Policy Title	Expectation of Privacy
Policy Holder	Senior Director – Computer Services and Project Management
Policy Approver(s)	Senior Team
Related Policies	
Related Procedures	
Appendices	
Storage Location	Website - https://www.confederationcollege.ca/policies-and-procedures
Effective Date	October 28, 2009
Next Review Date	January 30, 2026

Purpose

To protect its information technology infrastructure and data, the College balances the College's needs, security, standards, and values with the privacy rights of individual users. Users thus have a limited right to privacy while using College IT infrastructure.

Scope

This policy applies to all College staff.

Definitions

Governing Laws and Regulations

FIPPA - Freedom of Information and Protection of Privacy Act
PHIPPA - Personal Health Information Privacy Act

Policy Statements

College staff must be aware of the privacy implications for data they store and transmit using College equipment.

- The College reserves the right to access and manage all information, including images, stored on or transmitted within the College computing infrastructure. Information stored

within or transmitted using the College's computing infrastructure, including information in individual accounts and e-mail, is the property of the College.

- While it does not routinely do so, the College may monitor computer and network use to ensure that such use is consistent with the purposes, goals and policies of the College and with relevant legislation and regulations (FIPPA, PHIPPA). Such monitoring may occur at any time, without notice, and without the user's permission.
- College data is subject to FIPPA. Electronic (or other) records may be publicly released under this legislation. Users must take care when creating or modifying records, so that exposure of this data does not cause harm to the College.
- Wireless electronic traffic is presumed to be insecure and susceptible to unauthorized examination unless encrypted between the destination and source. Due to this lack of privacy, College users must not use unencrypted wireless networks to access critical and essential applications or transmit sensitive material and information, such as social insurance numbers. While on campus, users are to use the authenticated wifi service which ensures encryption. Individuals assume full responsibility and accountability for their wireless network communications.

Revision History

Version	Change	Author	Date of Change
Original	Original	Paul Inkila	28-10-2009
	Format and technology update	Paul Inkila	16-05-2022