Protection of Member Information and Privacy

Protection of Personal Information

- Education Credit Union (the credit union) has adopted the Credit Union Code for the Protection of Personal Information (the Code) effective April 25, 2002. 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 are required for the collection, use and disclosure of personal information, except in specific circumstances as described within this 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 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. **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.
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.

Accountability

The credit union 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.

- Education Credit Union (the credit union) has adopted the Credit Union Code for the Protection of Personal Information (the Code) effective April 25, 2002. The requirements of the Code establish the credit union's operational use of personal information as well as use of employee information.

Privacy Officer

- The Board of Directors will designate a Privacy Officer, in consultation with the CEO who has primary day-to-day responsibility for compliance with the Code. The Board of Directors will notify all employees, and any affected third parties, in writing of the appointment.
- 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 interest over any aspects of personal information protection.
- 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) 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 responsibility of the Privacy Officer to ensure these employees are adequately trained in order to understand and follow all Privacy policies and procedures.
  (Board Meeting of March 25, 2003)

Deputy Privacy Officer

- The Board of Directors will designate, in consultation with the 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.
  (Board Meeting of March 25, 2003)

Board Reporting and Notification

- The Privacy Officer will continually review compliance within the credit union and its third party suppliers, and will report to the Board of Directors and/or 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 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 appropriated. The report will also include an overview of the number of enquires, number of access requests, and details regarding challenges to compliance.

Identifying Purposes

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 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 of Directors 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. (See Employee Statement of Purposes and Consent form)

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 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, 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. 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 fulfil 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.

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 fulfil 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 fulfil 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 the personal information that is legally required is disclosed;
- Casual requests for personal information are denied; and
- Personal 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 it. Notification may be by telephone, or by letter to the member's usual address.

Retention and 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 Board & Management Responsibilities, **4 Records Management** for policies.

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. 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.

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 an Oath of Ethical Conduct annually. This statement must include a commitment to keep member's personal information secure and strictly confidential.

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.

Openness

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

The information will include the following:

- The name or title and the 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;
- A description of the type of personal information held at the credit union, including a general account of its use; and
- 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.

Individual Access

All request for access to personal information must be submitted in writing and include adequate proof of the individual's identity or 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;
- The information is protected by solicitor-client privilege;
- Providing access would reveal confidential commercial information;
- Providing access might threaten the life or security of another individual;
- The information was collected without knowledge or consent for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or
- 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.

Treatment of Opinions and Judgments

The credit union cannot withhold from a member any opinions and judgments 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 restriction mentioned above.

Response Time

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 member.

Cost of 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.

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 and Complaint Handling Process

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

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 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 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 the non-compliance to the Board of Directors, including the actions proposed or taken to resolve the issue.

Protection of Member Information with Third Parties

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