

Application Guide to the Privacy Code for Military Family Services Program

Contents

Introduction

About Canada's new National Standard for Personal Information Protection	1
Reasons why this Code is being adopted	2
Overview of the 10 Principles and Commentary	2

Detailed Explanation of the Code

Introduction	4
Definitions	6
Principles in Summary	8
Note about the continuing use of existing data	9
Principle 1 – Accountability	10
Principle 2 – Identifying Purposes	12
Principle 3 – Consent	16
Principle 4 – Limiting Collection	22
Principle 5 – Limiting Use, Disclosure and Retention	24
Principle 6 – Accuracy	28
Principle 7 – Safeguards	30
Principle 8 – Openness	32
Principle 9 – Individual Access	34
Principle 10 – Challenging Compliance	40
Appendix: Agreement for third party data processing	42

Introduction

This Application Guide is divided into two parts. The first three pages provide some background on the development of a new National Standard in Canada that forms the basis for the *Privacy Code for Military Family Services Program* (the Code), and why this new privacy code has been adopted.

Beginning on page 4 is a detailed explanation of the Code. The principles and sub-principles (commentary) of the Code appear on the left-hand pages. The right-hand pages contain detailed notes that help to explain the principles and how they should be applied.

About Canada's new National Standard for Personal Information Protection

The Canadian Standards Association *Model Code for the Protection of Personal Information* (CSA Code) was published in March 1996 and subsequently became a National Standard of Canada. This model code can be used by any organization as a basis for protecting the personal information of individuals. Personal information includes any information about a specific identifiable individual that is recorded in any form.

The CSA Code is based on privacy protection principles contained within a set of international data protection guidelines published by the Organization for Economic Co-operation and Development (OECD) in 1980. The OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* incorporate universally recognized privacy protection principles that were refined and restated in the CSA Code. The intent of the CSA Code was to make the OECD Guidelines more user-friendly and more relevant to the data processing environment of the 1990s.

Although the CSA Code was developed primarily for use by business organizations, it has equal application to any organization – including not-for-profit bodies, service agencies, etc. The 10 basic principles of the Code can be applied in any environment and to personal information collected in any form, including both paper-based files and electronic databases.

The Code is also intended to be tailored to specific organizational requirements. The drafters of the Code recognized that it would be applied to many different types of organizations with vastly different information management requirements. The CSA Code, therefore, has built-in flexibility to cover a wide variety of situations involving personal information collection, use and disclosure. Nevertheless, every one of the 10 principles expresses a strong obligation to safeguard the privacy rights of individuals whose personal information is collected by an organization.

The *Privacy Code for Military Family Services Program* is a tailored version of the CSA Code that incorporates all 10 principles and much of the commentary contained within the original Code.

Reasons why this Code is being adopted

Personal information about Canadian Forces (CF) members and their families that is collected and used within the CF is protected under the federal *Privacy Act*. However, the *Privacy Act* does not extend to organizations or institutions outside of the Government of Canada. Therefore, to ensure that personal information about members and their families continues to be adequately protected when transferred to a Military Family Resource Centre (MFRC) located within Canada, the *Privacy Code for Military Family Services Program* has been introduced.

The primary purpose is to ensure that nominal roll information about a member (including name, address and home telephone number) is only used for the purposes for which it is provided to an MFRC – to contact the member or family at the time of posting or deployment to explain the availability of mandated or other support services provided through the MFRC.

At the time of contact, the MFRC can provide information on all of its services and can collect other information from members and their families, with their knowledge and consent, in order to provide those services.

The personal information protections detailed in this Code apply equally to all personal information in the possession of the MFRC, including both nominal roll information transferred by the CF and any other information directly collected by the MFRC.

MFRCs will be expected to apply and maintain this Code with care and diligence on an ongoing basis. MFRCs may also be subject to provincial legislation governing the protection of personal information (see page 41). This Application Guide has been designed to provide guidance and advice in this process.

Overview of the 10 Principles and Commentary

The *Privacy Code for Military Family Services Program* includes all 10 principles of personal information protection contained within the *CSA Model Code for the Protection of Personal Information*, along with commentary from the CSA Code that is applicable to the operations of MFRCs.

The 10 principles and associated commentary are all inter-related and must all be applied with equal attention. Failure to adhere to the obligations established by every principle can weaken the overall protection of personal information under this Code.

The 10 principles establish core privacy rights for CF members and their families, as well as employees and voluntary staff of MFRCs, and any other individual about whom the MFRC collects uses or discloses personal information.

Under this Code, every individual about whom the MFRC may hold personal information has a right to inquire what specific information, if any, is held and for what purposes it is used. Individuals have a right to access their information, to have it amended if it is inaccurate or incomplete, and to challenge the purposes for which the information is collected, used or disclosed. Individuals can also challenge the compliance of the MFRC with any of the 10 principles.

Before collecting any personal information from members and/or their families, MFRC employees or volunteers, or any other individual, the MFRC must identify the purposes for which the information will be used or disclosed, and obtain the consent of the individual for those purposes. In addition, MFRCs must ensure the accuracy of information when used for decision-making purposes, safeguard the information appropriately, publicize their adoption of this Code, and engage in ongoing monitoring of their compliance with the Code.

Personal information collected prior to the adoption of this Code can continue to be used for existing purposes without the need to obtain consent, provided all other provisions of this Code are adopted and apply to this information (see the *Note about the continued use of existing data* on page 9 for more information on this).

Detailed Explanation of the Code

Introduction

In August 2000, the Director Military Family Services (DMFS) developed the *Privacy Code for Military Family Services Program* (the Code) to assist Military Family Resource Centres (MFRCs) in protecting the personal information of Canadian Forces (CF) members and their families that is provided to or collected by MFRCs located within Canada

The Code establishes the standard under which MFRCs within Canada collect and use personal information about Canadian Forces (CF) members and their families. Use of personal information, including nominal roll information provided directly by the CF when a member is posted or deployed is necessary for the provision of mandated services to members and their families. Personal information is also collected from MFRC employees, volunteers and third parties that provide services such as child care and will be similarly protected.

The *Privacy Code for Military Family Services Program* is a tailored version of the *CSA Model Code for the Protection of Personal Information - CAN/CSA-Q830-96*. The CSA Code became a national Standard of Canada in 1996. The 10 principles contained within the CSA Code reflect universal fair information practices that combine individual privacy rights with strong obligations to protect personal information collected and used by organizations.

For more information on the *Privacy Code for Military Family Services Program* and its application, please contact:

Director Military Family Services
Canadian Forces Personnel Support Agency
245 Cooper Street
Ottawa ON
K2P 0G2

Notes to the Introduction

The introductory text explains the purpose of the Code and its application to all personal information collected, used or disclosed by MFRCs that are located within Canada. Canadian Military Family Resource Centres (CMFRCs) located outside of Canada are subject to the federal *Privacy Act*.

