

Information Privacy Policy

Policy

Ensuring the privacy of personal information provided to the Nipissing First Nation by individuals is essential to not only ensure compliance with legislative requirements such as those outlined in the Personal Information Protection and Electronic Documents Act or substantially similar provincial legislation, but also to ensure continued stakeholder confidence in Nipissing First Nation and that accountability is maintained.

Purpose

The purpose of this policy is to provide guidance on the implementation and maintenance of appropriate information privacy practices within Nipissing First Nation related to the collection, use, disclosure, retention, and safeguarding of personal information.

Scope

This policy applies to all Council members, members of the Finance and Audit Committee, officers and employees of Nipissing First Nation and any contractors or volunteers performing services on behalf of the Council. The direction provided in this policy applies to all personal information created and acquired by Nipissing First Nation regardless of format (i.e., both electronic and hardcopy paper records).

Definitions

“**Personal information**” refers to all information that reveals factual or subjective elements of knowledge about an identifiable individual. In addition to the basic elements that are commonly used to identify and interact with an individual - such as the individual’s name, gender, physical characteristics, address, contact information, identification and file numbers - it also includes criminal, medical, financial, family and educational history as well as evaluative information and other details of the individual’s life.

“**Privacy Protection**” refers to the decisions made by Nipissing First Nation in regards to the acceptable ways to collect, create, use, share/disclose, retain, protect and dispose of the personal information that it needs for its administrative and operational needs.

Responsibilities

Council is responsible for:

- Establishing and implementing documented procedures for privacy and the management of personal information within Nipissing First Nation;
- Appointing a Privacy Officer to manage and oversee Nipissing First Nation’s compliance with privacy requirements; and this policy.

The Chief Executive Officer is responsible for:

- Ensuring compliance with the established information privacy policy.

The Privacy Officer is responsible for:

- Developing and maintaining standards, policies and procedures that support the objectives of Nipissing First Nation's privacy program;
- Ensuring that all the activities of Nipissing First Nation are conducted in compliance with the established privacy standards, policies and procedures and in accordance with the generally accepted privacy principles. For this, the Privacy Officer will:
 - i. Provide training and awareness on privacy protection.
 - ii. Ensure that community members are aware of their rights as they relate to privacy, including their right of access to, and the right to request the correction of, all the personal information which is kept about them by the Nipissing First Nation.
 - iii. Act as an expert resource on privacy matters within Nipissing First Nation.
 - iv. Conduct periodic reviews of Nipissing First Nation's activities that involve the collection, use, disclosure, retention, and safeguarding of personal information.
 - v. Investigating all complaints regarding the collection/creation, accuracy, use, sharing/disclosure, protection, retention and destruction of personal information and reporting the results to the appropriate managers and, where warranted, to Council;
 - vi. Recommending changes to policies, procedures and practices in response to the issues raised in the complaints;
 - vii. Responding in writing to the requests for access to, and correction of, personal information submitted by employees and community members within thirty calendar days from the date of the receipt.

Employees, contractors and volunteers are responsible for:

- Complying with the established information privacy policy.
- Immediately reporting to their supervisor privacy breaches of which they become aware.

Procedures

Accountability

Nipissing First Nation must appoint a Privacy Officer to ensure the principles outlined in this policy are appropriately implemented.

Nipissing First Nation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization should use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Identifying Purpose

The purposes for the collection of personal information should be communicated to individuals at or before the time of collection. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

Personal information should be collected directly from the individual whenever possible.

Persons collecting personal information must be able to explain to individuals the purposes for which the information is being collected.

Consent

With limited exceptions, Nipissing First Nation must obtain consent from an individual before collecting their personal information. Consent requires that the individual is advised of the purposes for which the information is being collected and how it will be subsequently used and disclosed.

Consent must be stated in such a manner that the individual within reason will understand how the information will be used or disclosed. Consent must not be obtained through deception.

