COQUITLAM COLLEGE
Established 1982

POLICY AND PROCEDURES

Information Security

Number:	1.2.3
Responsible Executive:	President
Approval Authority:	Senior Leadership Team
Effective Date:	January 30, 2026
Next Review Date:	January 29, 2031
Revised Date:	
Category:	Administrative

PURPOSE

This policy establishes consistent practices for managing access to information and ensures that Coquitlam College (the College) maintains appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of all information systems and assets.

SCOPE

This policy applies to all employees, contractors, volunteers, and agents of the College, and covers all information assets (digital and physical) created, received, stored, or maintained by the College in support of its operations.

POLICY STATEMENTS

1. Information created, received, or maintained in the course of College business is an institutional asset and will be governed by policies and controls that ensure its protection, appropriate use, and long-term preservation.
2. The College will protect information against unauthorized access, use, alteration, loss, or destruction, while ensuring that it remains accurate, reliable, and available to authorized users.
3. Privacy and security considerations will be integrated at every stage of information management, including system design, procurement, deployment, and operation.
4. All College data will be classified as Public, Internal, or Confidential and managed according to its sensitivity and potential impact of disclosure or misuse. Access to information will follow the Need-to-Know and Least-Privilege principles, ensuring that employees have only the access necessary to fulfill their responsibilities.
5. The College will respond promptly to suspected or confirmed security or privacy breaches. Where required under the *Personal Information Protection Act (PIPA*), affected individuals and the Office of the Information and Privacy Commissioner (OIPC) will be notified.

PROCEDURES

Responsibilities

<u>President</u>

6. The President holds executive responsibility for the College’s information security and privacy framework and, as the designated Privacy Officer, is accountable for fostering a culture of accountability and ensuring institutional compliance with all privacy and information security requirements.

The President will:

- Oversee the development, implementation, and continuous improvement of the information security program and related policies.
- Confirm that administrative, physical, and technical safeguards are in place to protect College information.
- Authorize audits, privacy reviews, and incident response evaluations to assess compliance.
- Receive reports on incidents or vulnerabilities and oversee corrective action.

7. The President, as the College's designated Privacy Officer, may delegate some or all day-to-day privacy and information security responsibilities to the Alternate Privacy Officer or other qualified delegates, as appropriate.

Data Steward

8. Data Stewards are responsible for classifying, handling, and managing information within their operational areas and serve as the primary contact for information integrity and access within their departments.
   Data Stewards will:
   - Identify and document information assets within their department.
   - Confirm staff understand and apply correct data handling practices.
   - Authorize access to departmental information based on legitimate need.
   - Work with the IT Custodian on technical configurations and access permissions.
   - Support employee awareness and training on secure data handling and storage.
   - Report suspected or confirmed data incidents to the President.

System Administrator

9. The System Administrator manages and protects the College's technology infrastructure to ensure system reliability and compliance.
   The System Administrator will:
   - Maintain and monitor all physical and virtual infrastructure, including servers, networks, and hardware.
   - Implement technical safeguards such as firewalls, patching, intrusion detection, and encryption.
   - Perform and test backups and disaster recovery to ensure data integrity.
   - Conduct vulnerability testing.
   - Conduct risk assessments for new or substantially changed systems.
   - Maintain a current inventory of all hardware and network assets, documenting configurations and lifecycle status.
   - Provide technical assistance during incident response
   - Ensure compliance with Canadian privacy and data protection standards.

IT Custodian

10. The IT Custodian administers data environments and access controls to safeguard the confidentiality, integrity, and availability of College information.
    The IT Custodian will:
    - Manage user accounts, permissions, and passwords as authorized by Data Stewards.
    - Maintain secure file structures and cloud environments.
    - Conduct access reviews and modify permissions when roles change.

- Coordinate with the System Administrator on data integrity and backups.
- Maintain documentation of configurations and access logs.
- Report security incidents to the President.

Data Users

11. Every member of the College community shares responsibility for protecting information and accessing only the information necessary for their work.
    Data Users will:
    - Use College information and systems only for legitimate business purposes.
    - Handle and store data according to its classification level and related College policies.
    - Protect passwords, devices, and physical records from loss, theft, or unauthorized use.
    - Immediately report any suspected breach, phishing attempt, or loss.
    - Complete assigned privacy and security training.

Data Classification and Handling

12. All information collected, created, or maintained by the College must be classified according to its sensitivity, value, and potential impact if disclosed, altered, or lost and must be handled in accordance with this policy and the Records Management Policy (1.2.2).

Class 1 – Public Information

Public Information is material formally approved for unrestricted release. Its disclosure poses no risk to the College, its students, employees, or partners.

