Policy Change Log

Date	Change	Edited by:	Approved by:
	Policy creation	Feb. 26, 2018	

Personal Information Privacy Protection Policy

Table of Contents

Instructions ..... **Error! Bookmark not defined.**
Policy Change Log 1
Purpose of the Policy 3
Scope of the Policy 3
Regulatory Compliance 3
Definitions 3
Responsibility for Policy Implementation 4
Policy Requirements 4
Communication of the Policy 5
Policy violations and non-compliance 5

Purpose of the Policy

The purpose of this policy is to prevent the unauthorized modification or disclosure of Personally Identifiable Information (PII) by ensuring that appropriate administrative, technical, and physical safeguards are implemented.

Scope of the Policy

This policy applies to all Township of the North Shore devices, employees, and contractors. All employees and contractors with access to the Township of the North Shore's computing devices or information systems shall comply with this policy as it applies to their job duties.

Regulatory Compliance

The Township of the North Shore is required to comply with the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56. Adherence to this policy is required for compliance.

Definitions

Personal Information means recorded information about an identifiable individual, including,

1. Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
2. Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
3. Any identifying number, symbol or other particular assigned to the individual,
4. The address, telephone number, fingerprints or blood type of the individual,
5. the personal opinions or views of the individual except if they relate to another individual,
6. Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
7. The views or opinions of another individual about the individual, and

8. The individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Personal Information Bank means a collection of personal information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual.

External Party means any person or entity that is not part of, or an employee of the Township of the North Shore.

Information Owner means the individual to whom a specific record in a Personal Information Bank pertains.

Responsibility for Policy Implementation

The Township of the North Shore's Privacy Officer shall be responsible for ensuring implementation of all items listed in the Policy Requirements section. Responsibility for the creation and implementation of specific procedures may be assigned to internal staff or contractors as appropriate.

Policy Requirements

1. Recordkeeping
   a. An "Index of All Personal Information Banks" shall be maintained and updated at least annually.
   b. A "Personal Information Bank Data Sheet" shall be completed and updated as necessary for each Personal Information Bank that we maintain.
2. Person Information Bank Custodians
   a. The Privacy Officer may designate a "Personal Information Bank Custodian" (PIB Custodian) for any particular Personal Information Bank.
3. Limiting access to authorized individuals
   a. The Privacy Officer, or the PIB Custodian, shall be responsible for authorizing individuals to view or modify the records in each Personal Information Bank.
   b. Physical records shall be kept in a locked drawer, cabinet, or room. Access to keys shall be restricted authorized individuals.

   c. Electronic records shall be stored in a central location. Access to each individual Personal Information Bank shall be restricted to authorized individuals, using Access Control Lists (ACLs) or other reliable means of restricting access.
4. Authorizations
   a. The Township of the North Shore employees – access shall be restricted to employees who require access in order to complete their job functions. All such access shall be recorded in a physical or electronic log.
   b. External parties – access shall be restricted to external parties that have been authorized based on legal statute or consent. All such access shall be recorded in a physical or electronic log.
   c. Information owners – Information owners shall be provided access to any records pertaining to them.
      i. Information owners shall be provided access to records pertaining to them only.
      ii. Information owners may request corrections to records, based on evidence or criteria established by the Privacy Officer or PIB Custodian.
      iii. All such access shall be recorded in a physical or electronic log.
      iv. The Privacy Officer or PIB Custodian shall create and maintain a process to ensure compliance with this policy.
5. Backup of electronic records
   a. There shall be a backup process to ensure that all electronic records are protected from hardware failures, software failures, and intentional or unintentional alteration.
   b. All backup copies of Personal Information Banks shall be subject to the same access controls as the primary records.
6. Retention
   a. For each Personal Information Bank, there shall be a defined retention period, after which records are “expired”.
   b. There shall be a documented process for reviewing each Personal Information Bank at least annually and for ensuring the deletion of destruction of expired records.

Communication of the Policy

The Township of the North Shore’s Privacy Officer shall communicate this policy to all employees and contractors to ensure proper implementation.

Policy violations and non-compliance

Intentional violations of this policy shall subject the violator to appropriate sanctions. These sanctions may include suspension or dismissal.

Policy non-compliance shall result in a written warning for the first violation. Subsequent sanctions will be at the discretion of the Privacy Officer.