POLICY TITLE: Information Technology – Acceptable Use & Electronic Monitoring

Category:	☐Institutional - Board ☐ Academic - Administrative ☒ Institutional - Administrative ☐ Employment - Administrative		
Approved by:	☐Board ☒President		
Date approved:	March 30, 2023	Effective date:	March 30, 2023
Policy Sponsor:	Chief Information Officer	Date last reviewed:	March 30, 2023
Date of Mandatory Review (expiry date):	March 2028	Date of last revision of Procedures:	March 30, 2023

1. POLICY

1. Access to CMCC information technology is a privilege. CMCC reserves the right to grant or deny access to and use of information technology.

2. The users of CMCC information technology are required to operate within the Information Technology rules, regulations and standards (see Procedures). Implicit in this is an obligation to report infractions of these Procedures.

3. Any use of CMCC information technology for the purpose of engaging in a form of commercial activity not directly related to CMCC business, including without limitation, advertising commercial products or transactions involving the purchase and sale of commercial products, is not permitted.

4. Users of CMCC information technology are not to assume that electronic communications or activities are private. CMCC reserves the right to electronically monitor, intercept, audit, review, and access all messages, emails, and files, without limitation, on CMCC's systems. This includes electronic monitoring of the online activity of users as well as the maintenance and review of electronic logs of activities on information systems accessed via CMCC's resources.

5. CMCC will retain records of electronic monitoring depending on technological limitations and as CMCC determines is reasonably required. Records are not necessarily maintained beyond 24 hours. CMCC assumes no responsibility for the retention of any records of electronic monitoring and is not liable for direct or indirect damages relating to the retention or non-retention of such records. Requests to view electronic monitoring records are to be made to the Privacy

Officer within 24 hours of any event having been recorded and may be provided if technically feasible and subject to reasonable cost.

6. Examples of ways CMCC electronically monitors its employees include, but are not limited to:

    a. Video Surveillance. Security cameras are located in selected locations across campus to provide a video record of persons entering and leaving the premises and using main hallways in the campus building. Cameras are not installed in washrooms, changing rooms, or assigned office spaces.

    b. Building Access. There is a record maintained of users accessing the building by using CMCC-issued keycards.

    c. Systems Access. CMCC maintains computer records of Network access, Internet access, Application access, Security information and events, and the use of software and software services licensed by CMCC. These records also include digital copies of messages sent and received by employees using the CMCC information technology services.

    d. Geographic Location. Mobile devices issued by CMCC (laptops, tablets, phones) may have location tracking capabilities, however this is intended for locating lost or stolen devices and not for active monitoring of user locations.

    e. Online Presence. Employees who work remotely and who are required to be online (e.g., using Microsoft Teams® or Zoom®) at certain times will have their status (i.e., online or offline) revealed to CMCC when using these remote productivity or conferencing platforms. Meetings taking place on any electronic meeting system may be recorded.

    f. Form Submission. There is an electronic record maintained of persons using the CMCC app for health screening or other form submissions.

    g. Application Usage. Persons using certain applications, such as the Panopto® video recording system or the clinic Electronic Health Record system, have their access and other usage tracked by those platforms.

    h. Room Reservations. Access to some laboratories and other rooms/spaces may be reserved and tracked by apps or other login/reservation systems.

    i. Collaboration. Use of collaboration software and platforms may produce a record of user activity.

7. Internet users are specifically prohibited from the type of activities listed below. This list is not comprehensive, but provides examples of inappropriate activities:

    a. accessing, copying, storing or transmitting material that could be considered illegal under applicable (including criminal) laws. (Such material would

include, for example and without limitation, material depicting sexual activity involving minors or those perceived or portrayed to be minors.)

b. accessing, copying, storing or transmitting material that is not strictly illegal, but by its nature is inappropriate material for work environment. (Such material would include for example and without limitation, material depicting pornographic/sexual acts or full/partial nudity.)

c. accessing, copying, storing or transmitting any other material (including jokes and cartoons) that could be considered defamatory, abusive, obscene, profane, or pornographic, which could offend or degrade others.

d. participating in chain letters.

e. fraudulently representing another individual or corporation.

f. any activities that are contrary to civil, criminal or administrative law.

g. any activity that would bring the reputation and/or goodwill of CMCC into disrepute.

8. Where required or appropriate, CMCC will assist outside law enforcement agencies with investigations to the extent permitted by law.

2. PURPOSE

To regulate the use of computing and information technology at CMCC and to inform users of electronic monitoring of users by CMCC.

