

## **Fundamentals of the College of Dietitians of Manitoba Privacy Policy**

In 1997, the Government of Manitoba passed laws, which set out the requirements for managing personal, and personal health information held by public bodies and organizations. The Acts were *The Freedom of Information and Protection of Privacy Act (FIPPA)* and *The Personal Health Information Act (PHIA)*. These Acts prescribe a number of information management practices regarding the collection, use, disclosure, retention, and security of personal information.

Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- Age, name, ID number, income, ethnic origin
- Employee files,
- medical information

Organizations who obtain personal information from individuals are required by the Act to develop a Privacy Code. The Code consists of 10 principles of fair information practices, which form ground rules for the collection, use and disclosure of personal information. These principles outline to individuals how their personal information is handled. The principles that businesses must follow are:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Provide recourse

Enclosed within this chapter is the privacy code of the College of Dietitians of Manitoba.

All individuals, who are employed, retained, volunteer or appointed by the College are required to preserve secrecy with respect to all information that comes to their knowledge.

All personal information obtained by the College is subject to the provisions of this Privacy Code. Personal information does not include the name, title, business address or telephone number of an individual. This information referred to as “business card” information is not covered under these Acts as private.

The Privacy Officer for the College of Dietitians of Manitoba is the Registrar.

---

## Definition of Terms

The following terms used in this Privacy Code are stated below:

### **Bylaws**

Means the bylaws of the College passed under the authority of section 51(1) of the *Registered Dietitians Act*.

### **College**

Means *College of Dietitians of Manitoba*.

### **Legislation**

Means *Registered Dietitians Act (2002) of Manitoba*, Regulations (2004) and Bylaws.

### **Member**

Means a member of the College.

### **Organization**

Includes an individual, a corporation, an association, a partnership, and a trade union.

### **Personal Information**

Means information about an identifiable individual but does not include the name, title, or business address or telephone number of an individual.

### **Regulations**

Means the Regulations under the *Registered Dietitians Act*.

---

## Principles

### Principle 1                      Accountability

The Registrar has been designated the official privacy officer for the College and is responsible for the organization's compliance to the legislation policy.

All volunteers of the college and employees shall receive an orientation and training, if necessary, of their obligations pursuant to this legislation. All individuals who, on behalf of the college, have access to personal information on college members shall be required to sign confidentially agreements (CDM Confidentiality Form) and uphold the confidentiality policies of the College.

All College confidentially policies can be obtained by the public during regular office hours. Once available, they shall be posted on our website.

### Principle 2                      Identifying Purposes

#### Information related to Members of the College

CDM may collect, hold and use the personal information in a member's file for the administration and enforcement of the *Registered Dietitians Act*. Those purposes within the Act are as follows:

1. Identifying and ensuring the accuracy of the information contained within the member's file;
2. To assess whether a potential member meets or a member continues to meet the standards of qualification for registration;
3. To investigate complaints regarding the conduct or actions of a member;
4. To investigate whether a member has committed an act of professional misconduct or is incompetent;
5. To hold a hearing of allegations of a member's professional misconduct or incompetent or of allegations that a member is incapacitated;
6. To carry out the obligations of the Continued Competence program of the college;
7. To assess whether a former member's certificate of registration should be reinstated;
8. Meeting all legal and regulatory requirements of the Act.

The College may collect personal information regarding a member for registration pursuant to section 7(2) of the Act.

The College may collect personal information regarding a member of the college or an employer as permitted within the Act Section 20(4).

Personal information disclosed to the College by a third party is used only for the purpose for which the disclosure was made or to enable the College.

---

---

### Information related to Employees or Volunteers of the College

CDM may collect, hold and use the personal information of an individual who is retained, elected or appointed for the purpose of administering the Registered Dietitians Act. Those purposes within the Act are as follows:

1. To communicate with the person on college business;
2. The purpose of making payroll and providing benefits as required by law;
3. To review prospective candidates and appoint persons as required by the Act.

### **Principle 3                      Consent**

The College collects personal information for the administration and enforcement of the legislation of the Registered Dietitians Act.

