Saskatchewan Council for International Cooperation I Privacy Policy

Policy Type: Board	
Policy Title: Privacy Policy	
Policy Number: 001	
Approved Date: November 24, 2007	
Scheduled for Review: 2025	
Document History: • *February 15, 2023*	

Policy Purpose

From time to time, Saskatchewan Council for International Cooperation (SCIC) will gather, maintain, and use personal information about its members, donors and subscribers, either directly or under the auspices of programs such as the WorldBeatProject or the Make Poverty History Campaign. This policy outlines the steps that SCIC will undertake to safeguard the privacy of this information.

1. Accountability

A. The SCIC Finance Officer shall act as the SCIC Privacy Compliance Officer.
B. Complaints and/or inquiries arising from the collection of personal information shall be directed to the Privacy Compliance Officer of the organization.
C. While SCIC may distribute information from other organizations to its mailing lists from time to time, subscriber's personal information shall not be shared with any third party. Information collected under the auspices of one SCIC program (such as the WorldBeat Project) shall not be merged with information from other programs, but be kept separate in order to receive specific program communications only and not general communications of the organization.

2. Purpose

Personal information will be used to correspond with members, donors or subscribers for the purpose of providing them with official documentation, informing them of upcoming events, circulating information on campaigns or issues, fundraising appeals, or other events as may from time to time arise.

3. Consent

A. Consent to gather personal information shall be inferred from a subscriber's actions (i.e. emailing a request to subscribe shall constitute consent to use subscriber's personal information).
B. This policy shall be made available to all subscribers.
C. Information collected under SCIC Programs may be disclosed to the Saskatchewan Council for International Cooperation only.
D. Limiting Collection
    a. The information collected shall be limited to
        i. Name
        ii. School or Organization Name (if applicable)
        iii. Address
        iv. Postal Code
        v. Telephone number
        vi. E-mail address
    b. Name, Address, and Postal Code information is needed to send communications to the subscriber.
    c. Telephone numbers are required to communicate with subscribers quickly (i.e. in the event of a program cancellation).

5. Limiting Use, Disclosure and Retention

Member, donor or subscriber information shall be retained for the life of the Council unless SCIC is requested by the member, donor or subscriber to remove or change such information.

6. Accuracy

A. Individuals shall be responsible to ensure they have provided the project with correct information.
B. Individuals shall be responsible for informing the project's Privacy Compliance Officer with appropriate updates to their personal information.

7. Safeguards

A. All reasonable measures shall be taken to protect subscriber's personal information against loss or theft.
B. Access to electronically stored information shall be limited to employees of the Saskatchewan Council for International Cooperation.
C. Employees shall annually be made aware of the need to protect the privacy of subscriber's personal information.
D. This policy shall be reviewed annually.

8. Openness

This policy shall be published on SCIC's website and the sites of associated programs.

9. Individual Access

A. Upon request by a subscriber, the Privacy Compliance Officer shall confirm the existence of a subscriber's personal information and shall provide a copy of this policy to the subscriber.
B. If a subscriber deems her/his personal information to be inaccurate, the subscriber shall be given the opportunity to correct any inaccuracy.

C. Challenging Compliance
    a. Complaints and/or inquires regarding this policy shall be directed to the Privacy Compliance Officer.
    b. Upon receiving a complaint and/or inquiry, the Privacy Compliance Officer shall attempt to resolve the issue as expeditiously as possible.

Attachment A

Examples of Fraud and Corruption

- Intentional concealment, omission, falsification or perversion of truth
- Inducing another to part with some valuable item or surrender a legal right
- Nepotism
- Bribery, kickbacks and/or gratuities
- Collusive behavior with vendors
- Keeping false records,
- False claims (e.g. requesting payment for goods, services or activities not actually performed)
- Embezzlement, and theft
- Receiving or providing financial and non-financial favors with the intent of facilitating activities that the person may not normally receive
- Conflict of interest

Falsification, misappropriation, and other fiscal irregularities refer to, but are not limited to:

- Any dishonest or fraudulent act
- Forgery or alteration of any document or account (including, but not limited to timesheets, payroll, accounts, travel and expense reports, procurement documents or inventory/asset registers)
- Forgery or alteration of a cheque, bank draft, or any other financial instrument
- Misappropriation of funds, commodities, securities, supplies, equipment, or other assets
- Impropriety in the handling or reporting of money, financial transactions, or bidding procedures
- Accepting or seeking anything of material value from suppliers or persons providing services/ materials as provided by applicable policies on gifts
- Destruction or misappropriation of records, furniture, fixtures, or equipment
- Diversion, alteration, or mismanagement of documents or information, and/or any similar or related irregularity
- Any malicious use of internet and IT documents or messages
- Cybercrime and/or identity theft

Attachment B

Suggested Language for Agreements with External Parties

Fraud and Corruption. SCIC does not tolerate fraud and corruption, and we expect the same from everyone with whom we work. [Insert outside party defined term] shall maintain and comply with written codes of conduct and policies and procedures that protect against any form of fraud and corruption, bribery, kickbacks, conflicts of interest, and others. Upon request, [insert outside party defined term] shall share with SCIC its applicable codes of conduct, policies and procedures. [Insert outside party defined term] shall inform SCIC immediately (within twenty-four hours) and in writing of any instance of actual or suspected fraud or corruption related to its work hereunder and shall respond promptly to and fully cooperate with any investigation SCIC, in their discretion, may require. [Insert outside party defined term] shall make all employees aware of and encourage reporting of any suspected or actual fraudulent or corrupt behavior through SCIC's notification system. [Insert outside party defined term] shall be financially responsible for any losses due to fraud, and shall promptly refund such amounts to SCIC.

Attachment C

Initial Investigation of Suspected Fraudulent Report

Pursuant to SCIC's Policy on Fraud and Corruption Prevention, Awareness, Reporting and Response, this form shall be submitted within three business days in all cases regardless of amount, or materiality, and shall be submitted prior to a full investigation. **One or two sentence responses to each item below are sufficient for the purposes of this initial report**.

1) Organization:
2) Project(s) compromised:
3) Date of discovery:
4) Method of discovery:
5) Date reported to SCIC:
6) Details:
7) Amount or value (estimate if necessary):
8) Initial internal control weaknesses or systems failures identified:
9) Initial remedial actions are taken:
10) Potential for additional related fraud or corruption losses:
11) Initial determination of fraud/corrupted amount:
12) Initial determination if funder reporting is required:
13) [Attach additional pages or attachments if necessary]

Attachment D

SCIC's Anti-Fraud and Corruption Responsibilities

Function	Activity
1) Prevention and Awareness	a. Orientation and training for new employees, partners, sub-projects, and refresher training.
	b. Systems review, spot-checks, and internal audits.
	c. Internal controls in place
	d. Funder regulations, policies, and reporting procedures
2) Violation Alert (tip-off, verbal or written report)	a. SCIC report received and shared with implicated entities.
	b. Report through SCIC general email received and shared with implicated entities.
	c. Report received by a Partner/sub-project and shared with implicated entities.
	d. Report directly to an office received and shared with implicated entities.
3) Initial Investigation	a. Conduct initial investigation.
	b. Results are shared in the preliminary report along with recommendations for further/larger investigation.
	c. Reporting back to the complainant if necessary.
	d. Initial funder report.
4) Reporting and Corrective Actions	a. Action / corrective action plan developed and shared.
	b. Funder report.
	c. Implement appropriate sanctions and corrective measures

5) Major Investigation	a. Sourcing external assistance if needed (e.g., TOR, cost, etc.)
	b. Draft report and recommendation produced and shared.
	c. Feedback for report finalization.