The information subject to this Code includes information about CF members and their families, which can include children, parents, other relatives or other persons in a dependency relationship.

The information subject to this code also includes any personal information collected, used or disclosed about a third party where the information has been collected by an MFRC in the provision of services, for example, personal information collected about MFRC staff, and personal information about service providers such as caregivers, counselors, or other resource persons.

As defined within the Code (see *Definitions* section), nominal roll information about a member of the CF includes a member's name, home address and home telephone number by base/unit. The CF provides this information to an MFRC when a member is posted or deployed.

A posting message may include other information such as the number, names and ages of children. In general, MFRCs should only use the member's name, address and home telephone number for contact purposes and should not use any additional personal information that may be on a member's nominal roll file without the knowledge and consent of the member or family. If nominal roll information is added to MFRC files or an automated database, only the name, address and home telephone number should be added to the files or transferred to the database without the specific knowledge and consent of the member or family.

Under the terms of the Code, nominal roll information provided by the CF may only be used to contact a member and/or family at the time of posting or deployment.

At the time of contact, the MFRC can ask the member or family if they consent to the use of their information (including any additional information provided by the member/family) for purposes specified by the MFRC such as mandated services. For more information on how to identify and document purposes and how to obtain consent to use information for these purposes, see *Principle 2 – Identifying Purposes* and *Principle 3 – Consent*.

Anyone seeking information about the policy and standard of practice contained in this Code should contact the Director Military Family Services at the address listed.

However, the MFRC Director or staff should answer routine inquiries about the Code and about the MFRC's compliance with the Code.

It is hoped that MFRCs will be able to answer most routine inquiries. This Application Guide is intended to provide advice and guidance that will assist in doing so.

Definitions

Collection – the act of gathering, acquiring, or obtaining personal information from any source, including third parties, by any means.

Consent – voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the MFRC. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Deployment – the relocation of forces or individuals to desired areas of operation, exclusive of normal training or exercises.

Director – refers to the Executive Director of a Military Family Resource Centre (MFRC) located within Canada.

Director Military Family Services (DMFS) – the Directorate within DND/CF that has an oversight role with respect to an MFRC's compliance with this Code.

Disclosure – making personal information available to others outside the MFRC.

Member/family – is a member of the CF, or the spouse, parent or child, or those in a dependency relationship with the member.

Military Family Resource Centre (MFRC) – includes, for the purposes of this Code, only MFRCs located within Canada. Any personal information concerning members/families collected, used, or disclosed by Canadian Military Family Resource Centres (CMFRCs) located outside of Canada is subject to the federal *Privacy Act*.

MFRC staff - for the purposes of this Code, MFRC staff includes both paid employees and volunteers.

Nominal roll information – information about a member of the CF that includes a member's name, home address and home telephone number by base/unit. The CF provides this information to an MFRC when a member is posted or deployed.

Personal information – information about an identifiable individual (e.g. CF member/family, MFRC staff or a third party) that is recorded in any form.

Use – refers to the treatment and handling of personal information within an MFRC.

Notes to the Definitions

When personal information is provided to a third party for data processing purposes (for example, the mailing out of a newsletter), this is considered to be a transfer, not a disclosure. Principle 1 – *Accountability* explains the MFRC's continuing obligation to protect personal information that has been transferred to a third party to perform a data processing operation on behalf of the organization.

A disclosure occurs when information is made available to a third party where the MFRC no longer has control over the information and any subsequent uses.

All consent must be voluntary and based upon an individual's knowledge of how personal information will be used or disclosed. Consent can be either express consent, e.g. where the consent is explicitly provided as, through example, a signature, or implied consent, such as through the action or the inaction of an individual. These concepts and the appropriate use of express and implied forms of consent are all described more fully under Principle 3 – *Consent*.

The concept of deployment is described in this Code. A more temporary deployment of less than 30 days would not qualify as a basis for the MFRC to contact a member's family.

The definition of Member/family within this Code includes anyone in a dependency relationship, which can be extended to include relatives such as a brother or sister, grandparent, uncle or aunt or another individual in a close relationship with the member. The key point is that all personal information that is provided via a nominal roll or is collected directly from a member or family must be equally protected under this Code.

Nominal Roll Information may include personal data other than a member's name, home address and home telephone number by base/unit. Any other personal information that may be contained on a nominal roll cannot be used without the consent of the member/family.

The definition of personal information does not include information that has been de-identified or aggregated for statistical purposes, provided this information cannot easily be re-personalized.

Principles in Summary

Principle 1 - Accountability

MFRCs are responsible for personal information under their control. The Director of an MFRC shall be accountable for the MFRC's compliance with the following principles.

Principle 2 - Identifying Purposes

The MFRC shall identify the purposes for which personal information is collected at or before the time the information is collected.

Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 - Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the MFRC. Information shall be collected by fair and lawful means.

Principle 5 - Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Principle 6 – Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7 – Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8 – Openness

MFRCs shall make readily available to individuals specific information about policies and procedures relating to the management of personal information.

Principle 9 - Individual Access

Upon request, a member/family, MFRC staff or third party shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 - Challenging Compliance

A member/family, MFRC staff or third party shall be able to address a challenge concerning compliance with the above principles to the Director of an MFRC who is accountable for the MFRC's compliance.

Notes to the Principles in Summary

The 10 principles are included within the Code in summary form for easy reference. However, in applying the Code, the commentary associated with each of the principles must also be taken into account. This commentary describes many further obligations that must be considered in implementation.

In addition, there are notes under Principles 3 and 9, which are considered to be part of the principles and provide further guidance on how these principles should be applied.

Note about the continued use of existing data

In adopting this Code, MFRCs can continue to use information previously collected about members/families, staff and third parties without the need to obtain consent for this existing data as long as the following requirements are met:

- 1) all other requirements of this Code apply to the existing data including the obligation to inform individuals about the purposes for which the data was collected and is being used and the individual right to withdraw consent for these purposes, as per clause 3.7;
- 2) any information not required to meet specified purposes, as per Principle 2 – *Identifying Purposes*, be removed from the files;
- 3) the existing information not be used for any new purposes without the knowledge and consent of the individual.

Principle 1 - Accountability

Principle 1 - Accountability

MFRCs are responsible for personal information under their control. The Director of an MFRC shall be accountable for the MFRC's compliance with the following principles.

- 1.1 Accountability for the MFRC's compliance with the principles rests with the Director, even though other MFRC staff may be responsible for the day-to-day collection and processing of personal information. In addition, MFRC staff may be delegated to act on the Director's behalf.
- 1.2 The MFRC is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The MFRC shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
- 1.3 MFRCs shall implement procedures as outlined in the Application Guide to the *Privacy Code for Military Family Services Program* to give effect to the principles, to include:
 - (a) implementing procedures to protect personal information;
 - (b) implementing procedures to receive and respond to complaints and inquiries about adherence to this Code;
 - (c) training staff and communicating to staff information about the principles and the accompanying procedures; and
 - (d) developing information to explain the principles and the accompanying procedures.