The College abides by the following principles in limiting use of information:

1. The individual shall be informed in a meaningful way of the purposes for the collection, use or disclosure of their personal data;
2. Personal information is used only for the purpose for which it was obtained or for a use consistent with that purpose under the privacy act;
3. Consent is obtained from the individual before using personal information for a purpose not consistent with the purpose for which it was collected or for a purpose not directly related to the purpose for which it was collected;
4. Policy 3.3.5 states the employee (s) who have access or use of the personal information and maintain a disclosure log or audit trail;
5. Access is limited to other individuals as a “need to know” basis and used with the highest degree of anonymity to meet the stated purpose;
6. If disclosure is not obtained, the disclosure is authorized according to a specific provision of Section 44 (1) of FIPPA or Section (22) of PHIA;
7. Consent can be obtained in a variety of ways, as outlined within the College Policy.
8. Once obtained, the record of consent shall be recorded as per the College Policy.
9. Training for staff is conducted to ensure that those employees collecting personal information are able to answer an individual’s questions about the purpose (s) of the collection.

### **Principle 4                      Limiting Collection**

The College will collect only the personal information that is required for the purposes outlined in Principle 2 of this Privacy Code.

Individuals, who are subject to the college requiring any personal information, shall be informed of the reasons and purpose of collecting their information.

---

---

## **Principle 5                    Limiting use, Disclosure and Retention**

The College abides by the following principles concerning the use, disclosure or retention of individual's personal information:

1. The use or disclosure of personal information is obtained only for the purposes outlined in Principle 2 of this Privacy policy;
2. The use or disclosure of personal information is released only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Registered Dietitians Act;
3. Personal information will be kept on file according to the College Policy.
4. Personal information which is no longer required will be destroyed as per the College Policy.
5. Any new purpose for the use of personal information shall be documented to those individuals effected by the release of the information;
6. Reviews, which determine whether personal information is still required to be retained, shall be conducted as per the College Policy.

## **Principle 6                    Ensure Accuracy**

The College shall ensure to the best of its ability that the information collected used and disclosed shall be accurate.

To ensure this accuracy, members are required to provide the College with current name contact information and employment information annually with the college renewal form.

Members are also asked to advise the College of any changes to the stated information within Thirty (30) days of the change.

## **Principle 7                    Safeguards**

The responsibilities of the College are to ensure all personal information is protected in the following ways:

1. Protect personal information against loss or theft;
2. Safeguard the information from unauthorized access, disclosure, copying, use or modification;
3. Protect all formats of personal information.

The College ensures that personal information is stored in electronic and physical files are secure. Security measures that are in place to safeguard this information as outlined by the College Policy.

Employees of the College will receive orientation training regarding the safeguarding for personal information.

The College ensures that all personal information that is no longer required is disposed of in a confidential and secure manner.

---

## **Principle 8                      Openness**

The policies in regards to confidentiality for all forms of personal information are available to the public and all college members by contacting the college.

Inquiry may be directed to the Registrar at the College office in a variety of ways:

College of Dietitians of Manitoba  
36-1313 Border Street  
Winnipeg, MB  
R3H 0X4  
Phone: 1-204-694-0532  
Fax: 1-204-889-1755  
Email: office.cdm@mts.net

## **Principle 9                      Individual Access**

The College has the responsibilities to provide an individual access to their personal information in the following ways:

1. When requested in writing to the Registrar, an individual may receive access to the personal information the College has on file;
2. Once access is obtained, the College can provide information on how this information has been used or is being used, and provide a list of any organizations to which this information has been disclosed;
3. Allow the individual to correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient;
4. Provide a copy of the information requested, or reasons for not providing access, subject to the exceptions as set out in Section 9 of the Act (stated below);
5. The College must note any disagreements on the file and advise third parties where appropriate.

Exceptions to access in Section 9 of the Act

The College *must* refuse an individual access to personal information:

1. If it would reveal personal information about another individual unless there is consent or a life-threatening situation;
2. If the organization has disclosed information to a government institution for law enforcement or national security reasons.

