THE AGENCY FOR CO-OPERATIVE HOUSING

POLICY MANUAL

DATE ISSUED:
November 2018

NUMBER:
2.5

REPLACING ISSUE OF:
March 2016

CROSS REFERENCE:
2.3.1: Communications, 2.4: Confidentiality and Access to Information, 3.1.1: Human Resources, 3.4 Records Management, 3.6 Information Security

REVIEW CYCLE:
3 Years

AUTHORITY:
Board of Directors

DUE FOR NEXT REVIEW:
March 2022

SUBJECT:
Privacy

---

1. Introduction

1.1 The Agency has adopted this policy out of respect for the privacy of individuals and to comply with the law.

1.2 The federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") regulates the collection, storage, use and disclosure of the personal information any non-governmental organization gathers in carrying out a commercial activity. In provinces that have adopted privacy laws that the federal government has deemed at least equal in the protection they afford to personal privacy that legislation governs in place of PIPEDA. Such laws currently exist in two provinces where the Agency is active: Alberta and British Columbia. In other provinces, the Agency is governed by PIPEDA.

1.3 PIPEDA defines personal information as "information about identifiable individuals, other than their names and titles, business addresses, e-mail addresses and listed phone numbers." It sets out principles for the protection of such information. These are summarized in Appendix A. PIPEDA and this policy do not apply to individuals' business-contact information where the information is collected, used or disclosed solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession.

1.4 The federal *Privacy Act* (the "federal act") protects the privacy of information the federal government holds about individuals and gives people a right of access to information about themselves. Information the Agency acquires or creates and uses in the course of providing services to Canada Mortgage and Housing Corporation

belongs to CMHC ("CMHC Information") and, as applicable, to any individual who provided the information about themselves. The Agency must respect CMHC's obligations under the federal act with regard to that information. The key provisions of the federal act are summarized in Appendix B.

1.5 For the purposes of this policy, CMHC Information does not include information about the Agency's personnel.

1.6 This policy complements the Confidentiality and Access to Information Policy, which applies to information the Agency holds about organizations.

2. Application of this Policy

2.1 Directors, employees, independent contractors acting in the Agency's name, and any other persons acting on the Agency's behalf, must all follow this policy. If unsure about the requirements of the Agency's methods for managing personal information, they may consult the Privacy Officer.

2.2 Through the agreements it enters into with them, the Agency requires independent contractors to comply with this policy.

3. Restrictions on Collection, Use and Sharing of Personal Information

3.1 The Agency may collect, use or disclose personal information produced by an individual about themselves in the course of their employment, business or profession without their consent, where doing so is consistent with the purposes for which the information was produced.

3.2 The Agency and its representatives may request only the limited personal information needed to deliver high-quality services, manage the organization effectively and fulfil the Agency's obligations to its co-operative and government clients, business associates and employees. Any personal information collected may be used only for the purpose for which it was gathered, unless an individual gives specific permission for another use or unless otherwise permitted by law.

3.3 Subject to Article 6, the Agency may only request personal information when three conditions are met:

- the information is needed for an identified purpose;
- that purpose has been explained to the person from whom the information is sought;
- the person has agreed in advance to the collection of information for that purpose and understands that they may withdraw their consent at any time.

3.4 The Agency will proceed as follows when it acquires personal information that it did not request:

- Where the Agency does not need the information to deliver its services, it will return it to the provider and destroy any copies it may hold, as required under Article 8.
- Where the information is required to deliver services, the Agency will
  - use it only for the purpose for which the provider made it available;
  - store it in accordance with this policy;
  - dispose of it as soon as practicable in accordance with this policy and the Records Management Policy.

4. Storage of Personal Information

The Agency must store personal information securely so as to prevent its unauthorized use.

5. Access to Personal Information

5.1 Subject to Article 6, access to personal information that the Agency holds about an individual will be restricted to that individual, persons who need the information for the purpose for which it was gathered or received, including, as appropriate, CMHC, and, as necessary, the Privacy Officer.

5.2 The Agency will direct all requests from individuals for access to information about themselves to CMHC, where that information belongs to CMHC under Article 1.

5.3 The Client Service Champion will log all such requests.

6. Exceptions to Requirement for Consent for Agency Disclosure

6.1 Disclosure in an Emergency

6.1.1 Subject to paragraph 6.1.2, the Agency may share personal information about an individual if the information is used to take action during an emergency that threatens the life, health or security of any individual.

6.1.2 The Agency will make diligent efforts to obtain CMHC's advance permission before disclosing any CMHC Information under paragraph 6.1.1 except where doing so would place the life, health or security of any individual at further risk.

6.2 Disclosure to Law-Enforcement Authorities

6.2.1 Subject to paragraph 6.2.2, the Agency may disclose personal information to an investigative body for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation.

6.2.2 The Agency will make diligent efforts to obtain CMHC's advance permission before disclosing any CMHC Information under paragraph 6.2.1.

