Policy Title: Personal Information Protection

Category:	☐Institutional - Board ☐Academic - Administrative ☐Institutional - Administrative ☒Employment - Administrative		
Approved by:	☐Board ☒President		
Date approved:	September 2, 2021	Effective date:	September 2, 2021
Policy Sponsor:	Vice President, Administration and Finance	Date last reviewed:	September 2, 2021
Date of Mandatory Review (expiry date):	September 2026	Date of last revision of Procedures:	September 2, 2021

1. POLICY

1. CMCC employees are to abide by this institution's procedures and practices when handling personal information.

2. Employees who disclose personal information, contrary to this policy, will be subject to disciplinary measures up to and including discharge for cause.

3. Only employees authorized through a specific assigned job responsibility are permitted to handle personal information and/or respond to third party requests

2. PURPOSE

To preserve the privacy of the CMCC community.

3. SCOPE

All CMCC employees who are granted access to personal, privileged and/or confidential information.

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

- *Personal Health Information Protection Act* (PHIPA
- *Personal Information Protection and Electronic Documents Act* (PIPEDA)

Protecting the privacy and confidentiality of personal information is an important aspect of the way CMCC conducts its business. Collecting, using, and disclosing personal

information in an appropriate, responsible, and ethical manner is fundamental to CMCC's daily operations.

5. RELATED POLICIES (not a comprehensive list)

- COVID-19 Vaccination (Interim)
- Privacy
- Sick Leave and Salary Continuance Benefits
- Use of Computing and Information Technology

6. DEFINITIONS

Personal health information is information about an identifiable individual that relates to the physical or mental health of the individual, the provision of health care to the individual, the individual's entitlement to payment for health care, the individual's health card number, the identity of providers of health care to the individual or the identity of substitute decision- makers on behalf of the individual.

Personal information is any information about an identifiable individual and includes race, ethnic origin, colour, age, marital status, family status, religion, education, medical history, criminal record, employment history, financial status, address, telephone number, and any numerical identification, such as Social Insurance Number. Personal information also includes information that may relate to the work performance of the individual, any allegations, investigations or findings of wrongdoing, misconduct or discipline. Personal information does not include job title or business contact information.

Third parties are individuals/organizations other than the subject of the records or representatives of CMCC. Note that in certain circumstances, CMCC may be legally entitled to provide personal information to an external party acting as an agent of CMCC.

New Policy Approved (date):	
Policy Revision History (dates):	December 13, 2011 September 2, 2021 now includes Third Party References 2011

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

7. PROCEDURES

1. Employees are responsible for:
   a. ensuring their personal information is kept current (name, address, phone number, dependents, etc.)

b. being familiar with and following policies and procedures regarding personal information

c. being familiar with and following policies and procedures regarding CMCC's approach to third party reference requests.

d. obtaining the proper consents and authorizations prior to disclosure of personal, privileged and/or confidential information.

e. immediately reporting any breaches of confidentiality to their manager.

f. keeping private passwords and access to personal, privileged and/or confidential data.

g. explaining this policy to clients and referring them to the Chief Privacy Officer, if necessary.

h. relinquishing any personal, privileged, confidential or client information in their possession before or immediately upon termination of employment.

2. Managers are responsible for:

   a. ensuring policies and procedures regarding the collection, use and disclosure of personal information are consistently adhered to.

   b. responding to requests for disclosure after the proper release is obtained.

   c. cooperating with the Chief Privacy Officer and Director of Human Resources to investigate complaints or breaches of policy.

   d. obtaining any personal, privileged, confidential or client information from terminated employees prior to their termination exit.

   e. ensuring that disclosure of personal information or personal health information to a third party is done with the approval of the Chief Privacy Officer and the Director of Human Resources in order to minimize risk of non-compliance with applicable legislation.

