QIA Privacy Policy

Approved by the Board of Directors on March 5, 2025

1.0 Introduction

This Privacy Policy is made by the QIA Board of Directors. The Executive Director has the authority to make and approve procedures to implement this Policy.

1.1. Policy Principles

QIA is committed to a high standard of privacy and transparency with respect to the collection, storage, and use of personal information.

The purpose of this Policy is to ensure that QIA has a robust system for:

- Limiting the collection, use, and disclosure of personal information to the purposes for which it was collected;
- Protecting personal information within its control; and
- Ensuring the accuracy of personal information within its control.

QIA follows best practices for the protection of personal information and has chosen to follow the principles of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). As a Nunavut society, QIA is not bound by the *Privacy Act (Canada),* PIPEDA, or the *Access to Information and Protection of Privacy Act (Nunavut).*

1.2 Application

This Privacy Policy applies to QIA's Board of Directors, employees, and authorized third parties including contractors and service providers.

2.0 Definitions

For the purposes of this Policy,

"Privacy breach" means the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards[1] that are referred to in clause 4.7 of Schedule 1 of PIPEDA, or from a failure to establish those safeguards.

"Personal Information" means any information about an identifiable individual that QIA collects in the course of its activities, including but not limited to prospective, current and former QIA Employees, Executive Committee Officers and Community Directors, or third parties. Examples of personal information include, but are not limited to, date of birth, social insurance number, Nunavut Tunngavik Inc. enrolment number, marital status, medical, criminal or employment history.

"Privacy Officer" is the individual who is accountable for QIA compliance with the Privacy Policy.

3.0 Accountability

3.1 The Executive Director, or their delegate, is the designated Privacy Officer to oversee QIA's compliance with the Privacy Policy.

3.2 The Privacy Officer is responsible for ensuring QIA provides training on this policy, complies with this policy, and responds to requests from individuals about their personal information.

3.3 QIA Employees, Executive Committee Officers and Community Directors, with access to personal information must take privacy training and commit to protecting the confidentiality of individuals' personal information.

3.4 QIA will ensure authorized third parties with access to personal information have contractual or other means to provide a comparable or better level of protection for the collection, use, disclosure and safeguarding of personal information as apply to QIA under this policy.

3.5 QIA may receive requests from any individual to find out whether QIA holds any personal information about them and to review that information. Requests to access personal information stored by QIA are received by the Privacy Officer. QIA will correct any mistakes in personal information where it is identified. Individuals may also complain or inform QIA of a privacy breach, which will be investigated and remedied as appropriate.

4.0 Identifying purposes for collection and obtaining consent for collection, use or disclosure of

[1] QIA refers to the security safeguards from the Principle 7 of the Model Code for the Protection of Personal Information included in Schedule 1 of Canada's *Personal Information and Protection of Electronic Documents Act* (PIPEDA):

- Security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification, regardless of the format of storage;
- Safeguards will depend on the sensitivity of the information. More sensitive information should be safeguarded by a higher level of protection;
- The methods of protection should include:
  (a) physical measures, for example, locked filing cabinets and restricted access to offices;
  (b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
  (c) technological measures, for example, the use of passwords and encryption;
- Organizations shall make employees aware of the importance of maintaining confidentiality of personal information; and
- In the disposal or destruction or personal information, care should be used to prevent unauthorized parties from access.

personal information

4.1 QIA only collects personal information to the extent necessary to carry out its activities. When collecting personal information from an individual, QIA must inform the individual of the purposes of the collection and how their information will be used, including whether it will be shared with authorized third parties. This should be available in Inuktitut and English.

4.2 The Privacy Officer will ensure there are privacy statements explaining QIA's privacy policy in forms, contracts, on QIA websites or other purposes used to collect personal information and obtain consent.

4.3 Except where required by law, QIA must obtain consent to collect, use or disclose an individual's personal information. Consent may be given in either English or Inuktitut, in writing (such as via an application form), with an electronic mark (such as a check box), or orally (such as over the telephone). Implied consent from an individual may be appropriate in limited situations, such as if the collection is for the benefit of the individual or the information is not sensitive.