Personal information can be collected, used, or disclosed without the knowledge and consent of the individual in only limited circumstances. For example, legal or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Consent may be sought from an individual's authorized representative in certain cases, for example, when an individual is seriously ill, mentally incapacitated, a minor, or has died.

If personal information is intended to be used or disclosed for a new purpose not identified during the original collection, and not related to the original purpose of the collection, the consent of the individual must be obtained.

Individuals can give consent in many ways. For example:

- a form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
- consent may be given orally; or,
- consent may be given through electronic means.

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Nipissing First Nation must stop using the individual's personal information within a reasonable time period and inform the individual of this time period and the implications of such withdrawal.

Limiting Collection

Nipissing First Nation cannot collect personal information indiscriminately. Both the amount and the type of information collected must be limited to that which is necessary to fulfill the purposes identified.

Limiting Use, Disclosure and Retention

Nipissing First Nation may only use or disclose personal information for the purpose for which it was collected, unless:

- The use or disclosure of the personal information is consistent with the original collection of the personal information;
- The consent of the individual is obtained; or,
- It is for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information.

Personal information that has been used to make a decision about an individual must be retained long enough to allow the individual access to the information after the decision has been made.

Identifiable personal information must only be used and disclosed if required. For instance, consider if reports, research, or audits/assessments can be done through de-identified or anonymous data.

Personal information that is no longer required to fulfill the identified purposes will be destroyed, erased, or made anonymous in accordance with Nipissing First Nation's retention and disposition schedule.

Accuracy

Nipissing First Nation shall take all reasonable steps to ensure that personal information that is used to make a decision on an individual is as accurate, up-to-date and complete as possible to minimize the possibility that inappropriate information may be used to make a decision about the individual.

Safeguards

Personal information should be protected with appropriate safeguards to ensure only those with a need to know will have access to the records:

For electronic records containing personal information, the records should be protected with controls on the document itself (such as password protection) and other administrative controls, such as restricting access to the electronic repositories in which the record is stored. Personal information should not be emailed without appropriate protection.

For hardcopy paper-based records containing personal information, the records should be stored in secure filing cabinets at all times unless being used, and transported in a secure manner if required to be taken offsite.

Nipissing First Nation must make its employees, contractors, and volunteers aware of the importance of maintaining the confidentiality of personal information.

Care must be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

Openness

Nipissing First Nation must be open about its policies and practices with respect to the management of personal information. Individuals will be able to acquire information about its policies and practices without unreasonable effort. This information must be made available in a form that is generally understandable.

The information made available should include:

- The name or title, and the address, of the Privacy Officer, who is accountable for Nipissing First Nation's policies and practices, and to whom complaints or inquiries can be forwarded;
- The means of gaining access to personal information held by Nipissing First Nation; and,
- A description of the type of personal information held by Nipissing First Nation, including a general account of its use.

Individual Access

When requested, an individual must be informed if Nipissing First Nation holds personal information about the individual and provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

The identity of an individual must be authenticated before discussing their personal information with them.

When requested, Nipissing First Nation must provide an individual with access to their personal information within a reasonable time and at minimal or no cost to the individual. The requested information will be provided or made available in a **form** that is generally understandable.

Commented [GC1]: format?

Individuals who are given access to their personal information may:

- Request correction of the personal information where the individual believes there is an error or omission therein;
- Require that a notation be attached to the information reflecting any correction requested but not made; and,
- Require that any person or body to whom that information has been disclosed for use for a decision-making process within two years prior to the time a correction is requested or a notation be notified of the correction or notation.

In certain situations, the Nipissing First Nation may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be

limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions may include information that:

- Is prohibitively costly to provide;
- Contains references to other individuals;
- Cannot be disclosed for legal, security, or commercial proprietary reasons; or,
- Is subject to solicitor-client or litigation privilege.

Challenging Compliance

Nipissing First Nation must ensure that a process exists to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint procedures will be easily accessible and simple to use.

Nipissing First Nation must investigate all complaints. If a complaint is found to be justified, the First Nation will take appropriate measures, including, if necessary, amending its policies and practices.