The College *may* refuse access to personal information in the information falls under one of the following:

1. Solicitor-client privilege
2. Confidential commercial information

- 
3. Disclosure could harm an individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law (the Privacy Commissioner of Canada must be notified).
  4. It was generated in the course of a formal dispute resolution process.

In order to provide access to individuals to personal information, the College shall:

1. Provide any help the individual needs to prepare a request for access to personal information.
2. Request from the individual to supply any information to enable it to account for the existence, use and disclosure of personal information.
3. Response to the request as quickly as possible and not later than 30 days after receipt of the request. Should the College be unable to respond within the 30 day time limit, the Act [Subsection 8(4)] allows an extension for a minimum of 30 additional days after notification to the individual.
4. Provide access at typically no cost or minimal cost to the individual, depending on the nature of the request and the amount of information involved. The College reserves the right to impose a cost recovery fee. In these circumstances, the College will inform the individual of the approximate cost to provide the response and proceed upon payment by the individual of the cost.
5. Ensure that the requested information is understandable, with an explanation of acronyms, abbreviations and codes, if necessary.
6. Provide the individual with reasons why, in writing, it is refusing to give access, setting out the reasons and any recourse available.
7. Maintain all personal information on members within their personal file, so the information is located in one place.

## **Principle 10                      Recourse**

All individuals have the right to recourse on a decision of the College on access to their personal information. Complaints, questions or concerns regarding the College's compliance with this Privacy Code can be directed to the Registrar of the College. If the Registrar cannot satisfactorily resolve a complaint, the individual can register a formal complaint with the Council of the College consistent with the College Policy.

---

## Access to Personal Information in College Files

Where the College holds personal information about an individual it shall allow access to this information unless in breach of the College Privacy Code (Principle 9). The College has a right of appeal where access is denied.

### Process

1. Upon receipt of a written request, the College shall allow the individual access to the information held within their file. Reasons where access would be denied are outlined within the College's Privacy Code.
2. Individuals should send their written request for access to the Registrar at the current College address.
3. The College makes every effort to respond to the request within thirty (30) days and to assist the individual in understanding the information.
4. In the case where the personal information or record was obtained from another organization, the College will refer the individual to the originating organization.
5. The College's response will typically be provided at no cost or minimal cost to the individual, depending on the nature of the request and the amount of information involved. However, the College reserves the right to impose a cost recovery fee. In these circumstances, the College informs the individual of the approximate cost to provide the response and proceed upon payment by the individual of the cost.
6. Should the individual's request be denied, a written response of the reasons for denying access will be sent.
7. If the Registrar is unable to satisfactorily resolve a complaint, the matter is referred to the College Council.
8. The Council reviews the complaint at the request of the individual, and take appropriate measures based on the legislation and Privacy Code.

---

---

## Records Retention of the College

Documents of the College are maintained, stored and disposed of according to the attached schedule.

### Membership Files

<u>Type of Record</u>	<u>Method of On-site Storage</u>	<u>On-site Retention</u>	<u>Archive (on-site, off-site or electronic format)</u>	<u>Method of Destruction</u>	<u>Additional Instructions</u>
Membership Data Base	Password protected electronic format on a server. Daily back up tape kept off-site.	Indefinitely in electronic format.	N/A	N/A	Historical data in maintained in the electronic file. Current information is updated on an ongoing basis.
Suspended	Locked Filing Cabinet	During period of suspension	N/A	N/A	
Non-Member (retired, resigned, revoked, nullified)	Locked Filing Cabinet	3 years	N/A	Confidential shred	Electronic information is retained
Deceased	Locked Filing Cabinet	1 year	N/A	Confidential shred	Electronic information is retained

