

Information Technology Acceptable Use Policy

Policy Type: Corporate

Policy Owner: Vice President, Finance, Administration and Applied Research

Approval Date: July 14, 2026

Replaces: Version 2022

Corresponding Procedure: IT Acceptable Use Reporting and Review Procedure

Purpose

This policy outlines the acceptable use of Cambrian College's ("the College") Information Technology Resources and establishes rules to protect the College and its community.

Improper use of these resources may expose the College to risks such as security breaches, system disruptions, and legal liability. Violations of this policy may result in sanctions, including loss of access to Information Technology Resources and/or legal action.

Scope

This policy applies to all members of the College Community and governs the use of the College's Information Technology Resources from any location, including on-campus and remote access.

It also applies to privately owned devices connected to College systems.

The College may take action regarding off-campus or non-College system use if such behaviour:

- Involves illegal activity.
- Poses a threat to individuals.
- Violates College policies.

Definitions

College Community: includes all registered students, both full and part-time; all paid employees; and all others associated with the College including Board of Governor

members, retirees, volunteers, contractors, suppliers, and such visitors as are granted temporary User status by the College.

Data: data used in this policy is characterized by one or more of the following:

- Information that is processed by means of equipment operating automatically in response to instructions given for that purpose.
- Information that is recorded with the intention that it should be processed by means of such equipment.
- Information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, and
- Information that does not fall within any of the above but forms part of a readily accessible record covering an individual.

Information Technology Resources: those physical, electronic, or intellectual resources used to produce, convey, transmit, store, analyze, collate, distribute, present, display, etc. Data or information in whatever form (e.g., text, pictorial, graphic, audio, etc.). These typically include, but are not limited to:

- Computer hardware and software.
- Networking cables, devices and equipment.
- Applications including browsers, servers, and databases.
- Telecommunications, audio-visual, and telephone equipment.
- Any device that connects to the network and/or the Internet.
- Other forms of information technology that exist today or may be developed in the future.

User: College Community member authorized to have access to certain designated Information Technology Resources.

User Account: a location on the College's network server used to store a User's computer username, password, and other information.

XaaS: "Anything as a Service" (XaaS) describes a general category of services related to cloud computing and remote access. It recognizes the vast number of products, tools, and technologies that are now delivered to users as a service over the internet.

Policy Statements

1. General

- 1.1. Information Technology Resources are provided to support the College's academic, administrative, and research activities.
- 1.2. Information Technology Resources are shared College assets intended to support the entire College Community. Misuse of these resources is not permitted.
- 1.3. No hardware, software, "Anything as a Service (XaaS)" solutions, services, or other Information Technology Resources may be procured, implemented, accessed, or used for College purposes without prior approval from the Information Technology Department, regardless of cost.
- 1.4. Information Technology Resources may be used only by authorized members of the College Community.
- 1.5. Users must comply with all municipal, provincial, federal, and other applicable laws, including but not limited to the [Freedom of Information and Protection of Personal Privacy Act, RSO 1990, c. F.31](#); the [Personal Health Information Protection Act, SO 2004, c. 3, Sched. A](#); the [Personal Information Protection and Electronic Documents Act, SC 2000, c. 5](#); and the [Criminal Code, RSC, 1985, c. C-46](#), as well as all applicable College policies and procedures.
- 1.6. Members of the College Community are responsible and accountable for their actions and communications in the electronic working and learning environment.
- 1.7. Members of the College Community are expected to use Information Technology Resources responsibly and efficiently, and in ways that do not interfere with the study, work, or working environment of other Users.
- 1.8. Users accessing external networks are subject to the policies governing those networks. Where both College and external network policies apply, the more restrictive policy will govern.
- 1.9. While the College aims to provide reliable access to Information Technology Resources, it does not warrant that such resources will meet all User requirements or operate without errors or interruptions.
- 1.10. The College is not liable for any indirect, incidental or consequential damages, including but not limited to loss of data, information, or profits arising from the use of, operation of, or inability to use Information Technology Resources.
- 1.11. The College reserves the right to remove a User from a computer lab if the User is not part of the class in progress.

- 1.12. All official email communication between the College and registered students will be conducted through the College-provided student email account. Students are required to use this account for electronic communications with the College, including communications with faculty. Messages sent from the College email system are considered official, and students are responsible for monitoring and responding through their College email account.

2. Acceptable Use of Resources

- 2.1. Information Technology Resources are to be used for College-related purposes.
- 2.2. For employees, the College does permit the personal use of email and internet access, provided that it:
- a. Does not interfere with work responsibilities.
 - b. Does not impact system performance.
 - c. Complies with this policy.
- 2.3. Users must **not use** College Information Technology Resources to:
- a. Conduct private business for personal financial gain.
 - b. Represent or imply College endorsement of any political, advocacy, labour, professional, or external organizations through the creation, display, transmission, or use of logos, images, messages, or other materials.
 - c. Access, create, store, or distribute content that is illegal, offensive, discriminatory, harassing, or otherwise prohibited by law or College policy.
 - d. Access, create, store, or distribute pornographic, obscene, or sexually explicit material.
 - e. Engage in, support, or facilitate illegal activity.
 - f. Create, introduce, distribute, or use malicious software or tools intended to compromise the security or operations of Information Technology Resources (e.g., viruses or hacking tools).
 - g. Support activities that do not relate to academic, administrative, or other authorized College purposes.
- 2.4. The College may restrict activities such as:
- a. Online gaming.
 - b. Downloading or sharing of non-essential software or materials.

