FirstOntario
CREDIT UNION

# Privacy Policy

Policy for the Protection of Personal Information

**Table of Contents**

**Commitment**

**Compliance**

- Principle 1 – Accountability
- Principle 2 – Identifying Purpose
- Principle 3 – Consent
- Principle 4 – Limiting Collection
- Principle 5 – Limiting Use, Disclosure and Retention
- Principle 6 – Accuracy
- Principle 7 – Safeguards
- Principle 8 – Openness
- Principle 9 – Individual Access
- Principle 10 – Challenging Compliance

Audit & Risk Committee
Reviewed February 2018
Amended February 2018

FirstOntario
CREDIT UNION

# Privacy Policy

**Commitment**

FirstOntario Credit Union is committed to protecting the confidentiality and privacy of the personal information of all members and other individuals whose personal information is held or controlled by the Credit Union.

**Compliance with Privacy Legislation**

In developing this policy FirstOntario Credit Union Limited has adopted Credit Union Central of Canada's Code for the Protection of Personal Information (the "Code") which is based on the principles set out in Schedule 1 of the Personal Information Protection and Electronic Documents Act (PIPEDA).

The Policy is based on the following ten interrelated privacy principles

1. Accountability- The Credit Union is responsible for personal information under its control and shall designate a Privacy Officer who is accountable for the Credit Union's compliance with the principles of the Policy.
2. Identifying Purposes – The purposes for which personal information is collected shall be identified by the Credit Union at or before the time the information is collected.
3. Consent – The knowledge and consent of the member are required for the collection, use and disclosure of personal information, except in specific circumstances as described within this Policy.
4. Limiting Collection – The collection of personal information shall be limited to that which is necessary for the purposes identified by the Credit Union. Information shall be collected by fair and lawful means.
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 member or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
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.
7. Safeguard – Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. The Credit Union will apply the same standard of care as it applies to safeguard its own confidential information of a similar nature.
8. Openness – The Credit Union shall make readily available to members specific, understandable information about its policies and practices relating to the management of personal information.

Audit & Risk Committee
Reviewed February 2018
Amended February 2018

9. Individual Access – Upon request, a member shall be informed of the existence, use, and disclosure of their personal information, and shall be given access to that information. A member is entitled to question the accuracy and completeness of the information and have it amended as appropriate.
10. Challenging Compliance – A member shall be able to direct questions related to compliance with the above principles to the Privacy Officer accountable for the Credit Union's compliance. The Credit Union shall have policies and procedures to respond to the member's questions and concerns.

**Principle 1 – Accountability**

**Privacy Officer and Deputy Privacy Officer**

FirstOntario's Board of Directors is responsible for the Credit Union's compliance with Privacy Legislation and the review and approval of Privacy Policies. The Board, in consultation with the CEO, is also responsible for the designation of the Privacy Officer and Deputy Privacy Officer, who have primary responsibility for compliance with the Policy. The Credit Union will notify all employees, the Credit Union's members and any affected third parties of the appointment by publishing the identity of this individual on FirstOntario Credit Union's external website as well as its intranet.

The Privacy Officer appointed by the Board of Directors must be a senior manager within the Credit Union who does not have a potential conflict of interests over any aspects of personal information protection. In order to avoid a potential conflict responsibility, the Privacy Officer and Deputy Privacy Officer would preferably not be the designated Compliance Officer under the federal regulations for the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, or other similar regulations where a conflict might exist.

The Deputy Privacy Officer will be available in the event of absences by the Privacy Officer and will have identical decision-making responsibilities during those absences.

Other individuals within the Credit Union, as delegated by the Privacy Officer, may be accountable for the day-to-day collection and processing of personal information, or to act on behalf of the Privacy Officer. It will be the responsibility of the Privacy Officer to ensure these employees are adequately trained in order to understand and follow all Privacy policies and procedures.

**Policies and Procedures**

The Privacy Officer shall implement policies and procedures to give effect to the Privacy principles including:

- Implementing procedures to protect information
- Establishing procedures to receive and respond to complaints and inquiries
- Training staff and communicating to staff information about the organization's policies and procedures and
- Developing information to explain the organization's policies and procedures

**Third Party Accountability**

The Credit Union is considered to have control of any personal information that has been collected by, is in the custody or possession of, and/or is used within the credit union, including information that has been transferred to a Third Party for processing purposes.