## Application Files

<u>Type of Record</u>	<u>Method of On-site Storage</u>	<u>On-site Retention</u>	<u>Archive (on-site, off-site or electronic format)</u>	<u>Method of Destruction</u>	<u>Additional Instructions</u>
Active Applications	Locked Filing Cabinet	While file is open	N/A	N/A	
Registration Refused	Locked Filing Cabinet	5 years following registration decision	N/A	Confidential shred	Refusal letter to indicate retention periods and indicate that the applicant may have original documents returned to them (copy retained for duration of the retention period) or have certified copies provided at a cost. Electronic information retained.
Closed File • Application Withdrawn	Locked Filing Cabinet	5 years following file closure	N/A	Confidential shred	File closure letter to indicate retention periods and indicate that the applicant may have original documents returned to them (copy retained for duration of the retention period) or have certified copies provided at a cost. Electronic information retained.
Failed Registration Exam	Locked Filing Cabinet	3 years	N/A	Confidential shred	Electronic information is retained.
Registration Policies	Filing Cabinet or open shelves and in electronic format	Indefinitely if current	Archive only if policy is older than 5 years	N/A	Policies must show the dates for which the policy was in effect.
Board of Assessors Minutes including agenda and materials considered by the board (excluding applicant files)	Locked Filing Cabinet	5 years	N/A	Confidential shred	
Registration Administration Files	Filing Cabinet	3 years	N/A	Shred	
Registration and Exam General Enquiries	Hard Copy – locked filing cabinet E-copy local drive	1 year	N/A	Shred or delete	

## Continuing Competence Files

<u>Type of Record</u>	<u>Method of On-site Storage</u>	<u>On-site Retention</u>	<u>Archive (on-site, off-site or electronic format)</u>	<u>Method of Destruction</u>	<u>Additional Instructions</u>
Members' CC Submissions	Locked Filing Cabinet	7 years	N/A	Confidential shred	
CC Committee – minutes, including agenda and meeting materials	Unlocked Filing Cabinet	5 years	N/A	Shred	
CC Screening Committee	Locked Filing Cabinet	1 year		Shred	
CC Program Audit Evaluations/ Reports	Locked Filing Cabinet if contain personal information	1 year		Shred Confidential shred if contain personal information	
Policy binders and legal opinions	Open shelves	Indefinitely, if the policy is current	Archive 5 years after the policy has changed.	Shred	Policies need to indicate the dates for which they were effective.
CC Contracts and RFPs	Locked Filing Cabinet	3 years		Confidential shred	
CC Program Development / Project files	Filing cabinet/ open shelves	5 years		Shred	
CC Committee and other Dietetic regulatory body resource files	Filing Cabinet/ open shelves	1 year, longer at staff discretion	N/A	Shred	

## Financial Files

<u>Type of Record</u>	<u>Method of On-site Storage</u>	<u>On-site Retention</u>	<u>Archive (on-site, off-site or electronic format)</u>	<u>Method of Destruction</u>	<u>Additional Instructions</u>
Financial Statements	Locked Filing Cabinet	10 years	N/A	Confidential shred	
General Ledger	Locked Filing Cabinet	Indefinitely	N/A	Confidential shred	
Other financial information – journal entries, analysis	Locked Filing Cabinet	10 years	N/A	Confidential shred	
Other financial information - electronic		10 years	2 years		
Bank Information – statements, investment statements and general correspondence	Locked Filing Cabinet	10 years	N/A	Confidential shred	
Payroll Records	Locked Filing Cabinet	5 years	N/A	Confidential shred	
Payroll Records – e-copy	Password Protected	Tenure of staff member	N/A	Delete	

## Administration Files

<u>Type of Record</u>	<u>Method of On-site Storage</u>	<u>On-site Retention</u>	<u>Archive (on-site, off-site or electronic format)</u>	<u>Method of Destruction</u>	<u>Additional Instructions</u>
Office Management (inventory control, service/ maintenance agreements)	Locked Filing Cabinet	Maintain current hard copy 2 years	N/A	Confidential shred	
Admin Policies/ Bylaws (Current & History)	Filing Cabinet & Current Policies on Server	Current indefinitely	Archive only after 5 years	Shred. Throw away duplicates only.	
Regulation (Current & History)	On-line File Cabinet Or open shelves	Indefinitely		N/A	
Admin Project Files (eg. web site, data base, jurisprudence handbook)	Filing Cabinet	Hard copy 3 years	N/A	Shred	
Publication Files (resume, booklets, CC handbooks, annual reports)	Filing Cabinet	Hardcopy – indefinitely. E-copy of serve and website – indefinitely.	N/A		
General Correspondence – Registrar/ Chair	Filing Cabinet	2 years – hard copy	N/A	Shred & Delete	
General Correspondence – Other (request for materials, etc.)	Filing Cabinet	Hard copy – 2 years	N/A	Shred	
Reference Materials (newsletters, Annual reports – from other colleges and associations)	Filing Cabinet & open shelves	Hard copy – 4 years	N/A	Throw away	
Reference Materials: Regulatory Documentation from a variety of sources.	Filing Cabinet & open shelves	2 years or longer on discretion of staff	N/A	Throw away	
Legislative/ Regulatory Files	File Cabinet & open shelves	Current - indefinitely	10 years	Shred	Material is to be culled before storage and only material critical to history be retained.

