Saskatoon Community Foundation	**Policy: Privacy Policy**	**Last Review Date: May 2023**
	Established: August 2013 **Assigned to: Governance Committee**	**Review Cycle: Every 3 Years** **Next Review Date: 2026**

COMMITMENT

Saskatoon Community Foundation (SCF) is committed to protecting the privacy of its donors, grant applicants, employees, volunteers, and other stakeholders. SCF values the trust of its stakeholders and of the public and recognizes that maintaining this trust requires the foundation to ensure personal information is gathered, stored, and managed in compliance with Canadian privacy legislation.

DESIGNATED CHIEF PRIVACY OFFICER (CPO)

Chief Privacy Officer shall be the CEO - ceo@saskatooncommunityfoundation.ca

PERSONAL INFORMATION - Definition

Personal information is anything that can be used to distinguish, identify, or contact a specific individual. This information includes a person's name, address, birth date, email address, phone number, and financial information.

Exceptions: business contact information and publicly available information, such as names, addresses and telephone numbers as published in telephone directories, are not considered personal information.

Personal information will not be rented, sold, or shared with any third party

PRIVACY PROTECTION PRINCIPLES

10 Privacy Protection Principles are fair information practices recognized worldwide as standard rules for the collection, use and disclosure of personal information and designed to meet the public's expectation for personal information privacy protection. In Canada these principles have been adopted within the Canadian Standards Association's Model Privacy Code and entrenched in Part 1 of federal privacy legislation – "**Personal Information Protection Electronic Document Act**" ("**PIPEDA**"). In addition to focusing on an organization's obligations with respect to the handing of personal information, the principles also impose logistical and administrative obligations.

These key privacy principles consist of the following:

Principle 1 – Accountability
An organization is responsible for the personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with established privacy principles.

Principle 2 – Identifying Purposes
The purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Principle 3 – Consent
The knowledge and informed consent of the individual are required for the collection, use, or disclosure of personal information, except where exempted by law.

Principle 4 – Limiting Collection
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

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 informed consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Principle 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.

Principle 7 – Safeguards
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8 – Openness
An organization shall make readily available to individuals' specific information about its policies and practices relating to the management of personal information.

Principle 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 shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 – Challenging Compliance
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance

ADMINISTRATIVE PROCEDURES

Principle 1 – Accountability

1) Accountability for privacy protection within an organization entails the development, implementation and adherence to privacy protection policies and practices, as well as carrying out ongoing evaluation and refinement of the organization's privacy protection program. A Chief Privacy Officer shall be appointed for SCF, who shall take charge of SCF's privacy protection program and shall be responsible for: understanding the broad impact of privacy; the implementation of the Privacy Policy and procedures; and shall oversee the handling of any complaints. The specific duties and responsibilities of the Chief Privacy Officer are detailed in Appendix 1.

2) This privacy policy shall apply to all personal information in SCF's control, which includes data not only in SCF's physical custody, but also personal information that may have been transferred or available to a third party. Accordingly, contracts and/or other measures shall be taken to ensure that when third parties' access or process personal information on behalf of SCF, a level of privacy protection, comparable to that of SCF, is maintained on their part.

3) To ensure awareness and consistent implementation, SCF's privacy policies and practices shall be reviewed periodically as set out is this policy with staff, management, and volunteers, as well as integrated into new Board Member and staff training processes.

Principle 2 – Identifying Purpose

1) Identifying the purpose(s) for which SCF seeks to collect personal information is a critical first step in defining exactly what personal information it needs to acquire. Accordingly, a written "Purpose Statement" shall be prepared that:
   - Identifies the legitimate purpose(s) for collecting personal information and further, this purpose(s) shall not be defined too broadly, so as to make its definition meaningless to the individual from whom personal information would be collected; and
   - Will assist in the management of this personal information while it is in SCF's custody.

   The "Purpose Statement" shall be prepared prior to any collection of personal information.

