ACCESS CREDIT UNION LIMITED		**POLICY**
Policy	**Privacy**	
Issued	Jul 2009	
Adopted/Amended	Mar 2019	
Review Date	Feb 2021	
Policy Owner	SVP & CFO	

CREDIT UNION CODE FOR THE PROTECTION OF PERSONAL INFORMATION

Access Credit Union Limited (the credit union) has adopted the Credit Union Code for the Protection of Personal Information (the code). The 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 derived from the code specified in the *Personal Information Protection and Electronic Documents Act*, and form the basis of the code.

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 code.

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 is required for the collection, use or disclosure of personal information, except in specific circumstances as described within the code.

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 fulfilment of those purposes and/or in accordance to the Retention and Destruction of Records Policy.

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. Safeguards

Security safeguards appropriate to the sensitivity of the information shall protect personal 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.

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 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.

1.1 Principle 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 code.

As such, the credit union Board of Directors (the board) 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.

1.1.1 Privacy Officer

The board will designate a Privacy Officer, in consultation with the President & CEO, who has primary day-to-day responsibility for compliance with the code. The board will direct the President & CEO to notify all employees in writing of the appointment.

The Privacy Officer appointed by the board must be a senior manager within the credit union who does not have a potential conflict of interest over any aspects of personal information protection such as marketing, sales, human resources or responsibility for technical safeguards.

In order to avoid a potential conflict of responsibility, the 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.

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 Privacy Officer's responsibility to ensure these employees are adequately trained in order to understand and follow all Privacy policies and procedures.

1.1.2 Deputy Privacy Officer

The board will designate, in consultation with the President & CEO, a substitute senior manager who will be available in the event of absences by the primary Privacy Officer and will have identical decision-making responsibilities during those absences.

1.1.3 Third-Party Accountability

A 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 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.

1.1.4 Board Reporting and Notification

1.1.4.1 Quarterly Reporting

The Privacy Officer will continually review the code and its compliance within the credit union and will report to the board and/or 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. The Privacy Officer will prepare a quarterly report for the board that identifies key activities.

1.1.4.2 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 appropriated. This report is due within four months of the end of each calendar year.

1.2 Principle 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.

1.2.1 Approval and Documentation of Purposes

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

If the proposed purpose is significantly different than existing purposes, board approval is required prior to implementation.

1.2.2 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.

1.2.3 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 an Employee Statement of Purposes and Consent Form.

1.3 Principle 3 – Consent

The knowledge and consent of the member is required for the collection, use, or disclosure of personal information, except in specific circumstances as described within this code.

Further consent will not be required when personal information is supplied to agents of the credit union who carry out functions such as, but not limited to, 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 disclosure without the member's knowledge and consent. Such instances are described in the Credit Union Code for the Protection of Personal Information.

1.3.1 Obtaining Consent

Due to the highly sensitive nature of personal financial information, express consent in writing, 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.

Implied consent will be used for marketing purposes or to disclose nominative information to an affiliated organization.

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

1.3.2 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 additional information that is non-essential to the product or service is sought from members, this shall be collected only as optional information, 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.

1.3.3 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.

1.4 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 these policies.

1.5 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 member or as required by law. Personal information shall be retained only as long as necessary for its purpose and/or in accordance to the Retention and Destruction of Records Policy.

1.5.1 Safeguard Standards

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 are issued;

b) only personal information legally required is disclosed, nothing more;

c) casual requests for personal information are denied; and

d) personal information disclosed to unrelated third-party suppliers is limited to programs endorsed.

The credit union will make reasonable attempts to notify the member when an order is received provided it is not in conflict with the credit union's security or not permitted legally. Notification will be done by telephone or letter.

1.5.2 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.

1.5.3 Destruction of Personal Information

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.

1.6 Principle 6 – Accuracy

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

1.7 Principle 7 – Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. The credit union will take the same standard of care as it takes to safeguard its own confidential information of a similar nature.

1.7.1 Credit Union Safeguards

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, use, copying, modification or disposal. The credit union shall 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 audits of the credit union's practices regarding personal information safeguards.

- periodically remind employees, officers and directors of the importance of maintaining the security and confidentiality of personal information.

Employees, officers and directors are required to complete privacy training annually, including electronic acknowledgment of their commitment to keep members' personal information secure and strictly confidential.

1.7.2 Third-Party Agents/Suppliers Safeguards

Third-party agents or suppliers are required to safeguard personal information disclosed to them in a manner consistent with the policies of the credit union.

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.

1.7.3 Destruction of Personal Information Safeguards

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.

Personal information will be disposed of by shredding. In-branch shredders or bonded contractors who shred documents on site will be used for this purpose.

1.8 Principle 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.

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

(a) the name or title, and the address of the Privacy Officer for compliance with the credit union's policies and procedures and to whom complaints or inquiries can be directed;

(b) the means of gaining access to personal information held by the credit union;

(c) a description of the type of personal information held by the credit union, including a general account of its uses;

(d) a copy of any brochures or other information that explains the credit union's policies, procedures, standards or codes; and

(e) the types of personal information made available to related organizations, such as subsidiaries or other suppliers of services.

1.9 Principle 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 challenge the accuracy and completeness of the information and have it amended as appropriate.

All access requests must be submitted in writing and include adequate proof of the individual's identity or right to access, and sufficient information to enable the credit union to locate the requested information.

1.9.1 Restricting Access

In certain situations, a 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:

- Providing access would not reveal personal information about a third party unless such information can be severed from the record or the third party consents to the disclosure, or the information is needed due to a threat to life, health or security;

- The personal information has been requested by a government institution for the purposes of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out any investigation related to the enforcement of any law, the administration of any law, the protection of national security, the defence of Canada or the conduct of international affairs;

- The information is protected by solicitor-client privilege;

- Providing access would reveal confidential commercial information, provided this information cannot be severed from the file containing other information requested by the individual;

- Providing access could reasonably be expected to threaten the life or security of another individual, provided this information cannot be severed from the file containing other information requested by the individual;

- The information was collected without the knowledge or consent of the individual for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;

- The information was generated in the course of a formal dispute resolution process.

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

1.9.2 Treatment of Opinions and Judgements

The credit union cannot withhold from a member any opinions and judgements formed about the member as a basis for determining their eligibility for any products and services. The credit union will provide a member, upon written request, access to all information that may have been used in making a

determination about a member's eligibility for a service, other than in the specific restricton mentioned in the above portion of the policy under restricting access.

1.9.3 Timeframe for Response

The credit union will respond to a member's request within 30 days. This timeframe may be expanded if required and upon written notification to member.

1.9.4 Cost for Response

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

1.10 Principle 10 – 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 is accountable for the credit union's compliance and will investigate all complaints.

1.10.1 Inquiry and Compliant Handling Process

The Privacy Officer will create and maintain documented procedures to respond to a credit union member or employee's questions or concerns. These procedures must be readily accessible to credit union members and employees, and must be simple to use.

Inquiries and complaints must be in writing, with a formal process in place to receive and track them and the credit union must respond as quickly as possible, but in any event, within 30 days.

1.10.2 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 the specified timeframe of 30 days;
- Revision of the challenged personal information;
- If required, revision to policies and procedures;
- Review of any complaint that requires disciplinary action against a credit union employee with the appropriate Manager(s);
- Reporting of non-compliance to the board, including the actions proposed or taken to resolve the issue, as specified in Board Reporting and Notification above.

Related Documents
Privacy Procedure
Retention and Destruction of Records Policy
Retention and Destruction of Records Procedure
Employee Statement of Purposes and Consent Form