Policy Title:	Computing and Information Technology Use and Monitoring - INTERIM		
Category:	☐ Institutional - Board ☒ Institutional - Administrative	☐ Academic - Administrative ☐ Employment - Administrative	
Approved by:	☐ Board	☒ President	
Date approved:	September 29, 2022	**Effective date:**	September 29, 2022
Policy Sponsor:	Chief Information Officer	**Date last reviewed:**	September 29, 2022
Date of Mandatory Review (expiry date)	December 2022	**Date of last revision of Procedures**	n/a

1 POLICY

1. Access to CMCC's computing and information technology facilities is a privilege. CMCC reserves the right to grant or deny access and utilization of computer and information technology facilities.

2. The users of computing and information technology facilities are required to operate within the Computing Code of Conduct (see Procedures). Implicit in this is an obligation to report infractions within this Code.

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

4. Users of CMCC's computing and information technology facilities are not to assume that electronic communications are private. CMCC reserves the right to review, audit, intercept, monitor and access all messages and files, including without limitation email, on CMCC's on-line systems. This includes random on-line monitoring of Internet users as well as the maintenance and review of electronic logs of all Internet websites accessed via CMCC's resources.

5. Examples of ways CMCC electronically monitors its employees include:
    a. Surveillance (security) cameras are located 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. There is a record maintained of users accessing the facilities by using CMCC-issued keycards.
    c. The IT division maintains computer records of network access, Internet access, network threat detection and use of software and software services licensed by CMCC. These records also include digital copies of emails sent and received by employees using the CMCC network and email services.
    d. 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. Employees assigned to 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.

f. There is an electronic record maintained of persons using the CMCC app for COVID-19 screening.
g. Persons using the Panopto® video recording system or the clinic electronic health record system have their access and other usage tracked by those platforms.
h. Access to some laboratories and other facilities may be reserved and tracked by apps or other login/reservation systems.
i. Use of collaboration software and platforms may produce a record of user activity.

6. 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 the civil, criminal or administrative law.

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 computing facilities.

4 INFORMATION AND COMPLIANCE PLANS (not a comprehensive list)

- Copyright Act
- Criminal Code of Canada
- Working for Workers Act, 2022

5 RELATED POLICIES (not a comprehensive list)

- Computing Device Security
- Conflict of Interest and Conflict of Commitment
- Email - Employees
- Email – Students
- Privacy
- Representation of CMCC

6 DEFINITIONS

Electronic monitoring - Using electronic means to observe, record, track, or collect data on employees (including but not limited to location and resource use), where such information may be accessed and/or reviewed by CMCC or someone acting on the CMCC's behalf.

New Policy Approved (date):
September 2005

Policy Revision History (dates):

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

7 PROCEDURES

CMCC's "Computing Code of Conduct" (below) outlines procedures appropriate for the use of CMCC computing and information technology.

Users shall:

- be responsible for using these facilities 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 those facilities for which they have authorization
- use facilities and services for their intended purposes only
- take reasonable steps to protect the integrity and security of the facilities 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 the facilities

- ensure that usernames and passwords are confidential, and that passwords are changed not longer than every 120 days

- 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 before the files are run

- 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 facilities 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 by completing an Offsite Equipment Release form

- 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 facility that has been installed to assure the safety and security of CMCC's networks

- access, archive, store, distribute, edit or record any sexually explicit material using CMCC's network or computing resources

- deliberately or knowingly propagate any virus, worm or Trojan horse

- download or distribute pirated software or data

- download or copy onto CMCC's computer and technological facilities any entertainment software or games, or play games against opponents on the Internet

- interfere with the processing of a system (such as deliberately overextending the resources of a system) by unnecessary use of the network or Internet

- 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

- change another employee's password without authorization

- use CMCC facilities and resources for unauthorized purposes, including unauthorized commercial purposes.

New Procedure (date):
September 2005

Procedure Revision History (dates):

8 ATTACHMENTS

None