Notes to Principle 1

Under Principle 1 an MFRC is responsible for the protection of all personal information under its control, as per the obligations set out in this Code. The accountability for ensuring that all of the privacy protection principles of this Code are properly and adequately enforced rests with the Executive Director of the MFRC (the Director).

Under this Code, the Director must respond directly to inquiries and complaints from individuals whose personal information is in the custody of the MFRC, take action to investigate complaints and take appropriate action to amend procedures as necessary. In some situations, DMFS must also be consulted (for more information on responding to complaints, see Principle 10 – *Challenging Compliance*).

The Director is also responsible for training and overseeing other staff who may be involved in the day-to-day collection and processing of personal information. The Director may, however, delegate someone else to act on his or her behalf during times of absence.

Clause 1.3 requires Directors to implement the procedures that are contained within this Application Guide. This includes communicating information about the Code to members and families, staff and other individuals whose personal information is collected, used or disclosed by the MFRC.

Under Clause 1.2, the MFRC continues to be responsible for protection of personal information when the data is transferred to a third party for processing on the MFRC's behalf. For example, if an MFRC publishes a newsletter and contracts with a printer to mail it directly to members/families, steps must be taken to protect the mailing list from unauthorized use or disclosure.

A contract is typically the most important tool to prevent unauthorized use of personal information when it has been transferred to a third party. The contract should specify that personal information provided by the MFRC to the contractor shall only be used for purposes specified and authorized by the MFRC, and shall be protected with appropriate safeguards against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. The MFRC Director should discuss with the contractor the importance of protecting member/family personal information and review what steps the contractor proposes to take to ensure personal information is adequately protected when it has been transferred to the contractor. A sample contract form is attached as an appendix to this Application Guide.

In some cases, the MFRC should also monitor the contractor's compliance with the contract. This can be done through site visits or, in the case of mailing lists, through "seeding" the list. Seeding is the inclusion of names or addresses (often fictitious) that can be monitored by MFRC staff to trace if a list is being used for any unauthorized purposes.

Principle 2 - Identifying Purposes

The MFRC shall identify the purposes for which personal information is collected at or before the time the information is collected.

- 2.1** The MFRC shall document the purposes for which personal information is collected in order to comply with Principle 8 – *Openness* and Principle 9 – *Individual Access*.

- 2.2** Personal information about members/families is usually collected from several sources. Nominal roll information as defined under this Code (see *Definitions* section) is transferred to MFRCs by the CF solely to communicate with a member/family when a member is posted or deployed. The consent of the member/family is not required to transfer nominal roll information to an MFRC. Other personal information about members/families, staff or third parties may be collected directly by the MFRC. However, the knowledge and consent of the member/family, staff or third party is required for the use and/or disclosure of this information (see Principle 3 – *Consent*).

Notes to Principle 2

A fundamental principle of personal information protection is that information must not be collected from individuals without first identifying the purposes. The MFRC must know why it needs specific personal information; the information that is collected must only be what is necessary to fulfil the purposes, and individuals must have a right to challenge both the purposes and the amount of information required to fulfill them.

As stated in clause 2.1, MFRCs must document all purposes for which they require personal information. In order to do so, they should review the services they offer and list the specific types of personal information required from all parties and all sources in order to provide these services. The result of this exercise should be a simple checklist with purposes in one column and the associated personal information required for these purposes in the other column, as per the following example:

Purpose	Personal Information Required
To mail out a newsletter to members.	Name and mailing address
To provide emergency child care.	Names of parents or legal guardians, address, phone number, number of children, names and ages, any other special information required (health, dietary or environmental concerns)

MFRCs must then use this checklist to review the current personal information under their control concerning members/families, MFRC staff and any third parties. Personal information that is not required for any of the specified purposes must no longer be used or retained and must be immediately deleted or destroyed.

The notes to Principle 5 – *Limiting Use, Disclosure and Retention* provide guidance on destroying personal information and address the issue of how long existing data that is linked to an identified purpose may be retained within a file. The notes to this principle should be reviewed before undertaking a file review.

Since reviewing all information within existing files may pose an administrative burden, this process can be accomplished over a number of weeks.

As explained in clause 2.2, member/family personal information can come from several sources, predominantly that which is provided by the CF (nominal roll information) and that which is subsequently collected by the MFRC directly from the member or family for the purposes of offering mandated services.

Nominal roll information must be used solely to contact the member and/or family at the time of posting or deployment to explain the services available through the MFRC. At the time of this contact, the consent of the member and/or family can then be obtained to allow personal information (including nominal roll information) to be used for subsequent purposes such as mailing out the MFRC newsletter or requesting participation in the annual needs survey.

Principle 2 - Identifying Purposes (continued)

- 2.3** The identified purposes for collecting all personal information except nominal roll information shall be specified at or before the time of collection to the member/family, staff or third party from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form or registration form, for example, may give notice of the purposes.
- 2.4** When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose.
- 2.5** Persons collecting personal information shall be able to explain to individuals the purposes for which the information is being collected.

Notes to Principle 2 (continued)

Since the CF provides nominal roll information so that an MFRC can make an initial contact at the time of posting or deployment, it is not collected from the member/family and therefore the consent of the member/family is not required for this use. Moreover, this particular use will be self-evident to the member/family at the time of contact.

Under Clause 2.3, the purposes for collecting any other information from a member/family must be specified at the time of collection. This gives the individual the best opportunity to ask any questions about the intended uses.

This explanation can be kept to a general description, for example:

"MFRCs use nominal roll information provided by the CF and information provided by CF members and their families to contact families at the time of postings and deployments to inform families about MFRC events and services, and to plan and evaluate MFRC services."

If registration forms are used to participate in some programs or services, the purposes for any information collection should be clearly stated on the form, for example, "Any personal information provided on this form will be used solely for the following purposes: (list the purposes)."

When personal information has been collected by an MFRC for one set of purposes, Clause 2.4 prohibits the use of the information for new purposes without the consent of the individual. To alleviate the necessity of constantly seeking new consent, MFRCs should attempt to obtain consent for a range of purposes at the time that initial contact is made with a member/family. Methods of obtaining consent that lessen the administrative burden on the MFRC are discussed in more detail under Principle 3 – *Consent*.

Under Clause 2.5, information collectors (MFRC staff) must be fully informed about the purposes for which personal information is being collected and be able to explain these purposes to the individual.

The Director must ensure that all staff who collect personal information are as informed as possible about the purposes for which the information will be subsequently used. In the odd case, where an individual asks a question about personal information uses that a staff member cannot answer, the individual can be referred to the Director for a more complete answer.

TIP: The checklist of purposes and the associated personal information needed to fulfill the purposes should be kept handy. There should either be a master checklist that the Director or staff can refer to when reviewing purposes and information collection needs, or when explaining these to other individuals, or when copies of the checklist should be appended to individual files.

Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge or consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated.