2) When defining purpose(s), as required by section 4b (1) above, the following shall be considered:
   - Collection – Why is this information being collected?
   - Use – How will this personal information be handled within SCF?
   - Disclosure – Will this personal information be available to third parties outside of SCF at any time? If so, then how and why?

   A sample "Purpose Statement" is attached as Appendix 2. You will find SCF's Purpose Statement set out in this policy.

3) The purpose(s) for which personal information is to be collected must be reasonable and within the context of SCF's activities as a community foundation.

4) Opportunities to use non-identifiable information (e.g. coded, anonymous, pseudonymous, or aggregate data), rather than personal information, to meet the identified purpose(s) must first be explored, prior to a decision being made to collect personal information.

5) The actual use of personal information shall be limited to the purpose(s) set out in the written "Purpose Statement". Any use for a new purpose, one that is not defined in the "Purpose Statement", will require new consent from the individual, unless the new purpose is one that is required by law.

Principle 3 – Consent

1) Before or at the time of collection, everyone shall receive a meaningful explanation as to why his personal information is being requested by SCF and how this data will be collected, used and disclosed. After providing this information, consent may then be requested.

2) Individuals shall be advised that they may withdraw consent at any time and be provided with an explanation, as to any implications that may be associated with their withdrawal.

3) An individual's consent may be obtained in a variety of ways, including – "express or implied," "opt-in or opt-out", "verbal or written" forms of consent. The consent mechanism shall be documented, and the following considerations considered:
   - The form of consent shall take into consideration the following factors: reasonable expectations of the individual; circumstances surrounding the collection; sensitivity of the information involved.
   - Express consent should be used wherever possible.
   - The more sensitive the information (or the greater the potential harm to individuals), the greater the responsibility to ensure that the consent is explicit.

4) If consent cannot be obtained, written explanation shall be made, as in the case where the consent requirement is exempted by applicable privacy legislation – currently being the federal *Personal Information Protection and Electronic Documents Act (PIPEDA).*

5) If information is sought from a third party, about an individual, steps must be taken to ensure that the third party has gained consent from the individual for the disclosure.

Principle 4 – Limiting Collection

1) Information must not be collected indiscriminately; a clear link must exist between information that is to be collected and the purposes that have been identified in the "Purpose Statement". The amount and type of information that is beyond that which is necessary to fulfil the identified purposes shall not be collected.

Principle 5 – Limiting use, disclosure, and retention of personal information

1) Regular reviews of personal information resources of SCF shall be conducted. Personal Information shall be kept for a minimum length of time – for only as long as it is needed to achieve the identified purposes and the required length of time to fulfill legal retention requirements, as imposed by Canada Revenue Agency and other authorities.

2) Destruction of personal information shall follow SCF office policy and procedures for secure purging of files and data.

Principle 6 – Accuracy

1) Personal information must be as accurate, complete and up to date, as is necessary for the purpose(s) for which it is to be used.

2) If personal information is used or disclosed on an on-going basis, this information should be routinely updated. However, if a purpose does not require current information, then efforts to update should be limited to only what is necessary, unless the individual might be harmed by use or disclosure of inaccurate information.

Principle 7 – Safeguards

1) Appropriate security measures, both electronic and physical, shall protect against unauthorized parties accessing, using, copying, disclosing, altering and destroying personal information that is within SCF's custody, regardless of the format that it is in. The nature of these security safeguards shall be determined by and proportional to the sensitivity of the personal information involved.

2) When determining the level of sensitivity of personal information, the following factors shall be considered:
   - The quantity of personal information that may be revealed, if accessed by an unauthorized party; and
   - The magnitude of potential harm that an individual may suffer, should his personal data be misused or disclosed in an unauthorized manner.

The greater the exposure and potential harm - the greater is the required security.

3) Physical measures (locked filing cabinets, restricted access to office, etc.), organizational measures ("need to know access", staff training, confidentiality agreements etc.) and technological measures (passwords, encryption, firewalls, anonymizing software etc.) shall be used to safeguard personal information, as appropriate.

4) Personal information may only be transmitted over secured channels and/or shall be encrypted over open (unsecured) channels.