Handling Requirements:

- May be shared, distributed, or published without restriction once authorized.
- Must be accurate, current, and approved by the appropriate administrator prior to publication.
- Stored and transmitted using standard College systems; encryption is not required.
- Updates and corrections must follow established approval and records-management procedures to ensure authenticity and version control.

Examples:

- Published academic calendars, brochures, and advertising materials
- Content on the public website and official social-media channels
- Publicly available policies, procedures, reports, and course outlines
- Institutional statistics or announcements already released to the public

Class 2 – Internal Information

Internal Information is intended for internal use within the College community. While not public or confidential, unauthorized disclosure could cause reputational, operational, or financial harm to the College or its stakeholders and may include administrative, instructional, or operational data.

Handling Requirements:

- Share only with employees, contractors, or instructors who have a legitimate business or educational need.

- Store in College-managed drives, databases, or other approved systems with access controls.
- When transmitting outside the College, use secure methods such as password-protected or encrypted attachments.
- Keep printed materials in staff-only areas; dispose of using shredding or locked bins.
- Disclosure to external parties requires written approval from the President or relevant Data Steward.

Examples:

- Draft policies, meeting minutes, and internal communications
- Departmental plans and schedules
- Non-public academic materials, exam templates, and internal assessment data
- Internal contact lists, routine employee correspondence, and procedural manuals

Class 3 – Confidential Information

Confidential Information is highly sensitive, legally protected, or critical to College operations. Unauthorized disclosure could cause significant harm to individuals or to the College's legal, financial, or reputational interests and includes all personal information under PIPA as well as information subject to contractual or legal confidentiality obligations.

Handling Requirements:

- Access limited to authorized individuals whose duties require it; all access must be documented.
- Store in secure, access-controlled systems; use encryption both in transit and at rest where feasible.
- Keep physical copies in locked cabinets or rooms with restricted access.
- Never send to personal email or store on unauthorized devices or cloud services.
- Transmit or access remotely only through encrypted channels (VPN, secure file-transfer).
- Destroy or delete securely following the *Records Management Policy (1.2.2)*.
- Report any loss, theft, or suspected breach immediately to the President.
- Handling must comply with *PIPA*, *ISA*, and applicable contractual obligations.

Examples:

- Student records, including Permanent Student Records (PSR Form 1704), official transcripts, grades, and disciplinary files
- Employee files, payroll and banking details, and performance reviews
- Financial statements, vendor contracts, and proprietary business data
- Health, medical, accessibility, or counselling records
- Passwords, encryption keys, and security configurations

Access and System Security

13. Access to information is based on Least Privilege / Need-to-Know Principle.
14. Requests for access must be approved by the appropriate Data Steward and implemented and tracked by the IT Custodian.
15. Permissions should be reviewed regularly or when roles or employment status change.
16. The System Administrator and IT Custodian will ensure that all College systems:

  a. Use strong authentication and password protocols;
  b. Are regularly updated, patched, and monitored for vulnerabilities;
  c. Are protected by firewalls, antivirus, and encryption where appropriate;
  d. Maintain secure, verified backups stored off-site or in approved cloud environments; and
  e. Are decommissioned securely (e.g., drive wiping, credential removal) when retired in accordance with the Records Management Policy (1.2.2).

17. Unauthorized attempts to access information are prohibited and may lead to disciplinary action.
18. Third-party vendors or service providers that store or process College data must meet equivalent security and privacy standards and comply with this policy.

Monitoring and Compliance

19. The System Administrator and IT Custodian will maintain appropriate monitoring of information systems and access logs to detect unauthorized activity.
20. The President or designate will ensure that periodic audits, risk assessments, and policy reviews are conducted. Findings will be used to improve institutional safeguards and staff awareness.

Training and Awareness

21. New employees will receive information security training during onboarding.
22. The College will provide specialized training and periodic refreshers for employees whose duties involve elevated information-security responsibilities.

DEFINITIONS

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

Information Asset: Any recorded information, data set, or system that supports the College’s teaching, learning, administrative, or operational activities.

Least Privilege / Need to Know Principle: Individuals are granted only the minimum level of access privileges and the specific information they require to perform their job functions. Access is limited both in terms of actions they can take (least privilege) and the data they can see (need to know), ensuring risks from unauthorized use or exposure are minimized.

RELATED RESOURCES

- Personal Information and Protection of Privacy Policy 1.2.1
- Records Management Policy 1.2.2
- Video Surveillance and Security Recordings Policy 1.2.4
- Employee Professional Standards and Conflict of Interest Policy 3.1.2
- Personal Information Protection Act, SBC 2003, c 63
- Independent School Act, RSBC 1996, c 216