The Privacy Officer is responsible to ensure that the Credit Union will use contractual or other means to provide a comparable level of protection while the information is being processed by a Third Party.

**Board Reporting and Notification**

The Privacy Officer will continually review the Policy and its compliance within the Credit Union and will report to the Board of Directors and Senior Management any matters concerning non-compliance with Privacy principles, polices or procedures. The Privacy Officer will prepare a quarterly report for the Board of Directors that identifies any known contraventions of privacy laws by the Credit Union, including privacy breaches, and recommended changes for the Board's consideration. The report will also include an overview of the number of inquiries received by the Privacy Officer, number of requests for access to, or correction of, personal information, and details regarding individuals' challenges to the Credit Union's compliance with these Privacy Policies.

The Board of Directors will review each quarterly report to determine whether additional steps, beyond those taken by the Privacy Officer, are required.

The Privacy Officer will review this policy annually to ensure continued compliance with the Code and to recommend to the Board of Directors any revisions as deemed appropriate.

Internal Audit Services will include periodic audits of FirstOntario Privacy practices and procedures in their annual audit planning process.

**Principle 2- Identifying Purposes Approval and Documentation of Purposes**

The purposes for which personal information is collected and used shall be documented and identified by the credit union at or before the time the information is collected, including any disclosure of the information to third parties.

Information collected must be limited to that necessary for the purpose identified. The primary communication method will be the use of written or electronic statements on applications, forms, contracts and agreements. 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. The Privacy Officer is to be informed of any new purpose for the collection, use or disclosure of personal information, prior to the collection of personal information for the new purpose.

**Employee Disclosure**

The Credit Union will ensure that all employees are aware of the purposes for which employee information is collected, including any disclosure of their personal information to Third Parties. This will be communicated verbally at the time of employment as well as in writing, through the use of Employee Online Privacy Training programs.

**Principle 3 – Consent**

The express knowledge and consent of the Member will be required in all cases for the collection, use or disclosure of personal information, except in some specific circumstances described below:

- When information is being collected for the detection and prevention of fraud or for law enforcement
- In legal, medical or security reasons where it may be impossible or impractical to seek consent

The Credit Union will seek consent for the use or disclosure of this information at the time of collection. To make the consent meaningful the purpose will be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

Due to the highly sensitive nature of personal financial information, written consent primarily through the use of applications, signed forms and contracts, will be used for obtaining consent for the collection, use or disclosure of such personal information.

While consent is primarily written, in some cases the Credit Union may rely on express verbal consent provided that the employee collecting the personal information communicates the purpose for the collection of the personal information, as well as what the personal information will be used for and to which other parties the personal information will be disclosed. The employee will record the time and date on which consent was provided verbally.

Express consent is when the Member giving consent has clearly stated, whether in writing, verbally, or through electronic means, the acceptance of the terms contained in a request for consent. Express consent is contrasted with implied or deemed consent, which is consent that is inferred from an

individual's actions and the facts and circumstances of a particular situation.

The Privacy Officer must review and approve all methods of obtaining consent.

Once express consent is obtained from an individual, further consent will not be required when personal information is supplied to agents of the credit union who carry out functions such as data processing, credit bureaus, cheque printing and cheque processing because the individuals could reasonably expect that these parties would be given the information in order to deliver the services of the Credit Union.

The Privacy Officer, must review all instances that are brought to the Privacy Officer's attention where a Member's personal information is collected, used, and/or disclosed without the Members' knowledge and consent. The Privacy Officer can authorize further action following the review, such as to the removal, destruction or anonymization of the personal information in the possession of the Credit Union.

**Consent Limits on Information Collection**

The Credit Union will not, as a condition of the supply of a product or service, require a member to consent to the collection, use or disclosure of information beyond that required to fulfill explicitly specified and legitimate purposes.

Where consent to the collection, use or disclosure of additional, non-essential personal information for a product or service is sought from a Member, this will be identified as optional information, and collected, used or disclosed only with the express consent of the Member.

