

**Privacy Code for
Military Family Services Program**

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 who 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 *Canadian Standards Association 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
1600 Star Top Road
Ottawa ON
K1A 0K2

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 operations, 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. This information is provided by the CF 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.

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.

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 (see appendix to Application Code for sample) 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.

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*).
- 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.

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; any information can be considered sensitive, depending on the context.
- 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. Consent can also be given by an authorized representative such as a legal guardian or a person having power of attorney.

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.

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.

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.

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.

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).

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.

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.

- 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.

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.