3. SCOPE

Everyone using CMCC information technology.

4. INFORMATION AND COMPLIANCE PLANS (not a comprehensive list)

Privacy and Confidentiality

CMCC's electronic monitoring is aimed at collecting information related to its business. However, some information collected by electronic monitoring may be considered personal information. When personal information is under CMCC control, it is the responsibility of CMCC to protect it.

All information collected through electronic monitoring will be securely stored and protected. If any personal information is collected, its use and disclosure will be limited to achieve the stated purpose of its collection. CMCC will adhere to all privacy and confidentiality legislation that applies to the collection, use, and disclosure of personal information obtained by electronic monitoring.

- Copyright Act
- Criminal Code of Canada
- Employment Standards Act
- Personal Health Information Protection Act (PHIPA)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Working for Workers Act (Bill 88)

5. RELATED POLICIES (not a comprehensive list)

- Attendance – Employees
- Code of Conduct
- Collective Agreement between CMCC and CUPE Local 4773
- Conflict of Interest and Conflict of Commitment
- Copyright
- Discipline – Employees
- Discipline - Students
- Email - Employees
- Email – Students
- Employment Classifications
- Examinations
- Hours of Work
- Information Technology - Device Security
- Privacy
- Recording of Lectures and Other Instructional Activities
- Record Management, Retention and Destruction
- Representation of CMCC
- Working from Home

6. DEFINITIONS

Electronic monitoring is using technological, electronic, or digital means to track, or monitor usage of CMCC information technology.

Personal information is any factual or subjective information about an identifiable individual.

New Policy Approved (date):	New Policy Approved (date): September 2005 – Computing and Information Technology Use
Policy Revision History (dates):	Policy Revision History (dates): September 2022 – Computing and Information Technology Use and Monitoring - INTERIM March 2023 – Information Technology – Acceptable Use & Electronic Monitoring

----------END OF POLICY----------

7. PROCEDURES

Below are the procedures appropriate for the use of CMCC information technology.

Users must:

- be responsible for using CMCC information technology in an effective, ethical, and lawful manner
- respect the property of others, including intellectual property
- respect the copyrights of the owners of all software and the data they use
- respect the licensing agreements entered into by CMCC
- respect privacy and confidentiality
- use only CMCC information technology for which they have authorization
- use CMCC information technology and services for their intended purposes only
- take reasonable steps to protect the integrity and security of CMCC information technology including hardware, software, and data
- properly identify themselves in any electronic correspondence and provide valid, traceable identification if required by applications or servers at CMCC, or in establishing connections with information technology
- ensure that usernames and passwords are confidential
- recognize that any and all software or file(s) downloads via the Internet into CMCC's network or directly onto the user's computer become the property of CMCC
- ensure that all files downloaded from the Internet are checked for viruses
- recognize that their hardware, software, and Internet use will be randomly audited to ensure that software license requirements are met, that there is no

activity which is harmful to the systems, and that there is no inappropriate information or data accessed or stored

- use the Internet for non-business research or browsing during meal time or other breaks or outside of work hours, provided that all other usage policies are adhered to.

Users shall not:

- access systems or data without authorization (e.g., hacking)
- alter systems and/or software configuration provided by CMCC without authorization
- remove from CMCC any hardware or software licensed to CMCC, without written authorization and approval from the Division of Information Technology
- copy software and/or data without authorization for personal use or distribution
- destroy or remove hardware, software and/or data without authorization, or disclose data without authorization
- attempt to disable, defeat or circumvent any security feature that has been installed to assure the safety and security of CMCC
- access, archive, store, distribute, edit or record any sexually explicit material using CMCC's network or computing resources
- deliberately or knowingly propagate malicious software (malware)
- download or distribute pirated software or data
- download or copy onto CMCC computer any entertainment software or games, or play games against opponents on the Internet
- deliberately and unnecessarily degrade or monopolize CMCC Internet connections and bandwidth
- misrepresent themselves as another user or as an official representative of CMCC, without expressed permission
- disclose confidential passwords, access codes, account numbers or other authorizations assigned to them
- use or change another employee's password without authorization
- use CMCC information technology and resources for unauthorized purposes, including but not limited to unauthorized commercial purposes.

New Procedure Approved (date):	New Procedure (date): September 2005 – Computing and Information Technology Use
Procedure Revision History (dates):	Procedure Revision History (dates): September 2022 – Computing and Information Technology Use and Monitoring - INTERIM March 2023 – Information Technology – Acceptable Use & Electronic Monitoring

8. ATTACHMENTS

None