Refusal to provide this optional information will not influence the member's consideration for a product or service.

The Privacy Officer will review the personal information requirements of all products or services to ensure that only personal information required for the legitimate purpose is collected and used and/or disclosed.

**Withdrawing Consent**

The Credit Union will obtain a written request (signed and dated) from a member who seeks to withdraw consent. The written request must acknowledge that the member has been advised that the Credit Union may subsequently not be able to provide the member with a related product, service or information that could be of value to the member.

In addition, when an individual makes a request to withdraw consent, the employee processing the request will communicate the consequences of withdrawing consent to ensure that the individual can make an informed decision of whether or not to proceed.

The withdrawal of consent is subject to any legal or contractual restrictions that the Credit Union may have with the member or other organizations such as: the Income Tax Act; credit reporting; or to fulfill other fiduciary and legal responsibilities.

**Principle 4 –Limiting Collection**

The collection of personal information will be limited to that which is necessary for the purposes identified by the Credit Union. Information will be collected by fair and lawful means, and not by misleading or deceiving Members about the purpose for which information is being collected.

The Credit Union will not collect personal information indiscriminately. It will specify both the amount and the type of information collected, limited to that which is necessary to fulfill the purposes identified in accordance with this policy.

**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 express consent of the member or as required by law. The Credit Union shall protect the interests of its members by taking reasonable steps to ensure that:

a) Orders or demands comply with the laws under which they were issued;
b) Only the personal information that is legally required is disclosed and nothing more;
c) Information is only disclosed to persons authorized to receive it and
d) Personal information disclosed to Third Parties is strictly limited to programs endorsed by the Credit Union and is protected by the same standards of care as personal information held by the Credit Union

The Credit Union will make reasonable attempts to notify the member that an order has been received, if not contrary to the security of the Credit Union and if the law allows it. Notification may be by telephone, or by letter to the member's usual address.

**Retention and Destruction**

The Privacy Officer will ensure that guidelines and procedures with respect to the retention of personal information are maintained within the Credit Union. These guidelines will include minimum and maximum retention periods and will conform to any legislative requirements.

Subject to any legislative requirement to retain records, personal information that is no longer required to fulfill the identified purposes will be destroyed, erased, or made anonymous. The Privacy Officer will ensure that the Credit Union has guidelines and procedures to govern the destruction of personal information. These will include procedures to ensure that personal information supplied to third parties has been destroyed once it is no longer required for the purposes identified.

The Privacy Officer will ensure that personal information held on the Credit Union's behalf by third parties (e.g., date service providers) is kept accurate, complete, and current.

**Principle 6 – Accuracy**

The Privacy Officer will ensure that the Credit Union has guidelines and procedures to ensure that member and Credit Union employee data it collects or generates directly is as accurate, complete and up-to-date as is necessary to fulfill the purposes for which the information was collected. The Credit Union shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected and/or at the request of the individual.

The Privacy Officer will ensure that personal information held on the Credit Union's behalf by third parties (e.g., data service providers) is kept accurate, complete, and current.

**Principle 7 – Safeguards**

**Credit Union Safeguards**

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Credit Union security safeguards will protect personal information against loss or theft, as well as unauthorized access, use, copying, modification, disclosure or disposal. The Credit Union will protect personal information regardless of the format in which it is held.

The Privacy Officer will collaborate with third parties specializing in security safeguards, as required, to ensure the required level of protection. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information will be safeguarded by a higher level of protection. The methods of protection will include:

(a) Physical measures such as locked filing cabinets and restricted access to offices;
(b) Organizational measures such as security clearances and limiting access on a "need-to-know" basis; and
(c) Technological measures such as the use of passwords and encryption

The Credit Union will apply the same standard of care as it applies to safeguard its own confidential information of a similar nature.

The Privacy Officer will periodically remind employees, officers and directors of the importance of maintaining the security and confidentiality of personal information.

Employees, officers and directors are individually required to sign the Statement of Ethical Conduct annually, including commitment to keep member's personal information secure and strictly confidential.