3. The Division of Human Resources and/or Payroll are responsible for:

   a. obtaining consent to the collection and use of personal information from employees.

   b. maintaining systems and procedures to ensure employee records are kept private.

   c. obtaining the proper consents and authorizations prior to disclosure of information contained in employee records.

   d. responding to employees' requests for access to their files.

   e. ensuring proper disposal of unnecessary files/information.

f. maintaining separate files to ensure that personal health information is protected

g. ensuring that disclosure of personal information or personal health information to a third party is done with the approval of the Chief Privacy Officer, Chief Health Records Custodian, and/or Director of Human Resources in order to minimize risk of non-compliance with applicable legislative or regulatory regimes bodies.

4. The Chief Privacy Officer is responsible for:

   a. internal compliance with applicable policies or legislation.

   b. cooperating with managers, Human Resources and/or Payroll personnel in developing internal policies for the collection, use and disclosure of personal information and personal health information of employees and clients.

   c. monitoring and responding to third party requests for personal information or personal health information.

   d. ensuring appropriate consents are obtained for the collection, use and disclosure of personal information and personal health information.

   e. where collection, use or disclosure is permitted without prior consent, notifying individuals of the collection, use and disclosure of personal information and/or personal health information after such occurrence.

5. Employee Records:

   a. Only Human Resources and Payroll personnel will have access to employee records containing personal information unless the Director of Human Resources determines that other access is permissible and necessary. Personal information and personal health information will not be disclosed outside of the organization without the knowledge and/or approval of the employee. Notwithstanding the foregoing, CMCC will cooperate with law enforcement agencies and will comply with any court order or law requiring disclosure of personal information without the employee's consent.

   b. Employees may request access to review their own file by making arrangements with the Division of Human Resources, providing at least 24 hours' notice. Employees may obtain a copy of any document in their file which they have signed previously. No material contained in an employee file may be removed from the file. A representative of the Division of Human Resources will be present during viewing of the file.

   c. Employee files cannot be removed from the Division of Human Resources.

d. An employee may provide a written notice of correction related to any data contained in the employee's file. The notice of correction will be provided to the Division of Human Resources.

e. Unless retention of personal information is specified by law for certain time periods, personal information that is no longer required to fulfil the identified purpose will be destroyed, erased or made anonymous within 12 months after its use.

6. Employee References:

   a. Any reference request, either oral or written, received by an unauthorized employee is to be forwarded immediately to the Director of Human Resources for action and/or response.

   b. Reference information to be provided to potential employers is to be limited to factual information authorized in writing by the employee or ex-employee in a document which is kept in the employee's or ex-employee's personnel file.

   c. The release of information related to a credit or loan application is to be authorized by the employee in writing. Alternatively, Human Resources may provide a letter of confirmation, on CMCC letterhead, to the employee which can then be used by the employee.

   d. In the event that no written authorization to release specified information to a third party is received, only the employee's or ex-employee's business title, job duties, and dates of employment will be disclosed.

7. Notwithstanding paragraph 5.e. above, personal information that is the subject of a request by an individual or a Privacy Commission will be retained as long as necessary to allow individuals to exhaust any recourse they may have under PIPEDA and PHIPA.
8. Concerns or complaints related to privacy issues must be made, in writing, to the Chief Privacy Officer setting out the details of the concern or complaint. The Chief Privacy Officer will investigate the matter forthwith and make a determination related to the resolution of the concern(s) or complaint(s).
9. An employee will not be penalized, disadvantaged or denied any benefit of employment pertaining to the actions described in a., b., and/or c. below as long as they have reasonable belief and are acting in good faith and have:

   a. disclosed to the Privacy Commissioner of Canada that CMCC or any other person has contravened or intends to contravene a provision of PIPEDA/PHIPA related to the protection of personal information.

   b. refused or stated the intention of refusing to do anything that it is in contravention of a provision of PIPEDA/PHIPA related to the protection of personal information.

c. done or stated an intention of doing anything that is required to be done in order that a provision of PIPEDA/PHIPA related to the protection of personal information not be contravened.

10. An employee who is found to be in breach of this policy will be subject to discipline up to and including discharge for cause.

New Procedure Approved (date):	
Procedure Revision History (dates):	December 13, 2011 September 2, 2021 now includes Third Party References 2011

8. ATTACHMENTS

None.