Personal Information and Protection of Privacy

Number:	1.2.1
Responsible Executive:	President
Approval Authority:	Senior Leadership Team
Effective Date:	January 30, 2026
Next Review Date:	January 29, 2031
Revised Date:	
Category:	Administrative
Replaces:	1.2.1 PIPP for Students
Merges:	1.3.9 PIPP for Employees and Volunteers

PURPOSE

This policy establishes the framework for the collection, use, disclosure, retention, and safeguarding of Personal Information at Coquitlam College ("the College").

SCOPE

This policy applies to all:

- Students (prospective, current, and former);
- Parents/guardians of grades 10–12 students;
- Employees (permanent, temporary, casual, contract);
- Volunteers and contractors acting on behalf of the College; and
- Visitors or individuals interacting with the College.

In applying this policy, the College recognizes that privacy obligations may vary depending on a student's program of enrolment (e.g. grade 10–12 or post-secondary) and the student's age and legal capacity under British Columbia law.

POLICY STATEMENTS

1. The College complies with applicable privacy legislation, regulations, and ministerial requirements in the administration of this policy.
2. The College's privacy framework is guided by the Ten Privacy Principles: accountability, purpose, consent, limiting collection, use/disclosure/retention, accuracy, safeguards, openness, access, and complaint process.
3. All Personal Information is classified as Confidential under the College's Information Security Policy (1.2.3).
4. The College does not sell, trade, or lease Personal Information.
5. This policy is supported by related College policies that address information, confidentiality, and privacy matters.

PROCEDURES

Principle 1: Accountability

6. The President is the Privacy Officer and may delegate operational responsibilities to trained staff who are responsible for day-to-day implementation of compliance measures.

7. All employees, volunteers, and contractors must comply with privacy requirements outlined in College policies and procedures, or as required by law.

Principle 2: Purposes

8. The College collects Personal Information only for purposes directly connected to its educational, administrative, and employment responsibilities, including:
    - Students (grades 10–12 and post-secondary): admission, enrollment, academic progress, program delivery, student services, and government reporting.
    - Employees/Volunteers/Contractors: recruitment, payroll/benefits, qualifications, criminal record checks, performance management, and statutory compliance.
    - Operations: communications, fundraising, events, IT systems, safety/security, regulatory reporting, and compliance.

Principle 3: Consent

9. Consent is required for the collection, use, or disclosure of Personal Information, except where exemptions are applicable by law.
10. For grade 10–12 students, consent is normally obtained from a parent/guardian, as permitted or required by law. The College may share student information with professional health providers, social service agencies, or other support service professionals for the purpose of planning or delivering services to students under 19 years of age without consent of a parent/guardian.
11. For post-secondary students, consent must be obtained directly from the student (parents/guardians do not have automatic access even if the student is under 19 years of age).
12. Consent may be express or implied depending on the sensitivity of the information. Express written consent is required for:
    a. Publication of names, photos, or bios in external marketing or online.
    b. Collection or disclosure of health and other sensitive Personal Information.
    c. Cross-border transfers where data may be stored or accessed outside Canada.
13. The disclosure of student information related to conduct or disciplinary matters will align with the College's relevant student conduct policies.

Principle 4: Limiting Collection

14. The College collects only the minimum information necessary to fulfill the purposes identified at or before the time of collection.

Principle 5: Use, Disclosure, and Retention

15. Personal information is used or disclosed only for identified purposes or as permitted or required by law.
16. Disclosures may include:
    a. Government bodies, such as the Ministry of Education and Child Care and Immigration, Refugees and Citizenship Canada.
    b. Other educational institutions for student record transfers, with consent or where legal authority exists.
    c. Service providers, under contractual safeguards consistent with PIPA.
    d. Law enforcement agencies, regulatory bodies, or other authorities, where disclosure is authorized or required by law.
17. If Personal Information is stored or accessed outside Canada, the College will implement reasonable contractual, technical, and organizational safeguards.