**Third Party Agents/Suppliers Safeguards**

Third Party Agents or Suppliers will be required to safeguard personal information disclosed to them in a manner consistent with the Privacy Policy of the Credit Union. Examples include data processors, credit bureaus, cheque printers, and cheque processors.

The Credit Union will use contractual or other means to provide a comparable level of protection while the information is being held or processed by a third party.

The Credit Union will not enter into any commercial relationships with organizations that do not agree to abide by acceptable limitations on information uses and appropriate safeguards.

The Privacy Officer must be satisfied that the personal information is adequately safeguarded by the third party.

**Destruction of Personal Information Safeguards**

When personal information is no longer required for legal or business reasons, the Credit Union will dispose of or destroy personal information in a secure manner to prevent any unauthorized access. The Privacy Officer will periodically review the disposal and destruction methods used by Credit Union employees and will provide recommendations for improvement, if required.

**Principle 8 – Openness**

The Credit Union will provide the name and contact information of the Privacy Officer to the Member making an inquiry.

The Credit Union will make readily available to members specific, understandable information about its policies and practices relating to the management of personal information.

This can be accomplished through the use of brochures, information sheets, online Web information, etc., and must include the following information:

- The name or title and the address of the Privacy Officer who is accountable for the compliance with the Credit Union's policies and procedures and to whom complaints or inquiries can be directed;
- The means of gaining access to personal information held by the Credit Union;
- A description of the type of personal information held at the Credit Union, including a general account of its use;
- The Credit Union's Privacy policy and standards
- The types of personal information made available to related organizations such as subsidiaries or other suppliers of services.

The Privacy Officer will review the methods of dissemination, and the form in which the information is presented to ensure that it is easy to locate, understandable and accessible.

**Principle 9 – Individual Access**

**Granting Access**

Upon request, a member shall be informed of the existence, use and disclosure of their personal information to third parties, and shall be given access to that information. The Member making the Access to Information Request must provide adequate proof of his or her identity, and sufficient information to allow the Credit Union to locate the requested information. Routine account information requests (e.g., account statement) can be made orally or in writing. If necessary, the Credit Union will refer the request to the Privacy Officer. The Credit Union will charge its standard fee (s), in accordance with its standard fee schedule, for providing the information. The member must be informed of an estimate of costs prior to the commencement of the request.

When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the Credit Union shall provide a list of organizations to which it may have disclosed information about the individual. When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the Credit Union shall amend the information as required at no cost. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

The Credit Union shall respond to a member's request within 30 days. This timeframe can be expanded, only if required, and upon written notification to the members.

**Restricting Access**

The Credit Union will provide information under an Access to Information Request subject to the restrictions set out in this section and under Privacy Legislation.

In certain situations, the Credit Union may not be able to provide access to all the personal information it holds about a member. Exceptions to the access requirement will be limited and specific and include the following:

1. Providing access would reveal personal information about a Third Party who has not provided consent for the disclosure;
2. Information that cannot be disclosed for legal, security, or commercial proprietary reasons;
3. The information is subject to solicitor-client privilege or litigation privilege;

If the Credit Union refuses a request for access to personal information in whole or in part, the Credit Union's response to the Access to Information Request will provide the reasons for refusal and refer the individual to the Privacy Officer who can answer the Member's questions about the refusal. The Credit Union may refuse to confirm or deny the existence of personal information collected as part of an investigation.

The Privacy Officer must be made aware of any situations involving employees, members or other individuals that would result in legal restrictions on access.

**Principle 10 – Challenging Compliance**

Any individual, not just a member or a Credit Union employee, can address a challenge concerning the Credit Union's compliance with Privacy Legislation to the Privacy Officer. The Privacy Officer will create and maintain documented procedures to track and respond to a Credit Union member or employee's privacy-related inquiries or complaints.

These procedures must be readily accessible to Credit Union members and employees, and must be simple to use.

The Privacy Officer will acknowledge the inquiry or complaint as soon as reasonably possible, and provide an estimated time for a more detailed response, if required. In all cases, a response must be provided within 30 days. The Credit Union will accept inquiries verbally or in written form but complaints will be accepted in written form only. The Privacy Officer will investigate all complaints and if a complaint is found to be justified, the Privacy Officer is responsible to take appropriate measures to resolve the issue.