COLLEGE POLICY

Policy No. & Title:	**P-114 Electronic Monitoring of Employees**
Policy Sponsor:	Director, People & Culture
Reference Cmtee:	Policy & Procedure Committee
Effective:	2022-10-11
Next Review:	2023-03-01
Supersedes:	N/A NEW

Purpose

The College is committed to the security of our electronic communications as well as to the expectation of privacy under the Personal Information Protection and Electronic Documents Act (PIPEDA) for employees. This policy governs the use of computers, networks, and related services of the College. Computers and networks can provide access to resources within and outside the College, as well as the ability to communicate with other users worldwide. Such access is a privilege and requires that individual users act responsibly.

College employees must respect the rights of others, respect the integrity of the computers, networks, and related services, and observe all relevant laws, regulations, contractual obligations, and College's policies and procedures.

As such, and as an organization of more than 25 employees, the College has the following policy in place regarding the monitoring of electronic communications by employees.

Scope

This policy applies to all employees of the College.

Definitions

College refers to any entity operating under parent company triOS Corporation, including: triOS College Business Technology Healthcare Inc., Eastern College Inc., Lifecycle Systems Corporation, or Eastern College Online.

Working for Workers Act refers to Bill 88 – An Act which includes a requirement for a written policy on electronic monitoring which received Royal Assent on April 11, 2022 which is detailed under Bill 88, Working for Workers Act, 2022 - Legislative Assembly of Ontario (ola.org).

The College's Computer System – includes computers and related equipment, e-mail, telephones, voice mail, facsimile systems, communications networks, computer accounts, internet and/or web access, network access, central computing and telecommunications facilities, and related services.

Electronic Communications refers to all messages, data files and programs stored in or transmitted via the Computer System.

Logging refers to the communications between a Computer System and the users of that system, or a data collection method that automatically captures the type, content, or time of transactions made by a person from a terminal with that system to understand the activity of the system and to diagnose problems. Logging records either event that occur in an operating system or other software runs, or messages between different users of a communication software.

Effective Date and Changes
This policy is effective as of October 11, 2022.

In the event of any future changes to this policy, the date of the changes made will be included in header of this Policy.

POLICY
Providing Copies of this Policy to Employees
The College will provide this written policy to all employees within 30 days of its effective date.

If any changes are made to this policy, employees will be provided with the updated policy within 30 days of any amendments.

In the case of newly hired employees, the College will provide a copy of this policy to them within 30 days of their date of hire.

Computer System Access
Access to and use of the College's Computer System is a privilege granted to the College's employees. All users of the Computer System must act responsibly and maintain the integrity of the Computer System. The College reserves the right to deny, limit, revoke, or extend computing privileges and access to the Computer System in its discretion.

The College may, in its discretion, limit the use of specified portions of the Computer System to certain employees, and/or deny the use of specified portions of the Computer system to certain employees.

The College's Computer System may not be used in any manner or for any purpose which is illegal, dishonest, disruptive, threatening, is damaging to the reputation of the College, is inconsistent with the mission of the College, or could subject the College to liability.

Any violation of this policy or of other College policies, in the course of using the Computer System, may result in an immediate loss of computing privileges, disciplinary action up to and including termination of employment, and referral of the matter to the appropriate authorities.

Electronic Monitoring of Employees

The College does not actively monitor employee voice or video communications. The College also does not actively monitor the activities on personal owned equipment, or the specific traffic that traverses between that equipment and the internet.

The College's network infrastructure is aware of destinations being requested by employees using any College device. This is because equipment on the College's infrastructure must:

a) use DNS to request the IP address of an Internet site, and
b) must cross a firewall that will inspect the traffic as it routes traffic through.

Logging may be turned on with either of these technologies for security and/or diagnostic purposes. The logging does not report an individual employee's specific actions but does capture enough data to enable the College to discover usage patterns by a device's network ID and confirm ownership by either administrative review (in the case of company owned equipment) or through confiscation or other similar means (personal devices).

