Acceptable Use of Information and Educational Technology

Number:	1.2.5
Responsible Executive:	President
Approval Authority:	Senior Leadership Team
Effective Date:	January 30, 2026
Next Review Date:	January 29, 2031
Revised Date:	
Category:	Administration

PURPOSE

This policy establishes expectations for the responsible and secure use of Coquitlam College's information technology resources. Its purpose is to support the College's academic and administrative activities, protect the integrity of College systems, and ensure that all users act in a lawful, ethical, and respectful manner.

SCOPE

This policy applies to all members of the College community, including students, employees, contractors, volunteers, and others who access or use College information technology resources. It covers all devices, networks, systems, applications, accounts, and data provided or supported by the College, whether accessed on campus or remotely.

POLICY STATEMENTS

1. The College expects all users of its information and educational technology to use these resources responsibly, lawfully, and in ways that support teaching, learning, and administrative activities.
2. College technology resources must be used in a manner that protects the security, integrity, and availability of systems and information, and that complies with all applicable laws and College policies.
3. Users are responsible for safeguarding their accounts, credentials, and devices, and for promptly reporting any suspected security incidents, misuse, or unauthorized access.
4. The use of College technology must not:
    a. involve illegal, harmful, or disruptive activities;
    b. compromise the privacy or security of others; and
    c. interfere with the normal operation of College systems.
5. The College may access or monitor system information, logs, or accounts when required for operations, security, or legal compliance, and will do so in accordance with the Personal Information Protection Act (PIPA) and College privacy policies.
6. Violations of this policy may result in the suspension of access privileges, disciplinary measures under the applicable student or employee conduct policies, and, where appropriate, referral to law enforcement.

PROCEDURES

Account Access and Use

7. The College will provide users with access to technology resources, including email, learning systems, networks, and applications, for academic and administrative purposes. Users will be given instructions for activating their accounts, setting secure passwords, and maintaining basic device and network security.
8. College-issued employee and student accounts must be used when engaging in College-related activities or accessing College systems. Personal accounts must not be used for activities involving College records, student information, instruction, or institutional communications.
9. Users must take reasonable steps to protect their accounts, login credentials, and devices from unauthorized access. This includes keeping passwords confidential, logging out of shared devices, and updating personal devices used to access College systems.
10. The College may implement technical controls such as access permissions, authentication requirements, usage limits, or restricted network access where needed to maintain system security and reliability.

Security Incident Response

11. Users must promptly report any suspected security concern, including unauthorized access, phishing attempts, malware, loss of a device, or unusual account activity. Reports should be made to the designated IT contact or a supervisor.
12. The College will review reported concerns, determine whether an incident has occurred, and take steps to contain or resolve the issue. These steps may include resetting passwords, adjusting access rights, or temporarily disabling accounts or devices.
13. Users are expected to cooperate with any inquiries into suspected incidents. This may include verifying recent activity, providing relevant information, or following instructions to restore security.
14. When appropriate, the College will notify affected individuals of confirmed security incidents, unless notification would impede an investigation or conflict with legal obligations.

System Oversight

15. To support system operations, troubleshoot problems, protect security, or meet legal requirements, the College may access system usage data to protect system integrity and maintain efficient operations. Such access will be limited to what is necessary for the task and will follow the College's privacy policy and the Personal Information Protection Act (PIPA).
16. System administrators may apply temporary restrictions to accounts, devices, or network segments if required to protect institutional systems. These restrictions may be lifted once the issue is resolved or mitigated.
17. Only authorized personnel may access system information for operational or investigative purposes, and all such access must comply with institutional privacy standards and applicable legislation.

Appropriate Use Expectations

18. The College may limit or restrict access to websites, applications, or online services that pose security risks, interfere with academic or administrative operations, or consume excessive network resources.

19. Users must not attempt to bypass security controls, gain unauthorized access to information, disrupt the performance of systems, or engage in illegal or harmful behaviour while using College technology resources.
20. Users must comply with this policy and with all related College policies, procedures, standards, handbooks, guidelines, terms of use, and user agreements that govern the use of College technology resources, including any role- or system-specific requirements communicated by the College.
21. Failure to meet these expectations may result in the suspension or revocation of access to College technology resources and may lead to further action under applicable student or employee conduct policies. Where appropriate, serious or unlawful matters may be referred to law enforcement.

Accessibility Supports

22. The College will provide reasonable accommodations to ensure that students and employees with disabilities can access technology resources. Accommodations may include alternative formats, assistive technologies, or adjustments to access methods.
23. Accommodation requests will be reviewed and implemented in accordance with the College's accessibility and accommodation procedures.

DEFINITIONS

Account: A username, password, or other credential issued by the College that allows a user to access College technology resources.

College Technology Resources: All information technology owned, licensed, managed, or supported by the College. This includes networks, systems, email, cloud services, software, hardware, learning platforms, and data.

Device: Any equipment used to access College technology resources, including College-issued devices and personal devices such as laptops, tablets, and smartphones.

Information Security Incident: Any event that threatens or may threaten the confidentiality, integrity, or availability of College systems or information. Examples include unauthorized access, malware, phishing, loss of a device, or unusual account activity.

User: Any student, employee, contractor, volunteer, or other individual who accesses or uses College technology resources.

RELATED RESOURCES

- Information Security Policy 1.2.3
- Personal Information and Protection of Privacy Policy 1.2.1
- Records Management Policy 1.2.2
- Student Academic Responsibility Policy 2.2.1
- Student Non-Academic Conduct Policy 2.2.2
- Employee Professional Standards and Conflict of Interest Policy 3.1.2
- Personal Information Protection Act, SBC 2003, c 63
- Criminal Code, RSC 1985, c C-46
- Copyright Act, RSC 1985, c C-42