Records Management

Number:	1.2.2
Responsible Executive:	Registrar
Approval Authority:	Senior Leadership Team
Effective Date:	January 30, 2026
Next Review Date:	January 29, 2031
Revised Date:	
Category:	Administrative

PURPOSE

This policy establishes standards for the management of records at Coquitlam College (the College). It supports compliance with provincial legislation and ministerial requirements, promotes accountability and transparency, safeguards personal information, and preserves the College's institutional memory.

SCOPE

This policy applies to all College employees, contractors, volunteers, and agents who create, receive, maintain, or manage institutional records in any format (paper, electronic, audiovisual, digital, or cloud-based).

A separate policy, Student Records (High School) 4.1.8, governs the creation, maintenance, and protection of student records specific to the College's high school program.

POLICY STATEMENTS

1. The College manages records in accordance with all applicable laws and standards, including the *Independent School Act (ISA)*, *ISB Student Records Requirements and Best Practice Guidelines*, the *Personal Information Protection Act (PIPA)*, and relevant requirements of the *Ministry of Post-Secondary Education and Future Skills*.
2. All records created, received, or maintained by employees as part of College operations are institutional assets and the property of the College, regardless of format or storage location.
3. The President serves as the College's Privacy Officer and is accountable for institutional compliance with privacy and records-management obligations under applicable legislation.
4. The College maintains a Records Retention Schedule (RSS) that classifies all institutional records, establishes retention periods, and outlines secure storage, preservation, and destruction methods.
5. Records must be protected against unauthorized access, loss, alteration, or destruction. Enhanced safeguards will be applied to records containing personal or sensitive information.
6. Access to records is granted on a need-to-know basis for legitimate academic, administrative, or legal purposes, consistent with *PIPA* and the College's Personal Information and Protection of Privacy Policy (1.3.9).

PROCEDURES

Oversight

7. The Registrar is the designated Records Management Officer (RMO) responsible for:
    a. implementing this policy and related procedures across departments;
    b. maintaining and updating the official Records Retention Schedule (RSS);
    c. conducting regular compliance reviews to verify that records are managed, retained, and destroyed in accordance with approved standards; and
    d. reporting breaches, losses, or unauthorized destruction of records to the Privacy Officer.
8. The Privacy Officer provides institutional oversight and approves updates to the RSS and related procedures.
9. Department Heads must ensure that records under their authority are created, classified, and retained in accordance with this policy and the RSS.
10. Employees are responsible for accurately creating, managing, and protecting the records they handle as part of their duties.
11. All employees are accountable for compliance with this policy and may be subject to disciplinary action for breaches.

Record Creation and Management

12. Employees must use approved systems to create and manage records that accurately document official College decisions and actions.
13. Records must be created, stored, and managed in authorized recordkeeping systems. Personal devices, local hard drives, portable media, and personal email accounts must not be used to store or transmit institutional records.
14. Correspondence or communications that document a decision, commitment, or obligation of the College must be saved to the appropriate system of record within five (5) business days. Examples include:
    - student academic or disciplinary decisions;
    - approvals of accommodations or program adjustments;
    - financial authorizations or agreements; and
    - formal communications with external agencies or sponsors.
15. Records should be created at the time of the activity and include sufficient context, including author and date, to ensure clarity and accountability.

Access and Retrieval

16. Records must be organized and stored to support efficient retrieval for academic, administrative, legal or accountability purposes.
17. Access to College records is restricted to authorized individuals with a legitimate business need, consistent with PIPA and College privacy policies.
18. Requests for access to personal information must be made in writing to the RMO and will be processed within 30 business days, unless an extension is authorized by law.
19. Employees must not share or email records containing personal information without encryption or prior authorization from the RMO.
20. Requests from external agencies (e.g., law enforcement, legal counsel, or regulators) must be directed to the RMO. Only the minimum necessary information may be released when responding to such requests.

21. All access to institutional records must be logged, including the date, requestor, purpose, and information released. Records containing health, counselling, or other sensitive personal information must be stored separately and accessible only to staff with a legitimate need to know.
22. The Registrar will ensure that access practices comply with the College's *Personal Information and Protection of Privacy Policy*, *Information Security Policy*, and *Records Retention Schedule*.

