Contents

01 PROTECTION OF MEMBER INFORMATION AND PRIVACY POLICY

Protection of Personal Information

The following ten interrelated privacy principles are specified in the *Personal Information Protection and Electronic Documents Act*:

- 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 Code.
- 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.
- 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 Code.
- 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.
- 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 if necessary for the fulfilment of those purposes.
- 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.
- Safeguards – 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.
- 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.
- 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 on proof of inaccuracy.
- Challenging Compliance – A member shall be able to question 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.

Accountability

The Board of Directors ("Board") is accountable for Credit Union compliance with the Code, the creation and review of all policies specific to the Code and the designation of a Credit Union Privacy Officer.

Privacy Officer

The Board , in consultation with the CEO, will designate a Privacy Officer, who has primary day-to-day responsibility for compliance with the Code. The Board will notify all employees, and any affected third parties, in writing of the appointment.

The Privacy Officer will be from Senior Management preferably with no potential conflict of interest over any aspects of personal information protection such as marketing, sales, human resources, or any responsibility for technical safeguards.

To avoid a potential conflict of responsibility, the Privacy Officer would preferably not be the Chief Anti-Money Laundering Officer ("CAMLO") designated under the federal regulations for the Proceeds of Crime (Money Laundering) Terrorist Financing Act, or other similar regulations where a conflict might exist.

Board Reporting and Notification

Quarterly Reporting

The Privacy Officer will continually review compliance within the Credit Union and its third party suppliers and will report to the Board and Senior Management any matters concerning non-compliance with the Credit Union's Code principles, policies or procedures that are likely to require input from the Board (e.g., any matter that could result in an investigation or audit by the Office of the Privacy Commissioner).

The Privacy Officer will prepare a Quarterly Report for the Board that identifies key activities (e.g., a review of third-party contracts, training initiatives, review of policies and procedures) and recommended changes for Board consideration. The report should also include an overview of the number of enquiries, number of access requests, and details regarding challenges to compliance.

The Board will review the steps taken to address any deficiencies or weakness in compliance.

Annual Reporting

The Privacy Officer will prepare an annual review of the effectiveness of the board policies to ensure compliance with the Code and to recommend any revisions as deemed appropriate. This report is due within four months of the end of each fiscal year.

Identifying Purposes

Approval and Documentation of Purposes

The Privacy Officer will document all purposes, including existing and new purposes, for which personal information is collected, used, or disclosed. All new purposes must be approved by the Privacy Officer prior to collection of information for the new purpose.

If the proposed purpose is significantly different than existing purposes or involves a new disclosure to a third party, the proposed purpose must be approved by the Board prior to implementation.

Member Disclosure

The Credit Union will make reasonable efforts to ensure that members are aware of the purpose for which their personal information is collected, including any disclosure of their personal information to third parties. The primary communication method will be the use of written or electronic statements on applications, forms, contracts, and agreements.

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 and in writing at the commencement of employment.

Consent

Once member consent is obtained, further member 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.

The Credit Union's Privacy Officer must authorize all instances where a member's information is collected, used, or disclosed without the member's knowledge and consent.

Obtaining Consent

Express consent in writing, using applications, signed forms and contracts, will be used for obtaining consent for the collection, use or disclosure of personal information.

Implied consent will be used for marketing purposes or to disclose nominative information to an affiliated organization. Implied consent must never contravene the "Act".

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

Limits on Consent to 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 additional, non-essential information for a product or service is sought from members, this will be identified as *optional* information, and collected only at the discretion 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 information required for the legitimate purpose is collected and used.

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.

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.

Limiting Collection

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 these policies.

Limiting Use, Disclosure and Retention

Safeguard Standards

The Credit Union will protect the interests of its members by taking reasonable steps to ensure that:

- orders or demands comply with the laws under which they were issued
- only personal information that is legally required is disclosed
- casual requests for personal information are denied
- all information disclosed to third parties receives the same standards of care as within the Credit Union (see Protection of Member Information with Third Parties).

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. Notification may be by telephone, or by letter to the member's usual address.

Retention & Destruction of Personal Information

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. The Privacy Officer will ensure that the Credit Union has guidelines and procedures to govern the destruction of personal information. Refer to Financial Administration –Records Retention for procedures.

Accuracy

The Privacy Officer will ensure the Credit Union has guidelines and procedures to ensure member and employee data is as accurate, complete, and current as necessary. The Credit Union will not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

Safeguards

Credit Union Safeguards

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
- conduct regular reviews of organizational and employee practices related to the safeguarding of personal information
- 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 a Statement of Ethical Conduct annually. The statement must include a commitment to keep members' personal information secure and strictly confidential.

Destruction of Personal Information Safeguards

The Credit Union will dispose of/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.

Openness

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

This information will include the following:

- name or title and address of the Privacy Officer 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
- types of personal information made available to related organizations such as subsidiaries or third-party 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.

Individual Access

All requests for access to personal information must be submitted in writing to the Privacy Officer and include adequate proof of the individual's identity/right to access, and sufficient information to allow the Credit Union to locate the requested information.

Restricting Access

Exceptions to the access requirement will be limited and specific and include the following:

- providing access would reveal personal information about a third party
- information protected by solicitor-client privilege
- providing access would reveal confidential commercial information
- providing access might threaten the life or security of another individual
- information generated during a formal dispute resolution process
- personal information to which the member has requested access has been requested by a government institution for law enforcement, or an investigation related to law enforcement
- information collected without knowledge or consent for purposes related to investigating a breach of an agreement or a contravention of Ontario or Canadian law.

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

Treatment of Opinions and Judgements

The Credit Union cannot withhold from a member any opinions and judgements formed about the member in determining their eligibility for any products and services. The Credit Union will provide a member, on written request, access to all information that may have been used in deciding about a member's eligibility for a service, other than in the specific restrictions mentioned above.

Response Time

The Credit Union will respond to a member's request for information within 30 days. This timeframe can be expanded, but only if required, and on written notification to the member.

Cost of Response

At the Privacy Officer's discretion, the Credit Union may impose a fee at a stated and reasonable hourly rate where collection of the requested information requires exceptional time and effort. The member must be informed of, and agree to, an estimate of costs prior to the commencement of the request.

Challenging Compliance

Any individual, not just a member or a Credit Union employee, can challenge the Credit Union's compliance with any of the Code principles. The Privacy Officer will investigate all complaints.

Inquiry & Complaint Handling Process

The Privacy Officer will maintain documented procedures for responding to all questions or concerns.

Inquiries and complaints must be in writing, with a formal process in place to receive and track them. The Credit Union must respond as quickly as possible within 30 days.

Required Measures for Justified Complaints

The Privacy Officer is responsible for ensuring appropriate measures are taken when a complaint is found to be justified. These measures will include:

- written response to the complainant within 30 days
- revision of the challenged personal information
- revision to policies and procedures, if required
- review of any complaint that requires disciplinary action against a Credit Union employee with the appropriate manager
- reporting non-compliance to the Board, including the actions proposed or taken to resolve the issue.

Protection of Member Information with Third Parties

Third Party Accountability

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.

Personal information disclosed to unrelated third-party suppliers is strictly limited to programs endorsed by the Credit Union. The Privacy Officer must be satisfied that the personal information is adequately safeguarded by the third party.

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 policies of the Credit Union. Examples include data processors, credit bureaus, cheque printers, and cheque processors.

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

Storage of Information outside of Canada

In some cases, the Credit Union uses service providers located outside of Canada including in the United States of America. In such cases, the information may be accessible to lawful authorities located in these jurisdictions. The Credit Union takes reasonable steps to protect such information from unauthorized access as outlined above.