Policy Title	Acceptable Use of Information Technology Resources
Policy Holder	Senior Director, Computer Services & Project Management
Policy Approver(s)	Senior Team
Related Policies	• Respectful Work & Learning Environment (Workplace Harassment) - (Ch4-s2-01). • Expectation of Privacy - (7-3-2) • Potentially Offensive Material - (7-4-1). • Over-Extension of Resources (7-4-2) • Code of Conduct - (4-2-6). • Student Code of Conduct - (5-5-2). • Use of Electronic Devices in Class - (5-5-6). • IT AUP Non-Compliance, Disciplinary Actions, and Appeals – (7-2-3).
Related Procedures	• College Collective Agreements for Support Staff and Faculty. • Terms and Conditions for Administrative Employees • The Ontario Human rights Code • The Criminal Code of Canada
Appendices	
Storage Location	Website - https://www.confederationcollege.ca/policies-and-procedures
Effective Date	Oct 28, 2009
Next Review Date	January 30, 2026

Purpose

This policy defines the general constraints as well as the acceptable practices for the use information technology resources for all users at Confederation College.

Scope

The Acceptable Use of Information Technology Resources policy is applicable to the entire College community.

Definitions

.

Word/Term	Definition
Information Technology Resources	Includes, but is not limited to, all College owned computer hardware, computer accessories, software, printers/copiers, network devices/system, software, servers, security systems, data, Internet,

	media, documentation, communications systems, user accounts, and audiovisual equipment.
IT Infrastructure	Refers to the entire collection of hardware, software, network resources, data centers, facilities, services, and related equipment, used for the existence, operation, and management of the College's IT environment.
College Community	Includes employees, students, student associations, contractors, visitors/guests, volunteers, alumni, Board of Governors, lessees/renters of space, or any other user who uses any College IT resources.
Potentially Offensive Material	Content, such as articles, photographs, videos, games, or websites that is likely to be upsetting, insulting, or objectionable to some or most people.
Junk E-mail	Unwanted e-mail, usually of a commercial nature, sent out in bulk.

Governing Laws and Regulations

- The Ontario Human rights Code
- The Criminal Code of Canada

Policy Statements

The computing and information technology resources of Confederation College serve to support and enhance the academic mission of the College and its community. Confederation College's IT Resources are the sole property of Confederation College. More specifically, IT resources are made available to employees in support of their teaching, research, and administrative activities and to students in support of their respective academic requirements. For all College IT users, access to these resources is a privilege to be used in effective, ethical, secure, and lawful ways that support the values of Confederation College. The College will endeavor to create an atmosphere that balances respect for individual users with that of the overall needs, security, standards, as well as values of the College community as a whole.

It is acceptable to use Confederation College IT resources:
- For purposes directly related to the learning process.
- In the case of employees and contractors, for the performance of necessary job-related tasks.
- For limited amounts of personal use providing that such activity does not 1) interfere with the person's work & responsibilities; 2) impose costs to the College; 3) degrades the performance of, or pose a security risk to the College IT infrastructure; or, 4) contravene the mission of the College. Note: that personal communications is subject to *7-3-2 Expectation of Privacy* when using College IT resources

Acceptable use of College IT resources also includes:
- Respect for the rights, privacy, and property of others.
- Consideration of other persons using shared systems, equipment, and facilities.
- Use of resources and tools for the purpose of which they are intended.
- Adherence to all applicable rules, policies, and laws including (but not limited to):
  - Respectful Work & Learning Environment (Workplace Harassment) Policy (Ch4-s2-01)
  - Code of Conduct (4-2-06)
  - Student Code of Conduct (5-5-02)

- Use of Electronic Devices in Class (5-5-06)
- Potentially Offensive Material (7-4-01)
- Over-Extension of Resources (7-4-02)
- Authentication and Cyber Security Login Measures (7-2-5)
- Applicable College Collective Agreements
- Terms and Conditions for Administrative Employees
- The Ontario Human rights Code
- The Criminal Code of Canada