- 3.1** Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, the MFRC will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use, for example, when the MFRC wants to use existing information for a new purpose not previously identified.
- 3.2** The principle requires "knowledge and consent". MFRCs shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.
- 3.3** The MFRC shall not require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes. Consent shall not be obtained through deception, for example, by misleading an individual about the true purposes for information collection, use or disclosure.
- 3.4** The form of the consent sought by the MFRC may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, MFRCs shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive; in fact, any information can be considered sensitive, depending on the context.

Notes to Principle 3

With limited exceptions, the knowledge and consent of the individual are always required for the collection, use, or disclosure of new personal information (see *Note on the continued use of existing data* – page 9).

Some exceptions to this requirement are identified in the note accompanying the principle. However, the passage in April 2000 of the federal government's *Personal Information Protection and Electronic Documents Act* further specified and limited the instances where data could legally be collected, used or disclosed without knowledge or consent by organizations subject to this Act.

The following situations where data may be collected, used or disclosed without the knowledge or consent of the individual are adapted from this Act and represent the sole exclusions to the consent requirement for MFRCs. In responding to any request by an outside source for the disclosure of personal information, the MFRC must first consult with the Chair of the Board of Directors of the MFRC who shall consult, in turn with DMFS.

Collection

Data may only be collected without the knowledge or consent of the individual where it is clearly in the interests of the individual and consent cannot be obtained in a timely way.

Use of collected data

Data may only be used without the knowledge or consent of the individual:

- i) where it is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- ii) to act in respect of an emergency that threatens the life, health or security of any individual.

Disclosure of collected data

Data may only be disclosed without the knowledge or consent of the individual:

- i) where it is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- ii) to a person who needs the information to respond to an emergency that threatens the life, health or security of another individual and, if the individual whom the information is about is alive, the MFRC informs the individual of the disclosure in writing, without delay;
- iii) on the MFRC's initiative to an investigative body or government institution and the information relates to an offence that has been or is about to be committed, or to activities suspected of constituting threats to Canada's security;
- iv) in response to a government institution with lawful authority to investigate any matter of national security, enforce any law, or administer any law of Canada or a province;
- v) to a barrister or solicitor, or in Québec, an advocate or notary representing the MFRC;

Principle 3 – Consent (continued)

- 3.5** The way in which the MFRC seeks consent may vary, depending on the circumstances, the type of information collected and the reasonable expectations of the individual. The MFRC should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. An authorized representative, such as a legal guardian or a person having power of attorney can also give consent.
- 3.6** Individuals can give consent in many ways, for example:
- (a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
 - (b) a checkoff box may be used to allow individuals to request that their personal information not be used for certain purposes. Individuals who do not check the box are assumed to consent to the use of this information; or
 - (c) consent may be given orally when information is collected over the telephone.
- 3.7** An individual may withdraw consent at any time, subject to reasonable notice. The MFRC shall inform the individual of the implications of such withdrawal.

Notes to Principle 3 (continued)

- vi) to comply with a subpoena, warrant or court order, or rules of court relating to the production of records;
- vii) as required by law.

Consent timing

There should be very few instances where it is not possible to obtain consent for the use or disclosure of personal information at the time that the information is collected. MFRCs must, whenever possible, obtain consent at the time of collection to avoid having to go back to the individual for subsequent consent, and to avoid the risk that the collected data will be inadvertently used before consent is obtained.

New purposes not previously identified always require new consent.

The knowledge requirement

In order to obtain a valid or meaningful consent, the individual must understand the purposes. This means that any explanation of the purposes, provided verbally or in writing must be clearly and simply stated. As stated in the notes under Principle 2, the statement of purposes should be broad enough to avoid the necessity of seeking additional consent for every specific and limited purpose. MFRCs should attempt to seek consent for future information purposes at the time that initial contact is made with a member/family.

Limitations on data required

As described in Clause 3.3, the MFRC cannot require an individual to provide any more information than is needed for the specified purpose. Where an MFRC wishes to acquire additional information that is legitimately needed to provide additional services or for planning purposes, the MFRC can ask for this additional information, as long as it is clear that the individual can decline to provide the additional data without any consequences.

Forms of consent

Clauses 3.4 through 3.6 address the methods of obtaining consent. There are two basic forms of consent: express consent and implied consent. Both are equally valid under the Code. However, because of its nature, implied consent is less certain and, therefore, should not be used where information of a more sensitive nature is being collected, used or disclosed.

As described in the *Definitions* section (see page 6) all consent is based on voluntary agreement with what is being done or proposed. However, express consent is explicit – in other words the individual has explicitly stated their consent to the collection, use or disclosure of personal information for the specified purposes either verbally or in writing. There is no ambiguity about the intent of the individual to allow their personal information to be collected, used or disclosed for the intended purposes. A verbal express consent should be recorded and dated by the MFRC.

This page intentionally left blank.

Notes to Principle 3 (continued)

Implied consent, on the other hand, is less certain because it often depends on the inaction of the individual. For example, one of the most common forms of implied consent results from offering an individual the opportunity to opt out of personal information uses (for example, with an opt-out reply card). If the individual declines to opt out, then the MFRC can assume that consent to use the information has been granted.

The uncertainty exists because the individual may have overlooked the opt-out opportunity, such as described under Clause 3.6 (b). For this reason, implied consent should not be used where sensitive data is involved. Moreover, when implied consent is used, the MFRC must provide continuing opportunities for the individual to opt out, for example, by posting information about the right to opt out of information uses on a regular basis in a newsletter, etc. The process for opting out should be as simple as possible and the MFRC must respond to any opt out request at the earliest possible opportunity.

Consent for minors

Where an individual is under the age of 14, MFRCs must obtain the consent of a parent or guardian for the collection, use or disclosure of any personal information.

Where an individual is between the age of 14 and the age of majority, MFRCs may collect or use personal information with the knowledge or consent of the individual, or a parent, or guardian at their discretion. In determining whether or not it is appropriate to obtain consent directly from the individual, the MFRC shall consider all relevant factors, such as the nature of the information, how it will be used, and whether a parent or guardian would reasonably expect to provide the consent. In some cases, where information is collected directly with the consent of the individual, it may also be appropriate to notify the parent or guardian about how the consent was obtained and how the information will be used.

Other than in a counseling relationship, no information concerning an individual between 14 and the age of majority may be disclosed to any other party without the knowledge and consent of a parent or guardian.

In a counseling relationship, where information is obtained from an individual between 14 and the age of majority, the decision on whether or not to disclose personal information about this individual to a parent, or guardian, or to a third party resides with the counselor, who is subject to the professional practice guidelines of the counselor-client relationship.

Consent withdrawal

Clause 3.7 addresses the right to withdraw consent. The "reasonable notice" reference recognizes that a withdrawal request cannot always be acted upon instantaneously (sometimes this is possible) and there may be a time delay before the information uses can be stopped, for example, if a newsletter is in the process of being mailed out. When consent is withdrawn, however, there must not be any new uses of the personal information.