6.3 Reporting

Any disclosure of information under paragraph 6.1 or 6.2 must be reported to the Privacy Officer and to the Chief Executive Officer, who will inform the Board of Directors.

7. Material Breaches of Personal Information

7.1 On the occurrence of any Material Breach, as defined in Appendix C, the Agency will

- report the Breach to the Office of the Privacy Commissioner;
- notify all individuals whose privacy was breached;
- notify any other organization or government institution the Agency believes may be able to reduce the risk of harm or mitigate the injury caused by the Breach.

7.2 The consent of individuals is not required for such disclosures.

7.3 The Agency will inform CMHC without delay of any Material Breach involving CMHC Information.

7.4 Reporting of Material Breaches will follow the procedure set out in Appendix C.

8. Retention of Personal Information

8.1 Notwithstanding the provisions of the Records Management Policy, the Agency will keep personal information under Article 1 no longer than is needed to achieve the purpose for which it was collected. Where personal information contributes to the making of a decision the Agency may need to review or explain, the Agency will keep the information as long as a review or explanation would be meaningful.

9. Destruction of Personal Information

9.1 While the absolute destruction of electronic data is difficult to achieve, the Agency will make every reasonable effort to eliminate all redundant personal information from its files.

9.2 Reasonable efforts include

- deleting an e-mail that contains personal information from both inbox and deleted items folders;
- shredding any paper document containing unneeded personal information or, if the document also contains useful information and the original will not be needed, redacting the personal information from the document.

9.3 Any personal information remaining in the Agency's possession that is also CMHC information under Article 1 will be transferred to CMHC with the records containing it as may be required under the Agency's agreement with CMHC.

10. Privacy Officer

10.1 The Client Service Champion will serve as Privacy Officer for the Agency. The Privacy Officer is responsible for the Agency's compliance with this policy and PIPEDA or any provincial legislation that supersedes PIPEDA, and will ensure that the Agency meets its obligations to CMHC with respect to the federal *Privacy Act*.

10.2 The Privacy Officer will advise any of the Agency's directors, staff and independent contractors who ask for guidance in complying with this policy and with the privacy laws that, either directly or through agreements with government clients, govern the Agency. The Privacy Officer will consult with CMHC's Privacy Officer as necessary before providing advice on the requirements of the federal act.

10.3 The Privacy Officer will respond to any inquiries or complaints about the way the Agency collects, uses or shares personal information, forwarding to CMHC those that fall under the federal act within one business day of receipt, and investigating the others.

10.4 The Agency will publish the Privacy Officer's contact information on its website.

11. Publication of this Policy

11.1 The Agency will publish this policy on its website, and, on request, will provide an explanation of what personal information the Agency collects, how and by whom it is used and how an individual can arrange to see any personal information the Agency holds about them.

11.2 Should an individual point out any errors in the personal information the Agency holds about them, the Agency will correct the error, if possible.

12. Misuse of Information and Complaints

12.1 Any individual dissatisfied with the Agency's handling of their personal information may make a formal complaint to the Agency's Privacy Officer, who will investigate and try to resolve the complaint, or, as appropriate, redirect it to CMHC. If the complainant remains dissatisfied, they may communicate in writing with the Agency's Board of Directors.

12.2 The Privacy Officer will document any misuse of personal information and report it to the Chief Executive Officer and, if the information concerned is CMHC Information, to CMHC. The CEO will report all misuses of personal information to the Board of Directors.

13. Education

The Agency will ensure that, once a year, Agency employees are reminded of this policy, its underlying principles and aims, and any associated procedures.

Appendix A: Principles for the Protection of Privacy

Schedule 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) sets out a code for the protection of personal information.

The code was developed by business, consumers, academics and government under the auspices of the Canadian Standards Association. It lists 10 principles of fair information practices, which form ground rules for the collection, use and disclosure of personal information. These principles give individuals control over how their personal information is handled in the private sector.

An organization is responsible for the protection of personal information and the fair handling of it at all times, throughout the organization and in dealings with third parties. Care in collecting, using and disclosing personal information is essential to continued consumer confidence and good will.

The 10 principles follow:

1. **Accountability** – An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following points.

2. **Identifying Purposes** – The purposes for which personal information is collected will be identified by the organization at or before the time the information is collected.

3. **Consent –** The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate. 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. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4. **Limiting Collection** – The collection of personal information will be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure and Retention** – Personal information will 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 must be retained only as long as necessary for the fulfilment of those purposes.

6. **Accuracy –** Personal information will be accurate, complete, and as up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards** – Personal information will be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness** – The organization will make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. **Individual Access** – Upon request, an individual will be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate. In certain situations, an organization 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 is prohibitively costly to provide, information that contains references to other individuals, and information that is subject to solicitor-client or litigation privilege.

10. **Challenging Compliance** – An individual will be able to address a challenge concerning compliance with the above principles to the Privacy Officer, the designated individual accountable for the organization's compliance.