5) Staff and volunteers of SCF shall annually sign a confidentially of personal information statement.

Principle 8 – Openness

1) Information management practices of SCF shall:
   - Be open and transparent to the public.
   - Be informed by SCF's privacy policy and practices; and
   - Ensure that individuals are able to obtain the information that they require to understand SCF's privacy protection policy and measures.

2) An abbreviated Privacy Policy statement shall be published in the annual report and other appropriate SCF publications, including its website. The Privacy Policy Statement shall include contact information for SCF's Chief Privacy Officer. A sample form of Privacy Policy Statement is set out in Appendix 3.

Principle 9 – Individual Access

1) To enable individuals to make informed decisions about their relationship with SCF, and to provide them with some control over their personal information, individuals must be able to access personal information about themselves. Upon request, and verification of identity, individuals shall be provided reasonable access to their personal information at SCF.

2) Situations may exist where providing access to such personal information is not possible – as in situations where such disclosure would reveal personal information about others, be illegal, or pose a security threat. Reasons for not allowing an individual to access their personal information should be limited, specific, reasonable and justified and a written explanation for denial provided to the individual.

Principle 10 – Challenging Compliance

1) Individuals may challenge SCF's compliance with its Privacy Policy and practices. The Chief Privacy Officer shall receive, investigate, and respond to all privacy complaints.

2) All public enquiries about privacy issues involving SCF shall be responded to in a fair, accurate and timely manner following the complaints process as set out in Appendix 4.

PURPOSE FOR COLLECTING INFORMATION

During regular business operations, SCF gathers and uses personal information. This information is carefully protected as per the foundation's privacy policy and practices.

As per agreements with fundholders and grant recipients, SCF publicly reports specific details of its endowed funds, donations, and impact. This information is printed in the annual report, available in print and on the SCF website. Fundholders and donors may request anonymity.

SCF gathers information from donors when funds are established with the foundation and when donations or sponsorships are accepted. Information may include contact information, financial information, decision makers, instructions for stewarding funds, recognition preferences, financial representatives, family members, biographical information, and photos.

SCF gathers information from community organizations when accepting grant applications and assessing community needs. Information may include contact information, financial information, staff, volunteer, and client information, program details, and photos.

SCF gathers information from volunteers when recruiting and onboarding volunteers and managing board, committee, and volunteer work. Information includes contact information, references, biographical information, and photos.

SCF gathers information from staff when recruiting and onboarding staff members and managing business operations. Information includes contact information, emergency contacts, financial information, biographical information, and photos.

CONTROL OF PERSONAL INFORMATION

Personal information gathered by SCF is kept in confidence. SCF staff is authorized to access personal information based only on their need to deal with the information for the reason(s) for which it was obtained. Personal information will only be collected and used by authorized staff consistent with the activities of the SCF. We take measures to ensure the integrity of this information is maintained and to prevent its being lost or destroyed. We collect and use personal information only for purposes that a reasonable person would consider appropriate considering the circumstances
(moved above paragraph from the next section)

Prospective donors and fundholders asked for their personal contact information and philanthropic goals for communication and business purposes at the time of their initial interactions with SCF staff. When a fund is established, the fundholder is asked to formally provide consent for publicity and is offered the opportunity to remain anonymous.

Donors are asked to provide personal contact information for receipting and business purposes when donating by cheque, e transfer, or donation website. When a gift is received, donors are offered the opportunity to remain anonymous.

Through SCF application processes, grant applicants, board members, and staff members are asked to provide personal contact information.

Stakeholders may withdraw consent for public acknowledgement or email communication at any time. Stakeholders may review information held on file.

DATABASE & WEBSITE HOSTING AND STROING

When SCF uses an outsourced database provider on the public cloud for transmitting or storing data, SCF requires that the secure data center and its backup is located within Canada.

SCF uses password protocols, encryption software and firewalls to ensure privacy and to protect personal and other information we may receive online. Our software is routinely updated to maximize protection of such information.