Where Electronic Monitoring of Employees Does Occur

1. Calls which run through the Contact Centre are recorded by Five9 for evaluation and training purposes. There is an outbound "campaign" channel enables employees to make calls for personal reasons which does not record calls.
2. MS Teams calls can be recorded by participants. This is a notified action within the meeting, so it will not be a surprise. We do not automatically record Teams videos or calls.
3. The IT team uses software called "Connectwise" which provides the IT team with remote access to company owned PC equipment. It does allow the IT team to shadow users, take screenshots, and recordings. The intent of Connectwise is to enable the IT team to support an employee with temporary access to resolve technical issues.
4. Many of our campuses use security cameras with recording capabilities which cover major traffic areas, and some campuses have cameras that extend into the classroom. These cameras are installed and are used for security purposes only.
5. Some campuses (or the CSC) use RFID cards and alarm codes to gain access to the building. In the case of RFID cards, their use is logged by the software which can give some indication of staff entering through locked doors.
6. Where there is suspicious or inappropriate activity or improper use.

No Expectation of Privacy

College employees have no expectation of privacy in College property and equipment. Such property and equipment includes but is not limited to, the College's Computer System, and all Electronic Communications. The College reserves the right to monitor, access, use, and disclose all messages, data files and programs sent over or stored in its Computer System for any purpose. The College management reserves the right to monitor, inspect, and examine any portion of the Computer System at any time and without notice.

The College may monitor or access an employee's e-mail, with or without notice, for any business-related purpose, including any situation in which a supervisor has reason to believe that an employee is misusing or abusing e-mail privileges, or is violating any other College policy.

Passwords

Portions of the College's Computer System may be accessible by password only. The purpose of a password is not to provide privacy, but to control and prevent unauthorized access.

Every password issued for the use of any part of the College's Computer System is the responsibility of the person in whose name it is issued. That individual must keep the account secure from unauthorized access by keeping the password secret, by changing the password often, and by reporting to the College when anyone else is using the password without permission.

Passwords are intended to help prevent unauthorized access and may not be shared with unauthorized persons. The contents of all password protected data files and programs belong to the College and are subject to access and disclosure by the College as set forth in this policy.

Improper Use of the Computer System.

Improper use of the Computer System is prohibited. The following are examples of improper use of the Computer System:

- *Storage, Transmission, or Printing of Improper Materials*: Storing, transmitting or printing any of the following types of Electronic Communications on the Computer System is prohibited: material that infringes upon the rights of another person; material that is obscene; material that consists of any advertisements for commercial enterprises; material or behaviors that violate laws, regulations, contractual obligations, and College policies and procedures; or material that may injure someone else and/or lead to a lawsuit or criminal charges.
- *Harassment:* Any electronic communication that violates the College's Anti-Violence Harassment Discrimination and P-105 Sexual Harassment Sexual Violence Prevention policies is prohibited. Additionally, any electronic communication that is annoying, abusive, profane, threatening, defamatory or offensive is prohibited. Some examples include obscene, threatening, or repeated unnecessary messages; sexually, ethnically, racially, or religiously offensive messages; and continuing to send messages after a request to stop.
- *Destruction, Sabotage:* Intentionally destroying anything stored on the Computer System, including anything stored in primary or random-access memory is prohibited. Deliberately performing any act that will seriously impact the operation of the Computer System. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer or peripheral.

- *Evasive Techniques:* Attempts to avoid detection of improper or illegal behavior by encrypting or passwording electronic messages and computer files are prohibited.
- *Unauthorized Use/Access:* Using the Computer System to gain or attempt to gain unauthorized access to remote computers is prohibited.

Other prohibited behaviors include actions that give simulated sign off messages, public announcements, or other fraudulent system responses; possessing or changing system control information (e.g., program status, protection codes, and accounting information), especially when used to defraud others, obtain passwords, gain access to and/or copy other user's electronic communications, or otherwise interfere with or destroy the work of other users.

