SPRUCE
CREDIT UNION

Preserving the human connection in banking

PRIVACY POLICY

Recommended by: Governance Committee 07/21/20
Approved by: Board of Directors 07/28/20

Privacy and Protection of Personal Information

Limitation:	Spruce Credit Union policy materials are **CONFIDENTIAL** and are not to be distributed outside of Spruce Credit Union without the prior written permission of Spruce Credit Union's CEO.
Scope:	This Policy applies to all business units of Spruce Credit Union, regardless of geographic locations.
Responsibility:	The Board of Directors, Management and Employees of Spruce Credit Union shall always strive to comply with all those aspects of Canada's Privacy Act, Personal Information Protection and Electronic Document Act (PIPEDA) and Personal Information Protection Act (PIPA), which apply to the various services provided to its members.
SCU Privacy Officer:	**Sue Peters, Sr Manager of Finance and Administration**
Alternate Privacy Officer:	**Ken Dickson, Chief Executive Officer**

Spruce Credit Union (SCU) 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 SCU.

The Code

SCU recognizes the Credit Union Code for the Protection of Personal Information ("the code") developed by Credit Union Central of Canada and set out in Canadian Credit Union Association manual, based on principles entrenched in the *Personal Information Protection and Electronic Documents Act* (Canada).

The Code is comprised of the following 10 interrelated privacy principles:

1. **Accountability** – SCU is responsible for personal information under its control and shall designate a Privacy Officer who is accountable for compliance with the principles of the Code.
2. **Identifying Purposes** – The purposes for which personal information is collected shall be identified by SCU at or before the time the information is collected.
3. **Obtain Consent** – The knowledge and consent of the individual are required for the collection, use, and 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 purpose identified by SCU. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure, and Retention** – 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. SCU will apply the same standard of care as it applies to safeguard its own confidential information of a similar nature.
8. **Openness** – SCU shall make readily available to individuals specific, understandable information about its policies and practices relating to the management of personal information.
9. **Individual Access** – Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual is entitled to question the accuracy and completeness of the information and have it amended as appropriate on proof of inaccuracy.
10. **Provide Recourse** – An individual shall be able to question compliance with the above principles to the Privacy Officer accountable for SCU compliance. SCU shall have policies and procedures to respond to the individual's questions and concerns.

The 10 principles of the code will form the basis for SCU privacy policies and practices (the "Privacy Policies"), as set out below.

1. ACCOUNTABILITY FOR COMPLIANCE WITH PRIVACY LEGISLATION

Compliance With Privacy Legislation

SCU will establish Privacy Policies that respect the Code and ensure that Spruce complies with applicable privacy legislation, [including the *Personal Information Protection Act* (BC), the *Personal Information Protection and Electronic Documents Act* (Canada), and the legislation commonly known as Canada's Anti-Span Legislation] (the "Privacy Legislation").

SCU Board of Directors is responsible for compliance with Privacy Legislation, the approval of Privacy Policies, and the designation of Spruce Privacy Officer and Alternate Privacy Officer.

SCU may also appoint a Privacy Review Team composed of managers and/or experienced employees representing all functional areas of the Credit Union.

Privacy Officer and Alternate Privacy Officer

Executive Management in consultation with the Board of Directors will designate a Privacy Officer who is responsible for managing and implementing the Privacy Policies and ensuring that SCU Privacy Policies comply with Privacy Legislation. Sue Peters has been designated Privacy Officer.

Executive Management, in consultation with the Board of Directors and the Privacy Officer, will designate an Alternate Privacy Officer who will have identical responsibilities to the Privacy Officer in the event of the absence of the Privacy Officer. Ken Dickson has been designated as Alternate Privacy Officer.

Breach Notification and Reporting

SCU will report any breach of security safeguards that results in real risk of significant harm to the Privacy Commissioner. Institutions that are subject to the *Privacy Act* and *Personal Information Protections and Electronics Document Act* may be required to report a privacy breach to the Office of the Privacy Commissioner of Canada (OPC) depending on the situation and its obligations under the applicable law. The Office of the Information and Privacy Commissioner (BC) may also be contacted depending on the details of the breach. A separate Privacy Breach Policy has been created and should be followed if a breach occurs.

Board Reporting

The Privacy Officer will continually review compliance with the Privacy Policies within SCU and its third-party suppliers and report to the board of Directors and Executive Management any material matters concerning non-compliance with SCU Privacy Policies.

The Privacy Officer will prepare an annual assessment report for the Board of Directors on the compliance effectiveness of the Privacy Policies. The report shall outline and identify key activities, any known contraventions of privacy laws by SCU, including privacy breaches, and any recommended policy or operational changes for the Board's consideration. The report will also include an overview of the number of inquiries or complaints received by the Privacy Officer, number of material requests for access to, or correction of personal information, and details regarding individual's challenges to SCU compliance with these Privacy Policies. The report is due within [five months of the end of each calendar year.