4.4 Where consent is not provided by the individual directly, an authorized representative or legal guardian may give consent. If consent is provided by a third party who is not an authorized representative or legal guardian, the collection must be for the benefit of the individual.

4.5 Where QIA receives personal information from a third party, it must ensure the third party providing the information obtained consent before disclosing it or the information is being disclosed to satisfy a legal requirement.

5.0 Using and storing personal information

5.1 QIA only uses personal information for the purpose for which it was collected. QIA must obtain individuals' consent to use their personal information for a new purpose.

5.2 All personal information must be stored and safeguarded in a secure manner (for example, by password protection or by filing documents in a locked cabinet). The use of external drives and shared drives is discouraged and may only be used where necessary.

5.3 QIA Employees, Executive Committee Officers and Community Directors, and authorized third parties may only access personal information for QIA activities.

5.4 Personal information that is not needed, or is no longer required for QIA's activities, must be deleted and/or securely destroyed as soon as practicable. QIA may retain personal information required for litigation or to meet regulatory requirements, such as limitation periods, tax, employment, or other applicable laws.

5.5 Except as allowed or required by the law, QIA Employees, Executive Committee Officers, Community Directors, or authorized third parties must not disclose or share personal information with any other third parties without the consent of the individual whose personal information is being disclosed or shared.

5.6 QIA ensures that adequate provisions for the protection of personal information in QIA's control to standards that meet or exceed this policy are included in any contracts with authorized third parties where necessary.

6.0 Privacy Breaches

6.1 All suspected or actual privacy breaches must be reported to the Privacy Officer. If the Privacy Officer is a delegate of the Executive Director, all suspected or actual privacy breaches must be reported to the Executive Director.

a. The Privacy Officer must consider the privacy breach in light of the sensitivity of the personal information involved and the probability of misuse to determine if there is a risk of significant harm.

b. Acting under the supervision of the ED if they are a delegate, if the Privacy Officer determines there is a real risk of significant harm to an individual resulting from a privacy breach, the Privacy Officer must ensure the affected individual(s) are informed about the breach. The Privacy Officer may determine whether to inform affected individuals directly or, if it would be unduly difficult, would cause additional hardship to the individual(s), or QIA does not have the individual's or individuals' contact information, to inform the affected individual(s) indirectly (for example, through an advertisement in English and Inuktitut).

c. A notification of a privacy breach will include the following information:

- A description of the circumstances of the breach;
- The date or estimated date of the breach;
- A description of the personal information that is the subject of the breach, to the extent that the information is known;
- A description of the steps QIA has taken to reduce the risk of harm that could result from the breach;
- A description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
- Contact information that the affected individual can use to obtain further information about the breach.

6.2 The Privacy Officer, with direction from the Executive Director if they are a delegate and legal advice if required, will determine an appropriate response in the event of a breach and who will be informed about a breach (such as affected individuals, the Board and/or other organizations, such as authorized third parties or law enforcement).

6.3 Whether or not the Privacy Officer determines that affected individuals must be informed, the Privacy Officer must create a record of any suspected or actual breach containing the following information:

- Date or estimated date of the breach;
- General description of the circumstances of the breach;

- Nature of information involved in the breach;
- Actions taken in response; and
- Any recommendations or lessons learned.

7.0 Electronic Messages

7.1 When QIA sends electronic messages such as e-mails or SMS of a commercial nature, which can include offers of goods, fundraising, donations or promotion of similar activities, it must ensure:

a. It has the consent of recipients;
b. The electronic message identifies QIA as the sender; and
c. The electronic message includes an unsubscribe mechanism.

8.0 Compliance with this Policy

8.1 The Privacy Officer will receive and review any complaints about the implementation of this policy, including information about potential breaches of this policy. The Privacy Officer will investigate and respond to complaints. If the Privacy Officer determines amendments to this policy are warranted, they may make recommendations to improve QIA's compliance or to change the Policy.

8.2 The Privacy Officer will supervise compliance with this policy and, if they are a delegate, report regularly to the Executive Director. Where necessary, and at least annually, the Privacy Officer will provide a report to the Board of Directors.

8.3 QIA will review and update this Policy as needed, including where privacy laws or best practices change (for example, for the use of new technologies or new activities).