- *E-Mail Forgery:* Forging e-mail, including concealment of the sender's identity, is prohibited.
- *Theft/Unauthorized Use of Data:* Data created and maintained by the College, or acquired from outside sources, are vital assets of the College and must be used only for authorized purposes. Theft of or unauthorized access to or use of data is prohibited.
- *Program Theft:* Unless specifically authorized, copying computer program(s) from the Computer System is prohibited.
- *Viruses, etc.:* Intentionally running or installing on the Computer System, or giving to another, a program that could result in damage to a file or the Computer System, and/or the reproduction or transmission of itself, is prohibited. This prohibition includes, but is not limited to, the classes of programs known as computer viruses, Trojan horses, and worms.
- *Security:* Attempting to circumvent data protection schemes or uncover security loopholes is prohibited.
- *Wasting Resources:* Performing acts that are wasteful of computing resources or that unfairly monopolize resources to the exclusion of others is prohibited. These acts include but are not limited to: sending mass mailings or chain letters; creating unnecessary multiple jobs or processes; generating unnecessary or excessive output or printing; or, creating unnecessary network traffic.
- It is understood that, occasionally, staff members use e-mail or internet access for non-commercial, personal use. Such occasional non-commercial uses are permitted if they are not excessive and are limited to breaks or lunch hours, do not interfere with the performance of the employee's duties, do not interfere with the efficient operation of the College, and are not otherwise prohibited by this policy or any other College policy.
- *Accessing User Accounts:* Unauthorized attempts to access or monitor another user's electronic communications are prohibited. Unauthorized accessing, reading, copying, changing, disclosing, or deleting another user's messages, files, or software without permission of the owner is prohibited.
- *Backup Copies*: All data on the Computer System is subject to backup at the discretion of the College.
- *Copyright Infringement*: The Copyright Laws of Canada prohibit unauthorized copying. Violators may be subject to criminal prosecution and/or be liable for monetary damages.

- *Deleting Electronic Communications*: Users of the Computer System should be aware that Electronic Communications are not necessarily erased from the Computer System when the user "deletes" the file or message. Deleting an Electronic Communication causes the Computer System only to "forget" where the message or file is stored on the Computer System. In addition, Electronic Communications may continue to be stored on a backup copy long after it is "deleted" by the user. As a result, deleted messages often can be retrieved or recovered after they have been deleted.
- *Criminal Laws:* Under Canada's Criminal Code (R.S.C., 1985, c. C-46), criminal sanctions are imposed for offenses involving computers, computer systems, and computer networks. Any person committing an offense with respect to them may be subject personally to criminal sanctions and other liability. Provincial laws may also apply to some circumstances.

In general, employees may not copy, download, install or use software on the Computer System without acquiring a license from the publisher. (For example, you may not copy it from a friend or other source.) Furthermore, employees may not copy the College's software, unless such copying is specifically authorized by the College and permitted by the license agreement.

The ability to download documents from the Internet, and to attach files to E-mail messages, increases the opportunity for and risk of copyright infringement. A user can be liable for the unauthorized copying and distribution of copyrighted material through the use of download programs and E-mail. Accordingly, you may not copy and/or distribute any materials of a third party (including software, database files, documentation, articles, graphics files, audio or video files) unless you have the written permission of the copyright holder to do so.

Complaints

Employees who have concerns about the College's **Electronic Monitoring of Employees** should first speak with their supervisor/manager to discuss the issue. In the event the concern is not able to be resolved at this level, employees are directed to bring the issue forward to the Director, Human Resources or the Director of Facilities, Information Systems, and Technology.

Related Policies

P-203 Employment Accommodations
P-201 Accessibility
P-205 Confidentiality
A-113 Audio and or Video Recording of Lectures
A-130 Copyright
C-210 Network Acceptable Use
C-311 Communications
C-405 Privacy

Supporting Documents/Forms

P-114p Electronic Monitoring of Employees Procedure