The Board of Directors will review each annual assessment report to determine whether additional steps, beyond those taken by the Privacy Officer are required.

2. IDENTIFYING PURPOSES FOR COLLECTION OF PERSONAL INFORMATION

When collecting personal information, SCU will state its purpose for collecting the personal information, as well as how it will be used and disclosed. SCU will also provide on request the position or title and contact information for an employee who can answer the individual's questions 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 form 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.

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

3. OBTAIN CONSENT

Express Consent

Express consent is when the individual giving consent has clearly stated, whether in writing, verbally, or through electronic means, his or her acceptance of the terms contained in a request for consent. Express consent is contrasted with implied or deemed consent, which is consent that is inferred from an individual's actions and the facts and circumstances of a particular situation.

Once express consent is obtained from an individual, further express consent will not be required when personal information is supplied to agents of SCU e who carry out functions such as data processing, cheque printing, and cheque processing, provided the use is consistent with the original stated purpose.

SCU Privacy Officer must review all instances that are brought to the Privacy Officer's attention where an individual's personal information is collected, used, and/or disclosed without the individual's knowledge and consent. The Privacy Officer can authorize further action following the review, such as the removal, destruction, or anonymization of the personal information from or on any of Spruce's systems.

Obtaining Express Consent

SCU will obtain express written consent for the collection, use, and/or disclosure of personal information through the use of standardized forms.

SCU will rely on express verbal consent only on an exceptions basis and the employee will record the date and time that the individual provided express verbal consent.

Notwithstanding the above exception, under no circumstances will SCU rely on express verbal consent to send a commercial electronic message ("CEM").

SCU will not rely on implied or deemed consent at any time, even on an exception basis.

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

Limits on Consents

SCU will not, as a condition of supplying a product or service, require an individual to consent to the collection, use, and/or disclosure of personal information beyond what is required to fulfill explicitly specified and legitimate purposes.

Where consent to the collection of additional, non-essential personal information for a product or service is sought from an individual, this will be identified as optional collection, use or disclosure, and will be collected, used, or disclosed only with the express consent of the individual.

Refusal to consent to such optional collection, use, and/or disclosure will not influence the individual's consideration for a product or service.

The Privacy Officer will review the personal information requirements of all products or service to ensure that only personal information required for the legitimate purpose is collected, used and/or disclosed.

Withdrawing Consent

SCU will require a written request from an individual who wants to withdraw consent. The request will be made on a standardized form provided by SCU. The standardized form will include the individual's acknowledgement that he or she has been advised that Spruce may not be able to provide a product or service that the individual requests, now or in the future, as a consequence of the withdrawal.

In addition, when an individual makes a request to withdraw consent, the employee processing the request will communicate the consequences of withdrawing consent to ensure that the individual can make an informed decision of whether or not to proceed.

The withdrawal of consent is subject to any legal or contractual restrictions. SCU will not allow the individual to withdraw consent if the withdrawal would impede the performance of a legal or contractual obligation.

4. LIMITING COLLECTION OF PERSONAL INFORMATION

SCU will not collect personal information unless there is a legitimate purpose for the collection. At the time of collection, SCU will specify the information to be collected, limited to what is necessary to fulfill the specified and legitimate purposes in accordance with the Privacy Policies.

5. LIMITING USE, DISCLOSURE, AND RETENTION OF PERSONAL INFORMATION

Limiting Use of Personal Information

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

Limiting Disclosure of Personal Information

SCU may share personal information with its subsidiaries and other carefully selected organizations with the express consent of the individual or as required or authorized by law. SCU will not disclose personal information except with the express consent of the individual or as required or authorized by law.

When disclosing personal information, SCU 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 required to be disclosed is disclosed, whether to comply with legal requirements or to fulfill contractual obligations (e.g. with a third-party service provider),
- Information is only disclosed to the person authorized to receive it, and
- All personal information disclosed to third parties is protected by the same standards of care as personal information held by SCU.

Limiting Retention and Destruction of Personal Information

SCU will retain personal information used to make a decision that affects an individual for a least one year after using it to make the decision.

The Privacy Officer will ensure that minimum and maximum retention periods are reviewed on a regular basis to ensure that they comply with legislative requirements. The Privacy Officer will also ensure that SCU securely disposes of, destroys, erases, or anonymizes personal information when there is no legal or business reason to retain it to prevent unauthorized parties from gaining access to the information.

The Privacy Officer will periodically review and evaluate the effectiveness of the disposal, destruction, and anonymization methods used by Spruce and will provide recommendations for improvement if required.

6. ACCURACY

The Privacy Officer will ensure that personal information held by SCU is as accurate, complete, and current as necessary to fulfill the purposes for which the information was collected. SCU will update personal information as necessary to fulfill the purposes for which the information was collected and/or at the request of the individual.

The Privacy Officer will ensure that personal information held on SCU behalf by third parties (e.g. data service providers) is kept accurate, complete and current.

7. SAFEGUARDS

SCU will protect personal information under its control through the combination of physical, electronic, and organization controls.