Unacceptable use of College IT resources includes (but is not limited to):
- Unauthorized access, alteration, destruction, removal and/or disclosure of data, information, equipment, software or systems.
- Disclosure of confidential account passwords or access information.
- Deliberate over-extension of system resources or the interference with the normal operation/functioning of a system.
- Attempts to access confidential information that they do not have rights and privileges to access
- Uses which violate copyright law.
- In general, any use of Confederation's IT Resources for personal commercial or financial gain or for political causes is considered to be a conflict of interest and in violation of this Policy and College's Conflict of Interest Policy
- Any form of illegal trade, negotiation, or conspiracy to conduct illegal acts.
- Uses to build support for personal causes.
- Any action or use of IT resources that contradicts the College's Potentially Offensive Material (Ch7-s4-01) policy or violate a person's right to work and study in an environment free from discrimination/ harassment is strictly prohibited.
- Uses for the creation, transmission, storage, access, or viewing of materials which are deemed in the sole discretion of the College to serve no useful academic or administrative purpose
- Issuance of junk e-mail.
- Theft of any College owned computer hardware, software, accessories, intellectual property, or data.
- Carelessness or misuse of College equipment or other IT resources.
- Malicious or unethical use.
- Interference with the work of others. This includes any process that causes a user to be deprived of services or resources that they would normally expect to have available.
- Creation, development, storage, transmittal, or replication of any program, code, subroutine, or other means intended to disrupt, interfere, damage, destroy, or corrupt the College's IT infrastructure (i.e. viruses, hacking, spyware, network snooping utilities).
- Uses that violate College policy or Provincial and Federal laws.

User Responsibilities

All College users are responsible for their use of the College's IT resources and as such must:

- Maintain secure passwords for all accounts assigned to them.
- Ensure and safeguard against others obtaining unauthorized access to their accounts.
- Not share account passwords or any other access control information for their accounts.
- Not subvert the restrictions associated with their accounts.
- Not attempt to gain access to systems/resources both inside and outside of the College for which they have no authorization.

- Ensure confidentiality and security of any information or data to which they have been granted access.
- Ensure that confidential information is not observed by unauthorized individuals while working at a computer, including while working off campus.
- Ensure computers have locking/password protection when unattended.
- Exercise discretion when printing confidential information which may be viewed or observed by unauthorized persons.
- Not copy, send, duplicate, or transmit by any means, confidential data from College systems for any purpose other than performance of College related business.
- Have a general awareness of copyright/piracy laws, policies, rules, and regulations. Further all users must:
    - Comply with all copyright, patents, intellectual property laws, license conditions, and contractual obligations associated with College computing systems.
    - Not move, copy, or transfer programs, files, or other forms of software from College computing systems to another without proper authorization to do so.
    - Not distribute, sell, or make available software to any person where prohibited by copyright or license.
    - Not access and/or use software owned by Confederation College without proper authorization and license rights.
    - Only use College computing resources for the purposes for which they are intended and authorized.
- Demonstrate general awareness of current cyber security issues that could lead to data compromise or system interruption (See 7-2-5 Authentication and Cyber Security Login Measures)
- Not attempt to interfere, disrupt, damage, destroy, or corrupt the authorized use of data, the computing equipment, or the normal operation of the Colleges IT infrastructure.
- Have respect and consideration for the rights, privacy, and property of others.
- Adhere to all applicable College rules, policies, as well as government laws.
- Immediately report any suspected breach of security, abuse, loss of information, or other infraction (as outlined above) to the Computer Services Department Help Desk at helpdesk@confederationcollege.ca
- *Users are responsible and accountable for their actions and statements when using College IT resources, including any activity related to their login account*. At all times, users must respect the public nature of the College and conduct themselves in a professional and businesslike manner.

Non-Compliance

See 7-2-3 – IT AUP Non-Compliance, Disciplinary Actions, and Appeals.

Revision History

Version	Change	Author	Date of Change
Original	Original	Paul Inkila	28-10-2009
	Format and content change	Paul Inkila	18-4-2022