

**GODERICH COMMUNITY
CREDIT UNION
LIMITED**

**PROTECTION OF PERSONAL
INFORMATION**

Code For The Protection of Personal Information:

Goderich Community Credit Union Ltd. (the credit union) has adopted the Credit Union Code for the Protection of Personal Information (the Code) effective October 27th, 2003. 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 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 purpose 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. **Limited 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 purpose 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. The credit union shall have policies and procedures to respond to the member's questions and concerns.

**Board of Directors Resolution for
The Protection of Personal Information**

Whereas, Canada is part of a global economy based on the creation, processing and exchange of information which provides a number of benefits that improve the quality of our lives, but also gives rise to concerns about the protection of privacy rights and the individual's right to control the use and exchange of personal information; and

Whereas, the credit union is a member-owned and controlled financial institution and, as such, has an inherent responsibility to be open and accessible while at the same time, demonstrating the greatest respect for protection of the member's privacy;

Therefore be it resolved, the "Credit Union Code for the Protection of Personal Information" is adopted by the Board of Directors of Goderich Community Credit Union Limited.

Dated at Goderich this 27th day of October 2003.

Credit Union Policies for the Protection of Personal Information:

***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.**

The Board of Directors will designate a Privacy Officer, who will have primary day-to-day responsibility for compliance with the Code. The Board of Directors will also designate a Deputy Privacy Officer to act on behalf of the Privacy Officer. The Board of Directors will notify all employees in writing of these appointments.

This Privacy Officer appointed must be a senior manager within the credit union. The Privacy Officer appointed should not be the designated Compliance Officer under the federal regulations for the Proceeds of Crime (Money Laundering) Act. Preferably the Privacy Officer appointed should not have a potential conflict of interest over aspects of personal information protection such as marketing, sales, human resources or responsibility of technical safeguards.

The Privacy Officer is responsible to ensure employees receive adequate training in order to understand and follow policies and procedures under this Code.

The Privacy Officer will prepare a Quarterly Report for the Board that identifies matters concerning non-compliance with the credit union's Code principles, policies or procedures that are likely to require input from the Board. Furthermore, 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.

Privacy Officer – Sandy Wilson
Deputy Privacy Officer – Kim McDougall

***Principle 2: Identifying Purposes* - The purpose for which personal information is collected shall be identified by the credit union at or before the time the information is collected.**

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

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 credit union will ensure that all employees are aware of the purpose, 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.

Whenever the credit union receives a resume or other personal information from an individual seeking employment, this shall constitute implied consent solely to determine the qualifications of the job candidate for employment. The information shall not be used for any other purpose and shall not be disclosed to any other organization. Resumes or similar information received by the credit union shall be retained a maximum period of six months from the date of reception.

To detect and prevent fraud, and to help safeguard the financial interests of the credit union and its members, the credit union can collect, use or disclose personal information to combat fraud, collect debts, or otherwise protect the financial interests of the credit union without the knowledge or consent of the individual.

***Principle 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.**

Due to the highly sensitive nature of personal information, expressed consent in writing, primarily through the use of applications, signed forms and contracts, will be used for obtaining consent from 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.

The credit union will not require a member to consent to the information, 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 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.

***Principle 4: Limiting Collection* - 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.**

***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 the fulfillment of those purposes.**

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 the personal information that is legally required is disclosed and nothing more
- c) Casual requests for personal information are denied; and
- d) Personal information disclosed to unrelated Third Party suppliers is strictly limited to programs endorsed by the credit union.

The Privacy Officer will ensure that guidelines and procedures with respect to the retention of personal information are maintained within the credit union. Furthermore, the Privacy Officer will ensure that the credit union has guidelines and procedures to govern the destruction of personal information.

***Principle 6: Accuracy* - Personal information shall be as accurate, complete, and up-to-date as is necessary for the purpose for which it is to be used**

***Principle 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.**

The 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 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, including a commitment to keep member's personal information secure and strictly confidential.

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. The credit union will dispose of or destroy personal information in a secure manner to prevent any unauthorized access.

***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.**

Openness 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; and
- The types of personal information made available to related organizations such as subsidiaries or other suppliers of services.

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 question 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 allow the credit union to locate the requested information. The credit union shall respond to a member's request within 30 days; this timeframe can be expanded upon written notice to the member. 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 commencement of the request.

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;
2. The personal information to which the member has requested access has been requested by a government institution for the purposes of enforcing any laws, carrying out an investigation related to the enforcement of any law, the administration of any law, the protection of national security and the defense of Canada or the conduct of international affairs
3. The information is protected by solicitor-client
4. Providing access might threaten the life or security of another individual
5. The information was collected without the 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
6. The information was generated in the course of a formal disputed resolution process.

Principle 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.

The Privacy Officer will create and maintain documented procedures to respond to 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 within 30 days.

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, as specified in Principle 1, Accountability.

See attached the following member/compliance forms:

1. Privacy and Disclosure Consent
2. Decline to Share Personal Information
3. Consent to Release Personal Information
4. Limiting the Use of Social Insurance Numbers
5. Board of Directors – Quarterly Report