MFRCs have an obligation to explain the impacts of withdrawing consent. The MFRC should consider this requirement as an opportunity to explain the value of their services to the member/family. However, having done so, the MFRC must respect the right of a member/family to make an informed choice not to allow the use of their personal information by the MFRC.

Principle 4 – Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the MFRC. Information shall be collected by fair and lawful means.

- 4.1** MFRCs shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the identified purposes. MFRCs shall specify the type of information collected as part of their information-handling procedures, in accordance with Principle 8 – *Openness*.
- 4.2** MFRCs shall not mislead or deceive individuals about the purpose for which information is being collected. Consent with respect to collection must not be obtained through deception.

Notes to Principle 4

The intent of Principle 4 is to limit personal information collection to what is necessary for the specified purposes and to prevent unfair or unlawful means of information collection.

The information collected as per Principle 4 must be limited to what is absolutely necessary to allow the MFRC to carry out the purposes consented to by the individual.

The notes on Principle 2 explain the importance of documenting the purposes and the information required to meet those purposes. Principle 8 – *Openness* subsequently describes what information about the purposes must be provided to the individual.

Despite the requirement to limit information collection, this principle does not conflict with the legitimate need to collect personal information necessary to provide services in a professional and responsible manner. For example, if character references or background checks are considered to be a necessary requirement for individuals such as child care providers, such information collection should continue so as not to jeopardize the service. A checklist should be used, however, to ensure that only pertinent information is collected.

The concept of collection by fair and lawful means prohibits such practices as badgering individuals into giving their consent. Individuals should be invited and/or encouraged to take advantage of MFRC services to which they are entitled, but MFRCs must avoid applying pressure on members or their families to do so. As per Clause 4.2, deception cannot be used to gain information about any individual.

Principle 5 – Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

- 5.1** When personal information will be used for a new purpose, the purpose shall be documented (see Clause 2.1).
- 5.2** MFRCs shall adopt minimum and maximum retention periods for all personal information. Personal information that has been used to make a decision about a member/family shall be retained long enough to allow the individual access to the information after the decision has been made.
- 5.3** Personal information that is no longer required to fulfill the identified purposes shall be destroyed, erased, or made anonymous. MFRCs shall implement procedures to govern the destruction of personal information.

Notes to Principle 5

While Principle 4 limits collection of personal information, this principle prevents further uses or disclosure of previously collected information without additional consent, unless required by law. It also requires that retention limits be put in place.

Specifically, MFRCs shall not use or disclose existing personal information for any new purpose without the knowledge and consent of the individual. Any proposed new purpose shall be documented and consent shall be obtained before personal information is used or disclosed for this new purpose. The importance of defining purposes and a checklist approach for doing so are discussed in the notes to Principle 2.

The only exception to the above limitation is where the information is required by law – as in the case of disclosures of personal information to report suspected instances of child abuse or neglect.

MFRCs shall adopt the following procedures for the retention of personal information.

1. The date of collection and the date of any amendments to personal information shall be recorded on the file or database (see also the notes to principle 6 – *Accuracy*). This need not be done retroactively, but must be done on a going-forward basis.
2. Personal information shall be kept for two years from the date of the last administrative action on the file.
3. When the personal information of a member/family, staff or other individual is amended (see Principle 9 – *Individual Access*), any out-of-date, incomplete or inaccurate information shall be immediately discarded and the new information shall be kept for two years from the date of the last administrative action on the file.
4. Personal information that is the subject of a compliance challenge shall be retained as long as is required for the individual to exhaust any procedure to which they may be entitled through this Code or under law. See also Principle 9 – *Individual Access* and Principle 10 – *Challenging Compliance*.
5. When an MFRC receives reliable information that a member has been posted elsewhere, has left the service, or is deceased, personal information concerning the member/family, other than counseling records, shall be retained for two years from the date of the last administrative action on the file.

This page intentionally left blank.

Notes to Principle 5 (continued)

6. Counseling records shall be retained as long as required under professional practice guidelines.
7. All personal information about paid employees of an MFRC shall be retained on file throughout the duration of employment and for seven years after the end of employment. After seven years the information must be destroyed.
8. Personal information about volunteer staff of an MFRC shall be retained for two years after the volunteer is no longer an active volunteer with the MFRC. This two-year period provides an opportunity for an MFRC to maintain contact with a former volunteer for a reasonable period of time and provides the volunteer an opportunity to obtain references, letters of endorsement, etc. The timeframe for retaining volunteer personal information can be extended at the request of the volunteer.

In accordance with the established retention periods, when personal information is no longer required for the identified purposes, it must be destroyed or made anonymous. Personal information in paper-based files can also be returned to the individual to whom the information pertains at the discretion of the MFRC.

If personal information is made anonymous, for example, converted to non-personally identifiable statistical data, this must be done in such a way that it cannot be re-personalized. The data should, therefore, not be aggregated by classifications that are so small so as to allow an individual to be re-identified.

When information is destroyed, this shall be done in the following manner.

Paper files shall be shredded to prevent unauthorized disclosure of the information.

Electronic files, including e-mail messages, shall be over-written or deleted in such a way that the deleted information cannot be subsequently recovered.

When files have been stored on computer diskettes, the diskettes should be overwritten or reformatted. If computers used by MFRCs are disposed of, the hard drives should be reformatted (this process removes all data contained on the hard drive).

Personal information stored on any other media such as answering machines tapes or electronic voice mail must be routinely deleted. Photographs or video recordings of individuals may only be retained for archival or historic purposes with the permission of the individual.

Principle 6 – Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

- 6.1** The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.
- 6.2** Personal information shall not be routinely updated unless such a process is necessary to fulfil the purposes for which the information was collected. Nominal roll information used to contact members/families in the event of an emergency shall be kept as up-to-date as possible. This can be done through an annual verification call.
- 6.3** Personal information that is used on an ongoing basis, including information that is disclosed to third parties, shall generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

Notes to Principle 6

Principle 6 requires that information be as accurate as necessary for its intended purposes, while prohibiting any routine updating, unless it is necessary to fulfill the purposes for which the information is required.

Generally the information collected by MFRCs is provided either by the CF in the case of nominal roll information or is collected directly from the individual concerned. In such cases, the MFRC can assume that the nominal roll information is accurate; however, the accuracy and completeness of nominal roll information should be verified with an individual when the opportunity arises and can be verified on an annual basis through a verification call.

In the case of other information which is provided directly by the individual, the individual should be informed of his or her right to access personal information and to have it amended, as required – see Principle 8 – *Openness* and Principle 9 – *Individual Access*.

The date of collection and the date of any amendments to personal information shall be recorded on the file or database.

The MFRC shall provide regular reminders to individuals to keep their personal information up-to-date, for example, when an individual moves. The MFRC should stress the value to members/families of doing so.