18. The retention and destruction of records will comply with legal and regulatory requirements and follow timelines listed in the College's Records Retention Schedule.

Principle 6: Accuracy

19. The College will take reasonable steps to keep information current, accurate, and complete.
20. Individuals are responsible for providing updates to their information to the Registrar (students) or Human Resources (employees).
21. Requests to correct information must be submitted in writing to the Office of the Registrar. Approved corrections will be made and, where appropriate, communicated to third parties. If a correction is denied, the decision will be communicated, and a statement of disagreement will be attached.

Principle 7: Safeguards

22. Records are stored in secure physical environments and/or restricted-access systems.
23. Electronic records are protected with appropriate technical safeguards including authentication, access controls, firewalls, and encryption.
24. Monitoring of IT systems, email, and surveillance tools is conducted only for legitimate operational, security, or compliance purposes.
25. Employees, volunteers, and contractors will receive relevant privacy training. Breaches of privacy obligations may result in discipline or termination of employment, volunteer, or service roles.

Principle 8: Openness

26. This policy is publicly available on the College website.
27. Additional information regarding the College's privacy practices may be obtained from the Privacy Officer.

Principle 9: Access

28. Access rights are determined in accordance with applicable legislation and the student's program of enrolment and legal capacity.
29. Individuals may request access to their Personal Information.
    a. For grade 10–12 students, parents/guardians may access student records in accordance with the *Independent School Act* and ISB requirements.
    b. For post-secondary, students control access to their own records.
30. Access will be provided within 30 business days, unless prohibited by law.

Principle 10: Complaints

31. Complaints may be submitted in writing to the Privacy Officer.
32. If unresolved, complaints may be escalated to the Office of the Information and Privacy Commissioner for BC (OIPC), the Independent Schools Branch (ISB), or the Federation of Independent School Association (FISA BC), depending on the nature of the matter.

Privacy Breach Response

33. All suspected or actual breaches of privacy must be reported immediately to the Privacy Officer. The College will:
    - Contain the incident;
    - Assess the risk and impact;

- Notify affected individuals, OIPC, and ministries as required; and
- Implement corrective/preventive measures.

DEFINITIONS

Access: The ability for an individual to view, or obtain copies of their Personal Information, subject to law and verification of identify prior to release.

Contact Information: Business contact details (name, title, business address, phone, or email). This is not considered Personal Information under PIPA.

Employee: An individual employed by the College in any capacity (full-time, part-time, permanent, temporary, term, casual, or contract). Contractors may also be subject to this policy where applicable.

Express Consent: Consent that is explicitly provided, either verbally or in writing, to the collection, use, or disclosure of Personal Information.

Implied Consent: Consent that can reasonably be inferred from an individual's actions, inaction, or the circumstances of the collection, use, or disclosure of personal information.

Personal Information: Recorded information about an identifiable individual, excluding Contact Information. Examples include home address, birth date, grades, employee files, photographs, or health and financial information.

Privacy Breach: The theft, loss, or unauthorized collection, use, disclosure, or disposal of Personal Information in the custody or control of the College or its Service Providers.

Privacy Complaint: A concern raised by any individual about how the College has handled Personal Information.

Record: Any recorded information created, received, or maintained by the College in any medium, that is in its custody or control.

Service Provider: An external individual or organization who are under contract or agreement to provide services on behalf of the College. Service providers must comply with PIPA and contractual privacy obligations.

Student: A prospective, current, or former individual enrolled in grade 10–12 or post-secondary courses or programs at the College.

Volunteer: An individual who provides services to the College without remuneration. Volunteers are subject to privacy requirements, including criminal record checks as required by the *Independent School Act*.

RELATED RESOURCES

- Records Management Policy 1.2.2
- Information Security Policy 1.2.3
- Video Surveillance and Security Recordings Policy 1.2.4
- Personal Information Protection Act, SBC 2003, c 63
- Criminal Code, RSC 1985, c C-46
- Independent School Act, RSBC 1996, c 216
- *Student Records Requirements and Best Practice Guidelines for Independent Schools (2021)*