

Protection of Personal Information3

Accountability4

 Privacy Officer 4

 Quarterly Reporting 4

Identifying Purposes for Collection of Personal Information5

Consent.....5

 Obtaining Consent 5

 Limits on Consent to Information Collection 6

 Withdrawing Consent 6

Limiting Collection6

Limiting Use, Disclosure and Retention6

 Limiting Use of Personal Information 6

 Limiting Disclosure of Personal Information 7

 Limiting Retention of Personal Information 7

Accuracy.....7

Safeguards7

 Credit Union Safeguards 7

 Third Party Safeguards 8

 Destruction of Personal Information Safeguards 8

Openness.....8

Individual Access9

 Restricting Access 9

 Response Time 10

 Cost of Response 10

Challenging Compliance10

 Inquiry & Complaint Handling Process..... 10

 Required Measures for Justified Complaints..... 10

Protection of Personal Information

The 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. The credit union recognizes the Credit Union Code for the Protection of Personal Information (the Code) developed by Credit Union Central of Canada and set out in Credit Union Central of Canada's Credit Union manual, based on principles entrenched in the *Personal Information Protection and Electronic Documents Act* (Canada). Requirements of the Code establish the credit union's operational use of personal information as well as use of employee information.

The following ten interrelated privacy principles are specified in the *Personal Information Protection and Electronic Documents Act* (Canada), and form the basis of the Code:

- **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 the 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 as long as 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 credit union’s Board of Directors is accountable for credit union compliance with the Code, the creation and review of all Board policies specific to the Code and the designation of a credit union Privacy Officer.

Privacy Officer

The Board of Directors, in consultation with the CEO, will designate a Privacy Officer, who has primary day-to-day responsibility for compliance with the Code. The Board of Directors will notify all employees, the credit union’s members, and any affected third parties of the appointment. The credit union will provide all reasonable resources to enable the Privacy Officer to perform their duties effectively. The Privacy Officer of PenFinancial Credit Union Limited is the Financial Controller.

Quarterly Reporting

The Privacy Officer will continually review compliance with the Privacy Policies within the credit union and its third party suppliers, and will report to the Board of Directors and/or CEO 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 (through the M & CR Committee) that identifies key activities, any known contraventions of privacy laws by the credit union, including privacy breaches and recommended changes for the Board’s consideration. The report should also include an overview of the number of enquiries, number of requests for access to, or correction of, personal information, and details regarding challenges to compliance.

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

Issued: January 29, 2003, March 28, 2007, July 12, 2017

Approved by the Board of Directors: Jan. 29, 2003, Mar 28, 2007, July 26, 2017

Identifying Purposes for Collection of Personal Information

When collecting personal information, the credit union will state its purpose for collecting the personal information, as well as how it will be used and disclosed. The credit union will also provide on request the title and contact information for an employee who can answer the individual's question about the collection.

The Privacy Officer is responsible for approving any new purpose for the collection, use or disclosure of personal information, prior to the collection of personal information for the new purpose. If the new purpose is significantly different from existing purposes or involves a new use or disclosure to a third party, the proposed purpose must also be approved by the Board of Directors.

The credit union will make reasonable efforts to ensure that members are aware of and understand the purpose(s) for which their personal information is collected, used and/or disclosed.

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, provided the use is consistent with the original stated purpose.

The credit union's Privacy Officer must review all instances that are brought to the Privacy Officer's attention where a member's information is collected, used or disclosed without the member's knowledge and consent.

Obtaining Consent

The credit union will obtain express written consent for the collection, use and/or disclosure of personal information through the use of standardized forms such as membership applications.

The credit union will also comply with Canada's Anti-Spam Legislation (CASL) and their own internal CASL policy regarding Commercial Electronic Messages (CEMs).

The Privacy Officer must review and approve all forms used to obtain consent.

Limits on Consent to Information Collection

The credit union will not, as a condition of the supplying 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 with the express consent of the individual.

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 unless there is a legitimate purpose for the collection. At the time of collection, the credit union will specify the information to be collected, limited to what is necessary to fulfill the specified and legitimate purposes in accordance with this policy.

Limiting Use, Disclosure and Retention

Limiting Use of Personal Information

The credit union will not use personal information for purposes other than those for which it is collected, except with the express consent of the individual or as required or authorized by law.

Limiting Disclosure of Personal Information

The credit union will not disclose personal information except with the express consent of the individual or as required or authorized by law.

When disclosing personal information, the credit union will take all reasonable steps to protect the privacy of its members and other individuals to ensure that:

- orders or demands comply with the laws under which they were issued
- only personal information that is legally required is disclosed
- information is only disclosed to the person authorized to receive it
- all information disclosed to third parties receives the same standards of care as within 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. Notification may be by telephone, or by letter to the member's usual address.

Limiting Retention 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 the credit union's Retention policy for specifics.

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 routinely update personal information as necessary to fulfill the purposes for which the information was collected and/or at the request of the member.

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.

Third Party Safeguards

The credit union will require third-party agents, or suppliers of products or services to the credit union, to safeguard personal information disclosed to them in a manner consistent with this policy. 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.

The credit union will not enter into any commercial relationships with organizations that do not agree to the credit union's restrictions on the use and disclosure of personal information and any safeguards required by the credit union.

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

Destruction of Personal Information Safeguards

The credit union will 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 inquires can be directed
 - the means of gaining access to personal information held by the credit union
-

Issued: January 29, 2003, March 28, 2007, July 12, 2017

Approved by the Board of Directors: Jan. 29, 2003, Mar 28, 2007, July 26, 2017

- a description of the type of personal information held at the credit union, including a general explanation of what the personal information is used for
- types of personal information made available to other organizations such as affiliates or third party service providers.

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

The credit Union will provide routine account information, such as copies of recent statements, recent transaction slips, and account agreements, upon request to the member entitled to receive the information. The credit Union will charge its standard fee(s), in accordance with its standard fee schedule, for providing the information.

The credit union will provide non-routine account information after receiving and reviewing a written request (an “Access to Information Request”). The individual 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.

The credit union will direct an inquiry about non-routine account information and/or an Access to Information Request to the Privacy Officer. The Privacy Officer will provide assistance to an individual making an access to Information Request. The Privacy Officer will respond to all Access to Information Requests, including any refusal to provide information in whole or in part.

Restricting Access

The credit union will not disclose information that is prohibited from disclosing and that is not required to be disclosed, including information that:

- contains the personal information of another individual who has not consented to such disclosure of his or her personal information
- could threaten the safety or health of either the requesting individual, or a third party
- would reveal personal information about another individual
- would threaten the life or security of another individual
- cannot be disclosed for legal, security, or commercial proprietary reasons
- is subject to solicitor-client or litigation privilege

The Privacy Officer will review any situations where the credit union refuses to disclose the requested information in whole or in part due to the reasons set out above, and can consult with the Corporate Solicitor.

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 the Privacy Policies and Privacy Legislation. The Privacy Officer will investigate all complaints and respond to the individual

Inquiry & Complaint Handling Process

- The Privacy Officer is responsible for maintaining and reviewing, from time to time, documented processes for responding to all privacy related inquires and complaints.
- 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 of Directors, including the actions proposed or taken to resolve the issue.