MFRCs should generally not collect information about an individual from third parties unless there is a legitimate reason to do so, for example, a character reference for an MFRC staff member or third party service provider. In such cases, the MFRC should take extra care to ensure the third party information source is credible and that the information provided is likely to be accurate. If in doubt, decisions should not be made on the basis of such third party information. The source of any such information should also be noted in the information file. In some cases, the source of third party information can be withheld from the individual (see the Principle 9 – *Individual Access* and the note immediately under the statement of principle, p. 34).

In cases where personal information must be disclosed to a third party, the MFRC shall clearly set out for the third party any limits on the accuracy of the personal information, for example, by specifying when the data was last updated.

Principle 7 – Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

- 7.1** MFRCs shall employ security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. MFRCs shall protect personal information regardless of the format in which it is held.
- 7.2** The nature of the safeguards will vary depending on the type of information that has been collected, the amount, distribution, and format of the information, and the method of storage. All personal information in the custody of an MFRC shall be treated as "highly sensitive".
- 7.3** The methods of protection shall include:
- (a) physical measures, for example, locked filing cabinets and restricted access to offices;
 - (b) organizational measures, for example, limiting access on a "need-to-know" basis; and
 - (c) technological measures, for example, the use of a computer password or encryption.
- 7.4** MFRCs shall make everyone with access to personal information aware of the importance of maintaining the confidentiality of the information.
- 7.5** Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 5.3).

Notes to Principle 7

Security safeguards can be a weak link in the MFRC's information protection since their effectiveness depends to a large extent upon the willingness of MFRC staff to maintain procedures. The importance of doing so must be constantly stressed.

MFRCs must treat all personal information in their possession as "highly sensitive" and employ appropriate safeguards, including continual staff training.

Safeguards shall consist of the following, as a minimum:

1. Secure locks placed on filing cabinets containing personal information;
2. Secure locks on offices containing personal files;
3. All personal files locked away at the end of every work day;
4. No personal information left in plain view in offices where unauthorized people could access them;
5. Use of conspicuous labels to identify confidential personal information files;
6. Passwords on computers (changed frequently);
7. Computers located so that unauthorized persons cannot see personal information on a screen or easily access personal information within the computer;
8. Use of firewalls, encryption or other technological means to prevent unauthorized computer access. The simplest way to secure a sensitive database may be to keep it on a floppy diskette or a ZIP drive and not on the computer's hard drive. All computer files should be backed-up and kept in a secure location when not in use;
9. If voice mail or an answering machine is used, limit access to prevent unauthorized eavesdropping;
10. If a fax machine is used to transmit or receive personal information, make sure it is in a secure location. Phone ahead to alert the individual before transmitting personal information;
11. If e-mail is used to communicate, limit access with passwords and delete messages when they have been read and/or responded to;
12. If individuals request personal information over the telephone, MFRC staff should not provide this information without verifying the identity of the caller and their right to access the information. In emergency situations, a judgment call may be required, if personal information is provided to a third party in an emergency, the individual about whom the information was disclosed must be informed of the disclosure at the earliest possible opportunity;
13. Regular training and reminders to staff of the importance of security safeguards.

The disposal or destruction of personal information is discussed in the notes to Principle 5 – *Limiting Use, Disclosure, and Retention*.

Principle 8 – Openness

MFRCs shall make readily available to individuals specific information about policies and procedures relating to the management of personal information.

- 8.1** MFRCs shall be open about policies and procedures with respect to the management of personal information. Individuals shall be able to acquire information about these policies and procedures without unreasonable effort. This information shall be made available in a form that is generally understandable.
- 8.2** The information made available shall include:
- (a) how to contact the Director of the MFRC, who is accountable for the implementation of policies and procedures under this Code and to whom inquiries or complaints can be forwarded;
 - (b) the means of gaining access to personal information held by the MFRC;
 - (c) a description of the type of personal information held by the MFRC, including a general account of its use;
 - (d) a copy of any brochures or other information that explains the MFRC's policies and procedures; and
 - (e) what personal information is made available to other organizations, if any.

Notes to Principle 8

The Code requires that organizations be open about their privacy policies and communicate basic information to individuals about how their personal information is used, how to access their files, and how to make an inquiry or complaint about information handling policies or procedures.

MFRCs will be required to communicate the following basic information to members/families, staff and third parties about whom they hold personal information.

1. The fact that the MFRC has adopted this *Privacy Code for Military Family Services Program*.
2. The fact that the Director is accountable for the MFRC's compliance with the Code's principles and is the person to whom inquiries or complaints should be addressed.
3. How an individual can gain access to any personal information held by the MFRC (see the notes to Principle 9 – *Individual Access* for guidance on providing access to personal information).
4. A general description of what information is collected about a member/family, staff or third party and how it is used. For example:

"MFRCs use nominal roll information provided by the CF and information provided by CF members and their families to contact families at the time of postings and deployments to inform families about MFRC events and services, and to plan and evaluate MFRC services".

N.B. Separate descriptions should be developed for staff and third parties, as applicable.

5. A specific mention of any circumstances where information is made available to other organizations or individuals, for example where personal information may be disclosed with the knowledge and consent of the individual to provide emergency child care services.
6. How individuals can obtain further information, including any fact sheets or brochures, or a copy of the Code.

Principle 9 – Individual Access

Upon request, a member/family, MFRC staff or third party shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, the MFRC may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that contains references to other individuals, information that cannot be disclosed for legal or security reasons, and information that is subject to solicitor-client or litigation privilege. Where such information can be severed from a file, MFRCs shall do so to provide as much access to personal information as possible.

- 9.1** Upon request, the MFRC shall inform an individual whether or not the MFRC holds personal information about the individual. Wherever possible, MFRCs must provide the source of this information. The MFRC shall allow the individual access to this information. In addition, the MFRC shall provide an account of the use that has been made or is being made of this information and an account of any third parties to which it may have been disclosed.
- 9.2** An individual may be required to provide sufficient information to permit the MFRC to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.
- 9.3** In providing an account of third parties to which it has disclosed personal information about an individual, the MFRC should attempt to be as specific as possible. When it is not possible to provide a list of the third parties to which it has actually disclosed information about an individual, the MFRC shall provide a list of third parties to which it may have disclosed information about the individual.

Notes to Principle 9

Principle 9 requires that individuals be provided with access to their personal information upon request and in reasonable circumstances, such as normal office hours.

Except in circumstances described below, individuals must be able to review all of their personal information, regardless of the format, and be able to understand how it is used or disclosed. Personal information should, therefore, be maintained in such a manner that it can be easily assembled for the individual to review (avoid scattered databases wherever possible). This may require creating a master database that specifies where other personal information about an individual can be found, for example, that an application form is contained in a file for a specific service.

Where access is provided to personal information, the source of the information must be noted wherever possible.