Access to Student Records

23. Authorized Access Within the College
    a. Access to student records will be limited to College personnel who require the information to perform legitimate educational, administrative, or legal duties.
    b. Staff granted access must use the information solely for the purpose for which it was collected, protect its confidentiality, and not further share or disclose it except as permitted by law or policy.
    c. The Registrar (or designate) must maintain a log of all internal and external access to student records.
24. Access by Students
    a. A student has the right to access their own student record, consistent with *PIPA*, the *Independent School Act*, and Ministerial Order 41/91.
    b. Access may be denied or limited only where:
        - it would reveal personal information about another individual;
        - it would threaten the safety or physical/mental well-being of any person;
        - it contains confidential evaluations supplied in confidence; or
        - it is protected by solicitor-client privilege.
    c. Students may request corrections to their personal information where errors or omissions are identified.
25. Access by Parents or Guardians
    a. For students under the age of 19, a parent or legal guardian has the right to examine the student's record and to receive copies, except where prohibited by a court order or other legal restriction.
    b. Both custodial and non-custodial parents may access records unless a court order or legal agreement explicitly limits this right.
    c. The College must take reasonable steps to verify the identity and legal authority of a parent or guardian before granting access.
    d. Where a student aged 19 or older provides written consent, parents or guardians may be granted access to relevant portions of the student's record.
26. Access by Education, Health, or Social-Service Professionals
    a. In accordance with the *ISB Student Records Requirements and Best Practice Guidelines*, access to student records may be granted, without the student's or parent's consent, to professionals who are planning for or delivering education, health, social, or other support services to the student, provided confidentiality is assured.
    b. Such access is restricted to the information necessary to plan or provide the relevant service.
    c. The professional receiving access must:

- use the information solely for the stated purpose;
- maintain the confidentiality of the information; and
- not further disclose it except as authorized by law or College policy.

d. All such access must be authorized and recorded by the Registrar (or designate).

27. Access Without Consent in Emergencies or Health/Safety Circumstances

    a. Under section 18 of *PIPA* and consistent with the ISA, personal information may be accessed or disclosed without consent if the information:
        - is clearly in the interests of the student and consent cannot be obtained in a timely manner; or
        - is necessary to respond to an emergency that threatens the life, health, or security of the student or another individual.
    b. Any such access or disclosure must be documented and reported immediately to the Privacy Officer.

Classification, Retention, and Disposal

28. Records must be classified, retained, and disposed of in accordance with the RSS and Information Security Policy (1.2.3), which defines information categories (Public, Internal, Confidential) and corresponding protection requirements.
29. Retention periods must comply with legislative, regulatory, and operational obligations and must reflect the sensitivity and classification level of the record.
30. No record may be altered, deleted, or destroyed except as authorized under the RSS. Destruction of records must be:
    a. Approved by the Records Management Officer;
    b. Conducted securely, using methods appropriate to the classification of the record (e.g., cross-shredding for paper, certified permanent deletion or secure erasure for digital); and
    c. Documented in a *Records Disposal Log* that includes the authorization, record type, date, and method of destruction.
31. Records subject to audits, investigations, or legal proceedings must not be destroyed until explicitly authorized by the President or RMO.

Storage, Security, and Protection

32. Records containing personal, financial, or confidential information must be stored in secure environments with controlled access, consistent with the classification and technical standards outlined in the Information Security Policy (1.2.3).
33. Physical records must be stored in locked cabinets or restricted-access rooms. Electronic records must be protected using secure passwords, encryption, and firewalls, with limited access to authorized personnel only.
34. Regular backups of critical electronic records must be maintained and tested for recoverability, and stored in secure, access-controlled environments.
35. The College's IT department or authorized third-party vendors must ensure that all data storage and backup locations comply with Canadian privacy and data-protection laws, including requirements for storage within Canada where applicable.
36. Portable devices (laptops, USB drives, external hard drives) must be encrypted and may not be used for long-term or sole record storage of official records.

37. Records containing personal or confidential information must never be stored on personal devices, email accounts, or unapproved cloud services.

Training and Support

38. The RMO, in collaboration with HR, will provide training for employees during onboarding and through period refresher sessions. Training includes:
    a. PIPA and confidentiality principles;
    b. Proper use of recordkeeping systems;
    c. Classification, retention, and disposal procedures; and
    d. Reporting of incidents and breaches.

Privacy Breach and Incident Reporting

39. Any loss, unauthorized access, or misuse of personal information must be reported immediately to the Privacy Officer (President).
40. The Privacy Officer will initiate the *Privacy Breach Response Plan* and, if required, notify affected individuals and the Office of the Information and Privacy Commissioner (OIPC).
41. The Records Management Officer will coordinate with IT and relevant departments to contain the incident, recover records if possible, and document the response

DEFINITIONS

Employee: An individual employed by the College on a full-time, part-time, permanent, temporary or contract basis.

Record: Information created, received, or maintained as evidence of College business, regardless of format (paper, electronic, audiovisual, digital).

Records Management: The systematic control of records throughout their lifecycle, including creation, maintenance, storage, retrieval, retention and secure disposal.

Records Retention Schedule (RSS): A timetable specifying retention periods, storage requirements, and approved disposal methods.

RELATED RESOURCES

- Personal Information and Protection of Privacy Policy 1.2.1
- Information Security Policy 1.2.3
- Video Surveillance and Security Recordings Policy 1.2.4
- Coquitlam College Records Retention Schedule (internal)
- Independent School Act, RSBC 1996, c 216
- Personal Information Protection Act, SBC 2003, c 63