SCF is strongly committed to protecting the privacy of those who use our website. This site compiles conventional log files to monitor and assess activity including traffic and visits on, and related to, the site. This activity does not specifically identify any individual user without prior notice to the user through use of the site.

SCF does not disclose information about individual visits to our website. Neither does it provide the information given to us on our website to outside companies. The information collected is used to improve and enhance the content and services of the website.

CANADIAN ANTI-SPAM LEGISLATION (CASL) - Compliance

SCF uses commercial electronic messages to share information with stakeholders, send newsletters, and provide grant application info to subscribers. Messages are sent to stakeholders who have provided express consent through new fundholder procedures, grant applications, staff or volunteer applications, or newsletter subscription procedures. Messages may be sent to stakeholders with implied consent where a continuing business relationship exists or where an inquiry has been made within the previous six months.

All messages are accurate and truthful, include the name of the sender the organization, and include a current mailing address plus either a phone number, email or website address which is valid for 60 days after the date of the message.

All messages contain an unsubscribe mechanism with clear instructions, and unsubscribe requests are actioned within 10 business days or less.

VIOLATIONS AND BREACHES

(a) Reporting – Any board of directors' member, committee member, volunteer, or staff member with knowledge of a possible violation of this Privacy Policy shall report it to the Chief Privacy Officer. If the possible violation involves the Chief Privacy Officer, the report shall be made to any other Officer or Member of Management of SCF.

(b) Breaches by board of directors' members and members of committees – Where it is determined, after discussion with the member, that he or she has violated this Privacy Policy, the Board will consider the extent to which the duty of honest, loyal and faithful service has been breached in its consideration of the need for redress. Breaches which are deemed by the board to be severe may result in the removal of the member from the board or the respective committee. Where it has been determined that the staff member or volunteer has breached this Privacy Policy, the CEO and Chair will consider the extent to which the duty of honest, loyal, and faithful service has been breached in considering the need for redress. Breaches deemed to be severe may result in the termination of employment, contractual agreement, or volunteer service.

ACKNOWLEDGEMENT

Each board member, committee member, staff member and volunteer shall file at the first commencement of the role with the CEO and Chair an acknowledgement that he or she has received and read this statement and has agreed to comply with the policy and associated practices.

MONITORING

The policy is to be reviewed as set out in the policy currently every 3 years by the board at the board meeting closest to the anniversary of its adoption.

CONTACT INFORMATION:

Questions, concerns, or complaints relating to SCF's privacy practices or the treatment of personal information, may be e-mailed to ceo@saskatooncommunityfoundaiton.ca, made by phone at 306-665-1768, or sent in writing to:

Chief Executive Officer
Saskatoon Community Foundation
101 -308 4th Ave North
Saskatoon SK S7K 2L7

Further information on privacy and your rights regarding your personal information may be found on the website of the Privacy Commissioner of Canada at https://www.priv.gc.ca/en/

You can also contact:

Office of the Privacy Commission of Canada
112 Kent Street
Ottawa ON K1A 1H3

APPENDIX 1

Duties & Responsibilities of a Chief Privacy Officer (CPO)

The role of a chief privacy officer is multi-disciplinary. This leadership role involves the interpretation of privacy law and the creation of privacy programs that ensure the protection of personal data and compliance with current legislation across an organization.

CPO shall be responsible for ensuring that the following duties are addressed:

- Leadership of the privacy program
- Conduct privacy risk assessments and audits
- Develop and implement corporate privacy policies and procedures
- Create and deliver educational, training and orientation programs
- Monitor systems development and operations for security and privacy compliance
- Ensure compliance related to privacy, security, and confidentiality
- Audit and administer privacy programs
- Provide counsel relating to business contracts and partnerships
- Track and report on compliance related to privacy, security, and confidentiality
- Resolve allegations of non-compliance
- Maintain current knowledge of federal and provincial privacy legislation and regulations
- Manage public perception of data protection and privacy practices for the organization
- Liaise with government agencies and the privacy commissioner's office

APPENDIX 2

Sample Purpose Statement

The following purpose statement can be adapted for situations:

"Saskatoon Community Foundation respects your privacy. It will protect your personal information and adhere to all legislative requirements with respect to protecting privacy. It does not share its mailing lists. The information you provide to the foundation will be used to deliver services and to keep you informed on its activities through periodic contacts. This includes impact reporting, financial reporting, news and announcements, opportunities for charitable giving, information on grant programs, invitations to special events, and opportunities to volunteer or learn. If at any time you wish to be removed from a foundation mailing list, you may contact Saskatoon Community Foundation by phone at (306) 665-1766 or by email at office@saskatooncommunityfoundation.ca, and your request will be accommodated."