The individual has a right to challenge the accuracy and completeness of any personal information made available to them and have it amended as appropriate. In most cases, this will not be an issue. The personal information held by MFRCs about members/families will be generally supplied by the member/family and accordingly there should be little dispute about its source or accuracy. This may not be the case for MFRC staff and/or third party service providers. Where there are disputes about the accuracy of personal information held about an individual, the MFRC must record the nature of the dispute in the file.

The MFRC must also tell the individual how the information is used or to whom it is disclosed and for what purposes. The notes to Principle 2 – *Identifying Purposes* provide some guidelines on creating a purposes checklist to simplify this explanation process (see in particular the TIP on page 15).

The note in principle 9 describes situations where personal information either can be or should be withheld from an individual. These circumstances should be as limited as possible and, wherever possible, information that is being withheld must be separated from information that can be disclosed in order to allow the greatest possible access to personal information. It is essential however that, when providing access to personal information, the privacy, safety or security of another individual is not compromised.

If the Director of an MFRC is in doubt about providing access to personal information to a specific individual, the Director must consult the Chair of the Board of Directors of the MFRC who shall consult, in turn with DMFS.

In providing access to any personal information, the MFRC must take appropriate measures to ensure the information is only provided to individuals who are entitled access. MFRCs can request identification from the individual or ask for authorization where a third party is seeking access to the information. The information provided to establish the identity of the individual or authorize access must only be used for this purpose.

Principle 9 – Individual Access (continued)

- 9.4** The MFRC shall respond to an individual's request within a maximum period of 30 days and at no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the MFRC uses abbreviations or codes to record information, an explanation shall be provided.
- 9.5** When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the MFRC shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.
- 9.6** When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the MFRC. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question. When appropriate, relevant details about the unresolved challenge shall be transmitted to DMFS.

Notes to Principle 9 (continued)

In cases where an individual has identified harmful consequences resulting from the reliance of inaccurate or incomplete information or improper use or disclosure of personal information, the Director shall consult at the earliest possible opportunity with the Chairperson of the Board of Directors of the MFRC who shall consult, in turn with DMFS.

MFRCs should never disclose personal information over the phone unless the identity of the individual and their right of access are clearly established, or in an insecure manner, for example, use of a fax machine where the recipient has not been alerted to the fax transmission.

Clause 9.4 specifies that a request to access personal information be responded to within a maximum timeframe of 30 days and at no cost to the individual. The Director shall put procedures in place to respond to all access requests. These procedures shall include the following.

1. Ensure that members and their families as well as MFRC staff and third parties are aware of their right to request access to their personal information and ensure MFRCs communicate this right to members and their families, staff and third parties.
2. Create a form to record and track access requests. This form should include the date of the access request, the name and contact information of the person filing the access request, any information required to establish the individual's right of access to the personal information, the substance of the access request, the date that the personal information was provided to the individual and any subsequent follow-up required.
3. Amend, correct, delete or add any personal information where the individual successfully demonstrates its inaccuracy or incompleteness and where appropriate to transmit amended information to third parties who have access to the information in question. This should only occur where the third parties, in the view of the Director, require the updated information for a specific purpose consented to by the individual.
4. When there is a dispute for any reason about amending personal information, the nature of the dispute must be recorded on the access request form that shall be appended to the individual's file. The nature of the dispute shall also be transmitted to third parties where, in the view of the Director, it meets the criteria used in point 3 above.
5. Upon request by an employee or volunteer, MFRCs must provide access to their personal information, but can withhold any information pertaining to the investigation of a breach of an employment contract or a contravention of a law, where the information is protected by solicitor-client privilege, or where providing the information might threaten the life or security of another individual.

This page intentionally left blank.

Notes to Principle 9 (continued)

6. MFRCs must sever non-disclosable information, wherever possible from other information within a file, to provide the greatest possible access to personal information.

Note: If an individual asked for access to all of the personal information concerning them that the MFRC had in its files, the MFRC must first review the file to remove or de-personalize only the information that they have a legitimate right to withhold (see note under Principle 9 and commentary on page 35), including personal information about any other individual where the person has no right of access. However, in an emergency situation where the time and effort required to review the file would unduly delay the response to the emergency, this step can be omitted at the discretion of the MFRC Director. In such situations, where any third party personal information has been accessed by an individual, the MFRC should inform the third party about the circumstances of the disclosure at the earliest possible opportunity.

7. Where an MFRC has sensitive medical information about an individual, the MFRC must make this information available through a medical practitioner, unless the medical information was directly provided by the individual or a family member.

Note: Where medical information has been provided directly by the individual or a family member, for example, listing a child's allergies on a form to participate in an event or activity, or providing a copy of a medical claim or prescription form obtained from a medical practitioner, the above requirement would not apply. Medical information that must be made available only through a medical practitioner includes any information provided to the MFRC directly by a medical practitioner or other source concerning an individual's physical or mental health. It is always preferable that such information be properly interpreted to the individual by a qualified medical practitioner.

8. Information collected or used by the Director of the MFRC for staff development purposes, including compensation planning, succession planning, the consideration of an employee for promotion, training or educational programs, is not considered to be the personal information of the individual for the purposes of this Code. This information may be withheld from or disclosed to the individual at the discretion of the Director.

Note: To prevent undue influence in decision-making processes, the Director and managers can withhold personal information created or used for such purposes. This could include, the names of employees under consideration for salary increases or promotions, or information related to a planned hiring or dismissal. All staffing decisions should be supported with objective and factual data to promote fairness and transparency. Once the decision has been made to hire, promote or dismiss an employee, the employee has the right to access any personal information that may have been used to make the decision.

Principle 10 – Challenging Compliance

A member/family, MFRC staff or third party shall be able to address a challenge concerning compliance with the above principles to the Director of an MFRC who is accountable for the MFRC's compliance.

- 10.1** MFRCs shall put mechanisms in place to receive and respond to complaints or inquiries about personal information policies and procedures under this Code. The complaint mechanisms shall be easily accessible and simple to use.
- 10.2** The Director of the MFRC shall investigate all complaints. If a complaint is found to be justified, the Director shall take appropriate measures, including, if necessary, amending procedures. The Director shall consult with DMFS on issues involving the interpretation of this Code and an MFRC's compliance with the Code.
- 10.3** A complaint that is not handled by the Director of the MFRC to the satisfaction of the individual may be referred by the individual to the Chair of the Board of Directors of the MFRC who shall consult, in turn with DMFS. MFRCs shall also inform individuals of the existence of any other applicable complaint resolution processes.
- 10.4** As part of the oversight role, DMFS will conduct oversight visits and cyclical compliance audits.

Notes to Principle 10

Principle 10 allows an individual whose information is held by the MFRC (member/family, MFRC staff or third party) to challenge how the MFRC adheres to this Code. An individual can challenge any denial of access to personal information or refusal to amend information under Principle 9, and can challenge any perceived lack of compliance with any of the principles of this Code.

The Director shall put mechanisms in place to respond to all complaints. These mechanisms shall include the following.