SCU controls will protect personal information against loss or theft, as well as unauthorized access, use, copying, modification, disclosure or disposal. SCU will protect personal information under its control regardless of the format in which it is held.

Third Party Safeguards

SCU will require third-party agents, or suppliers of products or services to SCU, to safeguard personal information disclosed to them in a manner consistent with the Privacy Policies. SCU will use contractual or other means to provide a comparable level of protection while the information is being held or processed by a third party.

SCU will not enter into any commercial relationships with organizations that do not, or cannot, agree to SCU restrictions on the use and disclosure of personal information and any safeguards required by SCU.

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

Ensuring Adequate Safeguards

The Privacy Officer will:

- Conduct regular reviews of organizational and employee practices related to the safeguarding of personal information; and
- Periodically remind employees, officers, and directors of the importance of maintaining the security and confidentiality of personal information.

Employees, officers, and directors are each required to commit in writing, on an annual basis, to keeping all personal information held by SCU secure and confidential. This commitment shall be included in SCU Confidentiality Agreement.

8. OPENNESS

SCU will direct inquiries about SCU Privacy Policies and processes to the Privacy Officer. SCU will provide the name and contact information of the Privacy Officer to the individual making the inquiry.

When responding to inquiries, the Privacy Officer can provide information that includes the following:

- The means that an individual can use to gain access to the personal information held by SCU
- A description of the type of personal information held at SCU 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 respond to inquiries in a form that is understandable and accessible to accommodate the reasonable means of the individual making the inquiry.

9. INDIVIDUAL ACCESS

SCU will provide routine account information, such as copies of recent statements, recent transactions slips, and account agreements, upon request to the individual entitled to receive the information. SCU will charge its standard fee(s), in accordance with its standard fee schedule, for searching and transcribing records.

SCU 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 SCU to locate the requested information.

SCU 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 non-routine Access to Information Requests, including any refusal to provide information in whole or in part.

Where SCU provides account information because of an Access to Information Request, and the account information is inaccurate, the individual can request that the information be corrected by making a written request (a "Correction of Information Request"). A Correction of Information Request will be reviewed by the Privacy Officer.

Restricting Access

SCU will provide information under an Access to Information Request subject to the restrictions set out in this section and under Privacy Legislation.

SCU will not disclose information that it 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, or
- Is subject to solicitor-client or litigation privilege.

However, if SCU is able to sever information that it is prohibited from disclosing and that is not required to be disclosed from its response to the requesting individual, it will do so.

If SCU refuses a request for access to personal information in whole or in part, SCU response to the Access to Information Request will provide the reasons for refusal and provide the name, position/title, address, and telephone number of an officer of SCU who can answer the individual's questions about the refusal. SCU may refuse to confirm or deny the existence of personal information collected as part of an investigation.

The Privacy officer will review any situations where SCU 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 Privacy Officer will respond to an Access to Information Request within 30 days. If additional time is required to provide the requested information, the Privacy Officer may extend the time to respond by up to an additional 30 days, subject to providing a written notice containing the required information to the individual who made the Access to Information Request.

If an extension of more than 30 days is required, the Privacy Officer will consult with Executive Management and the Board of Directors before making an application for approval to the Privacy Commissioner.

Cost of Response

SCU will charge a minimal fee in accordance with its access to information fee schedule for providing information under such a request. SCU will provide an estimate fee to the individual making the Access to Information Request. SCU will not proceed with processing the Access to Information Request unless the individual agrees to the fee estimate. SCU may require a deposit for all or part of the fee. SCU will not charge for correcting information.

10. PROVIDE RECOURSE

Challenging Compliance

Any individual can challenge SCU compliance with the Privacy Policies and Privacy Legislation. SCU will, on request, inform the individual of its complaint process, which will be accessible and simple to use. All inquiries and complaints regarding the Privacy Policies and any privacy-related matters will be referred to the Privacy Officer who is responsible for investigating the inquiry or complaint and responding to the individual.

SCU will accept inquiries verbally or in writing. Complaints will be accepted in writing only.

Inquiry and Complaint Handling Process

The Privacy Officer is responsible for maintaining and reviewing, from time to time, documented processes for responding to all privacy-related inquiries and complaints.

The Privacy Officer will acknowledge the individual's inquiry or complaint as soon as reasonably possible and provide an estimated time for a more detailed response, if required.

Depending on the nature of the complaint, the Privacy Officer will consult with Executive Management and/or the Board of Directors before providing a response.

Justified Complaints

If a complaint is found to be justified, the Privacy Officer is responsible for taking appropriate measures, including:

- Providing a written response to the complainant with the estimated time,
- Correcting incorrect personal information, if any,
- Revising the Privacy Policies and related processes, if required, and
- Reporting to Executive Management and/or Board of Directors on the actions proposed or taken to resolve the complaint.

Recommended by: Governance Committee 07/21/20
Approved by: Board of Directors 07/28/20