APPENDIX 3

Sample Privacy Policy Statement – for Publication

Commitment

Saskatoon Community Foundation (SCF) is committed to protecting the privacy of its donors, grant applicants, employees, volunteers, and other stakeholders. SCF values the trust of its stakeholders and of the public and recognizes that maintaining this trust requires the foundation to ensure personal information is gathered, stored, and managed in compliance with Canadian privacy legislation.

What is considered personal information

Personal information is anything that can be used to distinguish, identify, or contact a specific individual. This information includes a person's name, address, birth date, email address, phone number, and financial information.
Exceptions: business contact information and publicly available information, such as names, addresses and telephone numbers as published in telephone directories, are not considered personal information.

Privacy practices

During the course of regular business operations, Saskatoon Community Foundation (SCF) gathers and uses personal information. This information is carefully protected as per the foundation's privacy policy and practices.
As per agreements with fundholders and grant recipients, SCF publicly reports specific details of its endowed funds, donations, and impact. This information is printed in the annual report, available in print and on the SCF website. Fundholders and donors may request anonymity.

Control of your personal information

Prospective donors and fundholders asked for their personal contact information for communication and business purposes at the time of their initial interactions with SCF staff. When a fund is established, the fundholder is asked to formally provide consent for publicity and is offered the opportunity to remain anonymous.

Donors are asked to provide personal contact information for receipting and business purposes when donating by cheque, e transfer, or donation website. When a gift is received, donors are offered the opportunity to remain anonymous.

Through SCF application processes, grant applicants, board members, and staff members are asked to provide personal contact information.

Stakeholders may withdraw consent for public acknowledgement or email communication at any time. Stakeholders may review information held on file.

Website

Saskatoon Community Foundation is committed to safeguarding visitor privacy on its website.

Updating of privacy policy

Saskatoon Community Foundation regularly reviews and updates its privacy policy and practices. Visit Governance and Policies - Saskatoon Community Foundation for current privacy information.

Contact information

Questions, concerns, or complaints relating to Saskatoon Community Foundation's privacy practices or the treatment of personal information, may be e-mailed to ceo@saskatooncommunityfoundation.ca, made by phone at 306-665-1768, or sent in writing to:

Chief Executive Officer
Saskatoon Community Foundation
101 -308 4th Ave North
Saskatoon SK S7K 2L7

Further information on privacy and your rights regarding your personal information may be found on the website of the Privacy Commissioner of Canada at https://www.priv.gc.ca/en/

You can also contact:

Office of the Privacy Commission of Canada
112 Kent Street
Ottawa ON K1A 1H3

APPENDIX 4

Complaint Procedure

The Chief Privacy Officer shall:

- Create a detailed written record of the nature of the complaint (e.g. delays in responding to a request, incomplete or inaccurate responses, or improper collection, use, disclosure or retention) and the date upon which the complaint was received by HCF.
- Promptly acknowledge receipt of the complaint in writing.
- Deal with complaints in a timely fashion.
- Conduct a fair and impartial investigation and create a written record of all decisions that are made.
- Clearly and promptly notify individuals of the outcome of the Chief Privacy Officer's investigation.
- Correct any inaccurate personal information or modify policies and procedures based on the outcome of complaints received.

Privacy Policy

REVIEW AND SELF-REFLECTION DECLARATION

I have read the Privacy Policy & Procedure and agree to adhere to its provisions.

Signature: _____

Print Name: _____

Position: _____

Date: _____