Title	**Computer and Computing System Use**
Number	**B5002**
Category	**Administration**

1. PURPOSE

To ensure that all computing system use is lawful, responsible, and consistent with the College's vision, mission, and goals.

To ensure computer usage/conduct protects the organization from cyber-attacks and does not compromise the computing system's integrity, reliability, availability, and optimal performance.

The policy also seeks to protect and prevent data from being deliberately or inadvertently stored on an unsecured device or carried over unsecured networks where unsanctioned/unintended parties could access information.

2. DEFINITIONS

Academic purposes – means teaching, learning, research, and other purposes relating to the College's vision, mission, and goals.

Chief Information Officer (CIO) – means the senior administrator in the College's Information Technology (IT) department.

Computing system – means all computing and electronic communications resources, facilities and services owned, licensed, subscribed to, managed, or maintained by Langara College, both on or off College property. The computing system includes, but is not limited to, computers, cloud computing systems and data repositories/storage, printers, terminals, data files, software, mobile applications, networks, telephones, voicemail, digital signage, audiovisual equipment and systems, and computer lab facilities. For this policy, the computing system includes computer resources that an individual uses on College property or related facilities.

Employee – an individual employed and paid by the College to provide services on its behalf.

Executive Leadership Team (ELT) – the College's President and Vice-Presidents.

Incidental personal use – means personal use that does not interfere with a user's duties or responsibilities or another user's access to the email system and/or computing system or create a direct cost to the College. An example of incidental personal use is sending a personal email message during an employee's lunch hour.

Loaner Device – The CIO determines who is eligible for loaner computing devices based on available inventory and needs. Loaner devices are equipment Langara owns and provides to any College employee, contractor, student, or authorized individual to achieve their duties or responsibilities. They are provided for a period of time and must be returned to the IT department upon contract termination or at the end of the stipulated use period.

Personal device – means equipment owned by the user and can be used to connect to the College's computing system for academic or business-related work. This includes, but is not limited to, laptops, tablets, smartphones, and external hard drives.

Shared resources – any system or applications, files and directories that are password protected or encrypted. This includes, but is not limited to, data repositories, files, programs, printers, computer stations, audiovisual equipment and systems, and network resources that more than one person can use.

Student – an individual who has been granted admission to the College, is enrolled in, auditing, or participating in any College course or program, or when not enrolled or registered for a particular semester, is eligible to enroll in future terms without seeking readmission. Individuals between academic terms; on a leave of absence; awaiting a degree or credential; on suspension; or have withdrawn from the College while a disciplinary matter is pending are considered students under this policy.

3. POLICY

3.1 The CIO or designate is responsible for developing College policy regarding the use of the computing system.

3.2 Employees and students are given access to the computing system according to academic or operational needs, and access may be revoked at the discretion of the CIO or designate. College-allocated laptops, mobile devices, and desktop computers are for the exclusive use of Langara employees. These devices, including portable media containing College data, must not be used by or shared with third parties (including family members and/or friends).

3.3 Employees and students may use the computing system for incidental personal use, provided such use does not violate any provision in this policy or any other College policy.

3.4 Decisions regarding access to the computing system will be made by IT Governance Committee recommendation to the ELT member to whom IT reports. Sub-committees of the IT Governance Committee may be created to review and make recommendations regarding access required by employees and students or the impact on existing educational technologies. Access requests include providing connectivity to College databases, applications, other IT services and IT infrastructure, hosted internally or externally, with consideration for privacy and information security protection.

3.5 Employees and students will use the computing system in accordance with the B. C. Freedom of Information and Protection of Privacy Act, BC Human Rights Act, Canadian and British Columbia laws and statutes, and any other conditions, limitations, and restrictions that the College establishes, including, but not limited to, due care and safeguarding of College-assigned IT equipment and loaner devices.

3.6 All employees must complete an annual online Cyber Security Awareness training course every calendar year.

3.7 Given constantly evolving cyber threats, IT reserves the right to offer all employees additional Cyber Security Awareness Training and/or cyber testing campaigns at appropriate times.

3.8 Employees and students must not use on-premise network storage (e.g. network share drives) or storage local to College-provided computing devices in any way that is not permitted by law or might compromise the computing system. This includes, but is not limited to:

a) storage or distribution of materials unrelated to academic or business purposes;
b) materials deemed explicit by the College; or
c) access to shared resources without authorization.

3.9 When using the College's computing system to access a cloud computing system, storage or application which is not a College subscribed service, employees and students must not distribute materials that are deemed explicit by the College, or use such cloud storage or service in any way that is not permitted by law or could compromise the College's systems. This includes using personal devices (USB drives) to transport College data and student information outside the network.

3.10 Students with disabilities will have the right to priority access at specially designed workstations. Other students may use those workstations only if there are no students with disabilities waiting.

3.11 Employees and students will not engage in activities harmful to the computing system, such as:

a) creating or propagating malicious applications such as viruses;
b) disrupting services;
c) damaging files;
d) illegally downloading material; or
e) intentionally damaging equipment, software, or data belonging to the College.

3.12 IT staff, authorized by the relevant ELT member and the CIO, or if the CIO is involved, authorized by both the Vice-President, Finance and Administration and the President, may gain access to employee and student files, programs, account information, printouts, software licenses and other materials without the consent of the employee/student in the following instances:

a) when necessary for the maintenance and security of the computing system;
b) when there are reasonable grounds to believe that a violation of law or a breach of College policy may have taken place;
c) when there are reasonable grounds that suggest risk to the environment and/or the health and safety of the public or an individual, or conditions that could result in an escalation of mental health concerns and/or threats of violence; or
d) in accordance with handling electronic communications as outlined in Policy B4002 – Electronic Communication.

3.13 To safeguard the College's interests and computing systems, the IT Department, directed by and at the discretion of IT leadership, such as in the case of loss or theft, may elect to wipe a College-issued device's hard drive of locally stored data via remote command without the individual's consent.

3.14 All College-owned IT Assets must be returned to IT when they are no longer needed or no longer working. Any IT Assets containing storage devices must be removed from services and properly erased and wiped to ensure no data or information is left on the device in any manner before being considered for disposal or donation to an individual or organization.

3.15 Employees may only remove or modify any part of the computing system equipment with the approval of the CIO or designate.

3.16 Employees and students who discover a Computer and Computing System Use Policy breach will notify the CIO or designate immediately.

3.17 Violations of the Computer and Computing System Use Policy may result in disciplinary actions, up to and including termination.

4. RESPONSIBILITY

For inquiries related to this policy, contact the Chief Information Officer.

5. REGULATIONS/PROCEDURES

Computer and Computing System Use Procedures

History/Revision	
Origination Date	June 12, 2001
Amendment Date(s)	November 1, 2023 February 11, 2020
Next Review Date	November 1, 2026