## Human Resources Files

<u>Type of Record</u>	<u>Method of On-site Storage</u>	<u>On-site Retention</u>	<u>Archive (on-site, off-site or electronic format)</u>	<u>Method of Destruction</u>	<u>Additional Instructions</u>
Staff Files (excluding payroll)	Locked Filing Cabinet	Tenure of staff member plus 2 years	7 years	Confidential shred	
Staff Files – e-copy	Password protected	Tenure of staff			
Recruitment Files	Locked Filing Cabinet (Registrar access only)	1 year from close of recruitment	3 years	Confidential shred	
Vacation/ leave/ overtime charts with written requests and approvals	Locked Filing Cabinet (Registrar access only)	Tenure of staff		Confidential shred	Staff to sign off once a year on activity.

## Registrar Files

<u>Type of Record</u>	<u>Method of On-site Storage</u>	<u>On-site Retention</u>	<u>Archive (on-site, off-site or electronic format)</u>	<u>Method of Destruction</u>	<u>Additional Instructions</u>
Complaint Enquiries that contain personal complainant and/or member information	Locked Filing Cabinet (Registrar access only)	5 years	10 years	Confidential shred	Electronic information to be maintained
Complaints Files	Locked Filing Cabinet (Registrar access only)	5 years	10 years Archive only decision and reasons	Confidential shred	Electronic information to be maintained
Report Enquiries	Locked Filing Cabinet (Registrar access only)	5 years – unless additional reports received for the same concerns	10 years	Confidential shred	Electronic information to be maintained
Mandatory and other Report Files	Locked Filing Cabinet (Registrar access only)	5 years	10 years	Confidential shred	Electronic information to be maintained
Registrar's Report File – Formulation of Recommendation to Investigate	Locked Filing Cabinet (Registrar access only)	5 years	10 years	Confidential shred	Electronic information to be maintained
CC Referrals to Executive Committee	Locked Filing Cabinet (Registrar access only)	5 years from disposition or completion of undertaking	10 years	Confidential shred	Electronic information to be maintained
Discipline Files	Locked Filing Cabinet (Registrar access only)	5 years	10 years	Confidential shred	Electronic information to be maintained. Decision to be retained electronically.
Discipline Hearing Files	Locked Filing Cabinet (Registrar access only)	5 years	10 years	Confidential shred	Electronic information to be maintained. Decision to be retained electronically.
Policies related to Statutory Processes	File Cabinet or open shelves and in electronic format	Indefinitely if current	Archive after policy is older than 5 years, retain indefinitely	N/A	Policies must show the dates for which the policy was in effect.
Resource Material Related to Statutory Processes	Filing Cabinet Open Shelf Locked	Indefinitely if current and relevant	N/A	N/A	
Written Correspondence – including emails	Filing Cabinet/ drawer or in electronic format	3 years	N/A	Confidential shred	
Vendor Selection/ Contract files (current & expired)	Hard Copy – locked Filing Cabinet	3 years	4 years	Confidential shred	

---

---

### Council and Non-Statutory Committee Files

<u>Type of Record</u>	<u>Method of On-site Storage</u>	<u>On-site Retention</u>	<u>Archive (on-site, off-site or electronic format)</u>	<u>Method of Destruction</u>	<u>Additional Instructions</u>
Council and Committee Minutes including material used at meetings	Filing Cabinets or open shelves. Electronic copy retained on server.	5 years	Indefinitely archive an electronic copy.	Shred	