADORE COLLEGE

CORPORATE POLICY MANUAL

TITLE: **Protection of Privacy**

EFFECTIVE DATE: **November 18, 2025**

---

1. SCOPE

1.1 Authority

This policy is issued under the authority of the Board of Governors.

1.2 Application

This policy applies to:

- Employees;
- Students;
- Researchers;
- Associates;
- Contractors; and
- Agents

of The Canadore College of Applied Arts and Technology (hereafter referred to as "Canadore" or "the College") who collect, access, use, disclose, retain, or dispose of information on behalf of the College.

2. PURPOSE AND PRINCIPLES

2.1 The purpose of this policy is to set principles and controls for lawful collection, use, disclosure, retention, disposal, and safeguarding of personal information and, where applicable, personal health information. It advances transparency, privacy by design, and data minimization.

2.2 This policy is intended to:

- Promote information lifecycle safeguards and data controls in all systems and programs.
- Require documented Privacy Impact Assessments (PIAs/DPIAs) for new or materially changed systems or vendors that process PI/PHI.
- Provide clear collection notices describing purposes, legal authority, and contacts.

- Prefer de-identified/aggregated data for analytics, reporting, and external disclosures.
- Ensure appropriate security controls, role-based access and training that provide data users with guiding principles for the collection, use, disclosure and retention of personal information in the custody of the College that comply with applicable legislation.

3. DEFINITIONS

3.1 Personal information (PI)

Recorded information about an identifiable individual as defined by FIPPA, including but not limited to demographic information, identifying numbers, financial transactions, education/employment history, personal views, and correspondence that would reveal identity.

3.2 Personal Health Information (PHI)

Information related to an individual's physical or mental health, health history, care, or payment, as defined by PHIPA*; includes information that identifies an individual or could reasonably identify them. **Applies where the College or a unit acts as a Health Information Custodian (HIC).*

3.3 FIPPA

Freedom of Information and Protection of Privacy Act (Ontario).

3.4 PHIPA

Personal Health Information Protection Act (Ontario) and regulations.

3.5 PIPEDA

Personal Information Protection and Electronic Documents Act (Canada) – applies to College activities that are commercial in nature (e.g., retail to the public, fee-for-service offerings), in addition to provincial law.

3.6 CASL

Canada's Anti-Spam Legislation governing commercial electronic messages (consent, identification, and unsubscribe requirements).

3.7 Confidential Information

Information intended for limited distribution and not generally or publicly available (e.g., human resource records, draft materials, proprietary third-party information, assessments).

3.8 Custody

Collection, use, integrity, storage, and security of a record for a legitimate business purpose.

3.9 Data Steward

An individual accountable for a defined set of data, including quality, access, retention, and breach preparedness within their domain.

3.10 De-identification

Processing data to remove personal information in accordance with IPC De-identification Guidelines for Structured Data; residual re-identification risk must be assessed prior to disclosure, analytics, or public release.

3.11 Employees, Contractors, and Agents

Employees, Contractors, and Agents represent the college and complete required privacy training and follow College policies and procedures, including breach reporting without delay.

3.12 Privacy Officer/Privacy Office

The Privacy Officer oversees compliance; advises on FIPPA/PHIPA/PIPEDA/CASL; maintains procedures; manages PIAs/DPIAs; coordinates training; manages FOI responses and breach responses; and serves as contact for privacy inquiries and complaints.

4. POLICY

4.1 Lawful Collection & Notices

The College collects only what is necessary for explicit, legitimate purposes identified at or before collection. Individuals are informed of purposes, legal authority, and a College contact responsible for responding to questions. Program-specific notices (students, applicants, employees, alumni, partners, regulated programs, community, etc.) will be published or linked. The College takes reasonable steps to ensure personal information is accurate, complete and up to date where it is used to make decisions about individuals.

4.2 Use, Disclosure & Data Sharing

PI/PHI is used and disclosed only for the identified purposes or as authorized by law. Data sharing agreements and contracts with third-party service providers must include privacy and security requirements, incident reporting, audit, and restrictions on secondary use.

4.3 Cross-border Processing

Where systems or service providers store or access information outside Canada, collection notices will indicate applicable jurisdictions and associated risks; contracts must require equivalent safeguards and breach reporting.

4.4 Access & Correction Rights

Individuals may request access to and correction of their information under FIPPA, or

PHIPA where applicable. The College will respond within statutory timelines and escalate complex cases to the Privacy Office.

4.5 Privacy Impact Assessment

A Privacy Impact Assessment is required before launching or materially changing systems, services, or research projects that involve PI/PHI, or introduce new data linkage, automated decision-making, or high-risk analytics.

4.6 De-identification & Open Data

When sharing datasets internally or externally, the College will prefer de-identified/aggregated data and apply recognized techniques to mitigate identification risk.

4.7 Security Controls & Training

The College maintains administrative, technical, and physical safeguards proportionate to risk, including role-based access, encryption in transit/at rest (where feasible), audit logging for PHI, vendor due diligence, and annual privacy training for employees and contractors.

4.8 Breach Response

The College maintains a Breach Response Procedure consistent with IPC guidance: identify, contain, assess risk, notify, remediate, document, and review. Notification to affected individuals and, where required, to the IPC occurs at the first reasonable opportunity. For PHI, annual breach statistics are reported to the IPC by March 1 for the prior calendar year.

4.9 Retention & Disposal

Information is retained according to approved records retention schedules and securely destroyed (paper and electronic media) when no longer required or upon expiry of statutory retention periods. Public summaries of retention schedules will be posted where feasible.

4.10 Research

Human participant research complies with Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2 (2022)) and applicable law. Research involving PI/PHI must undergo ethics review and, where relevant, a PIA/DPIA.

4.11 Commercial Activities

Where the College engages in commercial activities, PIPEDA applies in addition to provincial law. Commercial electronic messages comply with CASL, including consent management and unsubscribe.

5. ROLES AND RESPONSIBILITIES

5.1 Board of Governors

The Board of Governors is responsible for the initial approval of the policy and subsequent amendments.

5.2 President

The President is responsible for the overall management and operation of the College. The President will ensure the policy is implemented and that compliance is monitored.

6. EVALUATION

This policy will be evaluated every 3 years.

7. RELATED AND REFERENCED DOCUMENTS

FIPPA (Ontario)
PHIPA and regulations
IPC Privacy Breach Guidelines
IPC De-identification Guidelines
TCPS 2 (2022)
PIPEDA (where applicable)
CASL guidance (where applicable)