3. Integrity and Security of Resources

- 3.1. Any action or attempt by an individual to subvert or disrupt the intended use or functioning of any Information Technology Resources, or to affect their use or operation in a manner detrimental to other Users, is prohibited.
- 3.2. No User shall deliberately jeopardize the integrity of the College's Information Technology Resources. Any attempts to bypass system security, or tamper with, or cause damage to, Information Technology Resources is viewed as jeopardizing the functioning of College Information Technology.
- 3.3. The College reserves the right to review any material stored in files and programs on a device connected to Information Technology Resources, and will edit or remove any material which it, in its sole discretion, believes may be unlawful, obscene, abusive, or otherwise objectionable.
- 3.4. Users are responsible for any, and all, use of their User Accounts. As such, Users must:
 - a. Maintain secure passwords for any, and all, accounts assigned to them.
 - b. Ensure and safeguard against others obtaining unauthorized access to their accounts.
 - c. Not share passwords or any other access control information for their User Accounts.
 - d. The Information Technology Department reserves the right to delete a student's email account if unused for more than (1) year.
- 3.5. Computing activity is centrally monitored. Each User is responsible for the activity conducted under their User Account.
- 3.6. Users must comply with all copyright and license conditions associated with Information Technology Resources. As such, Users:
 - a. Must not move, copy or transfer programs, files or other forms of software from one computing system to another without proper authorization to do so.
 - b. Must not distribute, sell or make available software to any person where prohibited by copyright or license.
 - c. Must not access or use software belonging to, or owned by, the College without proper authorization and license rights.
- 3.7. While the College provides central backup services for central computer systems, College computers are not backed up and are rebuilt on a periodic basis. Users of

these networks are responsible for backing up information that they place on these computers and/or utilizing central computer storage areas provided to Users.

4. Confidentiality and Privacy

- 4.1. Generally, with respect to computing User Accounts established for students, faculty, and staff, there is a presumption of privacy. However, if the College suspects an infraction, it will investigate the traffic and files in accordance with the appropriate College policies and in compliance with the law.
- 4.2. Users are responsible for the confidentiality of any restricted data or information for which the College has granted access. As such, Users must:
 - a. Ensure confidential information is not shared.
 - b. Not leave their devices unattended while logged-on to their User Accounts.
 - c. Exercise discretion when printing confidential information.
 - d. Not copy, send, duplicate or transmit by any means confidential data from College systems for any purpose other than performance of College-related business.

5. Sanctions

- 5.1. Violations of this policy will be addressed under applicable College policies and procedures (e.g., employee and student disciplinary policies), including the [Code of Conduct Policy](#).
- 5.2. Sanctions may include:
 - a. Temporary or permanent loss of access to Information Technology Resources.
 - b. Disciplinary action.
 - c. Legal action in accordance with applicable laws and contractual agreements.

Responsibilities and Accountability

Vice President, Finance, Administration, and Applied Research is responsible for:

- Ensuring the overall quality assurance and access of the Information Technology Resources of the College.

Director, Information Technology is responsible for:

- The administration and oversight of the [Information Technology Acceptable Use Policy](#), including:

- Establishing and maintaining the framework governing access to and use of the College's Information Technology Resources, which may be implemented through standards, guidelines, system-specific rules, operational practices, and technical controls.
- Ensuring acceptable use expectations are communicated and made available to the College Community.
- Delegating operational responsibilities related to access, system administration, and monitoring to appropriate Information Technology roles, while retaining overall accountability.
- Authorizing technical actions, including restriction or removal of access, where required to address inappropriate use or mitigate operational, legal, or security risks.
- Coordinating with the Academics, Human Resources, Student Services departments, and other appropriate College offices in cases involving alleged policy violations, recognizing that disciplinary actions are administered through established College policies and procedures.

College Community is responsible for:

- Complying with the requirements of this policy.
- Reporting unacceptable use of College Information Technology Resources.

Procedures/Forms

- IT Acceptable Use Reporting and Review Procedure

Related Policies

- [Academic Integrity Policy](#)
- [Code of Conduct Policy](#)
- [Free Speech Policy \(Freedom of Expression\)](#)
- [Harassment and Discrimination Policy](#)
- [Internal Privacy Policy](#)
- [Procurement Policy](#)
- [Records Retention Policy](#)
- [Social Media Use Policy](#)

References

- [Freedom of Information and Protection of Personal Privacy Act, RSO 1990, c. F.31](#)
- [Personal Information Protection and Electronic Documents Act, SC 2000, c. 5](#)
- [Personal Health Information Protection Act, SO 2004, c. 3, Sched. A](#)
- [Criminal Code, RSC, 1985, c. C-46](#)