1. Ensure that members and their families as well as MFRC staff and third parties are aware of their right to address complaints to the Director and ensure that staff communicate this information to members and their families, as required.
2. Create a form to record complaints. This form should include the name and contact information of the person filing the complaint, the date and nature of the complaint, and when the investigation is complete, how the complaint was eventually resolved; including any measures taken to change administrative practices, if necessary.
3. When a complaint is received, an acknowledgement within five working days by the Director to the individual that the complaint is being investigated.
4. A further response to the individual within 30 days of receiving the complaint detailing the results of the complaint investigation and any actions taken to resolve the complaint, to include amending administrative practices, if necessary.
5. The Director shall notify an individual if a response to a complaint will take longer than 30 days and explain the reasons why; include any delays as a result of points 6 and 7 below.
6. In cases where an individual has identified harmful consequences resulting from the improper use or disclosure of personal information or where a complaint has not been handled by the MFRC to the satisfaction of the individual, the Director shall consult at the earliest possible opportunity with the Chair of the Board of Directors of the MFRC who shall consult, in turn with DMFS.
7. In cases where a complaint concerns the principles of the Code itself or MFRC compliance with the Code or Application Guide, the Director shall consult at the earliest possible opportunity with the Chair of the Board of Directors of the MFRC who shall consult, in turn with DMFS.
8. Where a complaint is not handled to the satisfaction of the individual, the Director shall also inform the individual of any alternate complaint resolution processes. These processes may include the right to file a complaint under any existing provincial laws such as Québec's *Act respecting the protection of personal information in the private sector*.

Appendix: Agreement for third party data processing

AGREEMENT TO SAFEGUARD PERSONAL INFORMATION

THIS AGREEMENT, made (date), between:

Name of MFRC
Address
("The MFRC")

-and-

Name of company or individual
Address
("The Recipient")

RECITES THAT:

- a. On and subject to the terms and conditions of this Agreement, the MFRC intends to disclose certain Personal Information to the Recipient for purposes of the Activity whose terms are defined in this Agreement.

THEREFORE, in return for the promises and mutual agreements contained in this Agreement and other good and valuable consideration (the receipt and sufficiency of which is acknowledged by each of the Parties), the Parties agree as follows:

1. **DEFINITIONS.** In this Agreement, unless the context otherwise requires:

"Activity" means (define the activity);

"Agreement" means this Agreement to Safeguard Personal Information and any document signed by the Parties amending this Agreement;

"Personal Information" means any information about an identifiable individual provided by the MFRC to the Recipient for the purposes of the Activity defined within this Agreement;

"Processing" means any manual or automated form of collection, use, transmission, disclosure, storage, reproduction, manipulation, modification, or access to the Personal Information defined within this Agreement;

"Safeguards" means any method or combination of methods that have been agreed to between the Parties to protect the Personal Information from loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

2. SAFEGUARDS TO BE APPLIED

The Recipient acknowledges and confirms that the Personal Information is being disclosed to the Recipient for the purposes of the Activity only. Accordingly the Recipient agrees:

- (1) to protect the Personal Information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification;
- (2) to use the Personal Information for the purposes of the Activity only;
- (3) not to use the Personal Information for its own benefit or the benefit of third parties;
- (4) upon request of the MFRC, cease any and all use of the Personal Information and return the Personal Information to the MFRC or destroy the Personal Information in a manner agreed to by the MFRC;
- (5) upon reasonable notice, to permit site visits by the MFRC to examine the measures taken by the Recipient to protect the Personal Information;
- (6) not to disclose the Personal Information to any person other than an employee of the Recipient, and only then on a need-to-know basis.

3. BEGINNING AND EXPIRY OF THE RECIPIENT'S OBLIGATIONS

The Recipient's obligations under this Agreement take effect as of the date of this Agreement and survive until (number) years from that date, the completion of the Activity, or the MFRC's request for a return of the Personal Information, whichever comes last.

4. INDEMNITY

The Recipient indemnifies and holds the MFRC harmless from and against any and all loss, liability, damage, claim, cost, and expense (including legal fees) however arising, out of any breach or non-performance by the Recipient or its Representatives of any of the Recipient's obligations under this Agreement including, without limitation, the Recipient's obligations regarding the use of the Personal Information.

5. INJUNCTION

The Recipient acknowledges that a breach by it or any of its Representatives of any of the Recipient's obligations under this Agreement may cause irreparable harm to the MFRC which may be difficult or impossible to ascertain, and that an award of damages will not be a sufficient remedy for such breach. Accordingly, the MFRC will be entitled to specific performance of this Agreement and an injunction to prevent any breach or threatened breach of this Agreement. No remedy referred to in this section is exclusive but each is cumulative and in addition to any other remedy otherwise available at law or in equity, including damages.

6. GENERAL

- 6.1 Nothing in this Agreement is to be interpreted to:
- (i) obligate the MFRC to enter into any further agreement with the Recipient; or
 - (ii) grant to the Recipient any right, title, or interest in the Personal Information, or in the MFRC's operations.
- 6.2 The MFRC makes no representation or warranty, explicit or implicit, regarding the Personal Information or its fitness for a particular use or purpose.
- 6.3 Any communication under this Agreement is deemed to have been properly made when, in the ordinary course of delivery or transmission, it is sent to a Party at its address above or other address as a Party advises, in writing.
- 6.4 Notwithstanding any dispute arising between the Parties, the Recipient must proceed diligently with the performance of this Agreement.
- 6.5 No delay or failure of a Party to exercise any of its rights under this Agreement operates as a waiver of such right or affects any other of that Party's rights or the exercise of those rights.
- 6.6 This Agreement benefits and is binding on the Parties and their respective heirs, executors, administrators, successors, and permitted assigns, as the case may be.
- 6.7 This Agreement is governed by and must be construed in accordance with the laws of the province of (Province), and the laws of Canada as applicable in that province, and the Parties irrevocably submit to the nonexclusive jurisdiction of the courts of (Province) for the interpretation and enforcement of this Agreement.
- 6.8 If any term of this Agreement is held to be invalid, illegal, or unenforceable, it will not affect the validity of any other terms of this Agreement and this Agreement will be read as though the invalid term does not exist.
- 6.9 The Recipient agrees not to assign this Agreement or any of its rights, obligations, or interests under this Agreement without the prior written consent of the MFRC. Notwithstanding such consent, no assignment relieves the Recipient of any of its obligations under this Agreement.
- 6.10 This Agreement expresses the final Agreement between the Parties as to the subject matter of this Agreement. Accordingly, the Parties agree not to amend this Agreement except by and in accordance with a document signed by the Parties which document is styled solely as an amendment to this Agreement.

EACH OF THE PARTIES have executed this Agreement and in so doing confirm their authority and intention to bind the Party they represent.

THE MFRC (Name of MFRC)

By: _____

Name: _____

Title: _____

THE RECIPIENT (Name of Company)

By: _____

Name: _____

Title: _____