A full explanation of these 10 principles can be found in the PIPEDA Fair Information Principles in the PIPEDA guide for businesses.

Appendix B: Privacy Act Principles and Definitions

The *Privacy Act* protects the privacy of individuals with respect to personal information about themselves held by a government institution and provides individuals with a right of access to that information.

General Principles

1. Individuals have a right of access to personal information about them held in government records.

2. The collection and use of personal information is only permitted in accordance with the *Privacy Act*.

3. Information on individuals must be accurate and appropriately protected.

Collection, Retention and Disposal of Personal Information

- No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.
- All personal information, wherever possible, shall be collected directly from the individual to whom it relates.
- Government institutions shall inform any individual of the purpose for which the information is being collected.
- Personal information that has been used by a government institution for an administrative purpose shall be retained for a period of two (2) years following the last administrative action in order to ensure that the individual has a reasonable opportunity to obtain access to the information.
- A government institution shall dispose of personal information in accordance with the regulations and guidelines issued by the designated minister.

Definition of Personal Information

Personal information is information about an identifiable individual that is recorded in any form, including, without restricting the generality of the foregoing,

- information relating to race, origin, colour, religion, age or marital status, education, medical, criminal or employment history or an individual's financial information;
- any identifying number or symbol, or other particular assigned to the individual (e.g., SIN number);
- address, fingerprints or blood type;

- personal opinions or views of the individual, except where they are about another individual (e.g., performance reviews);
- correspondence of a private or confidential nature with a government institution.

Non-personal Information

Personal information as defined in the *Privacy Act* and *Access to Information Act* does not include

- information about an individual who is an officer of a government institution;
- information that relates to the position or functions of the individual including the fact that the individual is a government employee;
- title, business address and telephone number;
- classification, salary range and responsibilities of the position;
- name of the individual on a document prepared in the course of employment.

Appendix C: Managing Material Breaches of Personal Information

The *Digital Privacy Act* received royal assent in June 2015. The Act amended PIPEDA to add mandatory reporting obligations for material breaches of personal information. The obligation came into force on 1 November 2018.

Definition of Material Breach of Personal Information

A Material Breach of personal information occurs when

- unauthorized access to, or unauthorized disclosure of, sensitive personal information under the Agency's control takes place; and
- it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

Sensitive personal information includes, but is not limited to, the following:

- medical, psychiatric or psychological information;
- information compiled and identifiable as part of an investigation into a possible violation of law;
- criminal history;
- information on the eligibility for social benefits or the determination of benefit levels;
- information describing an individual's finances (income, assets, liabilities, net worth, bank balances, tax returns, financial history or activities, or creditworthiness);
- information containing personal recommendations or evaluations, personal opinions about a sensitive subject, character references, or personnel evaluations;
- information concerning an individual's racial or ethnic origin or religious or political beliefs and associations or lifestyle; and
- certain tombstone information, including birthdate and Social Insurance Number.

Significant harm to the individual includes the following:

- identity theft or some other related fraud;
- material financial loss to the individual, including loss of employment, business or professional opportunities, damage to or loss of property or negative effects on the individual's credit record; and
- bodily harm, humiliation or damage to reputation or relationships.

Reporting to the Office of the Privacy Commissioner

The Agency will determine whether or not a Material Breach of personal information has occurred by conducting a risk assessment.

- The report of a Material Breach of personal information to the Commissioner will be in writing and will include the following: a description of the circumstances of the breach and, if known, the cause;
- the day on which, or the period during which, the breach occurred or, if neither is known, the approximate date or period;
- a description, to the extent known, of the personal information that is the subject of the breach;
- the number of individuals affected by the breach or, if unknown, the approximate number;
- a description of the steps that the Agency has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;
- a description of the steps that the Agency has taken or intends to take to notify affected individuals of the breach; and
- the name and contact information of a person who can answer the commissioner's questions about the breach.

The Agency will provide the Commissioner with any new information that it becomes aware of after having made the report.

The report will be sent by any secure means of communication.

Notification to Affected Individuals

The notification to an individual that a Material Breach of their personal information has occurred will include the following:

- a description of the circumstances of the breach;
- the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
- a description of the personal information that is the subject of the breach to the extent that the information is known;
- a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;
- a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and

- contact information that the affected individual can use to obtain further information about the breach.

The notification will be given in person, by telephone, mail, e-mail or any other form of communication that a reasonable person would consider appropriate in the circumstances. An indirect notification, such as public communication, will be given in any of the following circumstances:

- Direct notification would be likely to cause further harm to the affected individual.
- Direct notification would be likely to cause undue hardship for the Agency (for example, if required to notify a large number of customers of a data breach).
- The Agency does not have contact information for the affected individual or individuals.

Recordkeeping

The Agency will keep a record of every Material Breach of personal information for 24 months after the day on which it has concluded that the breach has occurred. The Agency will provide any record that is less than 24 months old to the Commissioner upon request.