THE CORPORATION OF THE NATION MUNICIPALITY

PRIVACY BREACH POLICY
#AD-01-2019

Effective date: September 23rd, 2019

Resolution: 584-2019

Table of Contents

PRIVACY BREACH POLICY

1. Statement of Organizational Commitment

The Corporation of The Nation Municipality is committed to protecting personal information in the custody or control of the municipality and comply with the privacy protection requirements as mandated by the *Municipal Freedom of Information and Protection of Privacy Act*.

2. Background

The *Municipal Freedom of Information and Protection of Privacy Act* provides a right of access to information under the control of institutions in accordance with the principles and to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

Sections 31 & 32 of the *Municipal Freedom of Information and Protection of Privacy Act* outlines when an institution can use and/or disclose personal information in its custody or under its control. When the use or disclosure of personal information or records containing personal information violates Sections 31 or 32 of the *Municipal Freedom of Information and Protection of Privacy Act* or other applicable legislation, a privacy breach occurs. Privacy breaches can occur when personal information of residents or employees is stolen, lost, or mistakenly disclosed (eg. personal information is mistakenly emailed to the wrong person).

3. Purpose

The purpose of this policy is to ensure that all Nation Municipality employees and Members of Council, at all times, comply with the privacy protection requirements as mandated by the *Municipal Freedom of Information and Protection of Privacy Act*.

This policy confirms The Nation Municipality's obligation to protect personal information in the custody or control of the institution. Privacy Breaches undermine public trust in an institution and may result in significant harm to the Municipality and to those whose personal information is collected, used or disclosed inappropriately.

This policy outlines the steps that shall be followed when an alleged Privacy Breach is reported to ensure that it is quickly contained and investigated to mitigate the potential for further dissemination of personal information.

4. Scope and Responsibility

This policy applies to all Nation Municipality employees, volunteers, agents, contractors, and members of Council.

The CAO/Clerk is responsible for the overall implementation and enforcement of this policy.

5. Definitions

"Act" means the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Chapter M. 56.

"Employee" means any paid employee, including, but not limited to, full-time, part-time, paid apprenticeships, and seasonal employees.

"Municipality" means the Corporation of The Nation Municipality.

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

a) Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;

b) Information relating to the education or the medial, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

c) Any identifying number, symbol or other particular assigned to the individual;

d) The address and telephone number of the individual;

e) The personal opinions or views of the individual except if they relate to another individual;

f) 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;

g) The views or opinions of another individual about the individual; and

h) 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.

"Privacy Breach" means the use or disclosure of personal information or records containing personal information in violation of Section 31 or 32 of the Act.

"Record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes:

a) Correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine-readable record, any other documentary material, regardless of physical form or characteristics, and copy thereof; and

b) Subject to regulations, any record that is capable of being produced from a machine-readable record under the control of an institution by means of a computer hardware and software of any other information storage equipment and technical expertise normally used by the institution.

6. General Procedure

When a privacy breach is alleged to have occurred, municipal staff shall undertake immediate action. In all instances of a privacy breach or alleged breach the following procedure, conducted in quick succession, or concurrently, shall be followed.

6.1 Step 1: Identify and Alert

If a complaint has been received or you suspect that a privacy breach has occurred, contact the CAO/Clerk or designate immediately. The CAO/Clerk will then investigate the validity of the complaint or suspicion. The "Risk Assessment Chart," attached hereto as Appendix A, can be

used to assist in determining if a privacy breach occurred. If a privacy breach is confirmed, the CAO/Clerk or designate will evaluate the severity of the breach and proceed accordingly.

6.2 Step 2: Contain

The CAO/Clerk shall, in cooperation with other staff, undertake the following actions to contain the alleged privacy breach:

- Retrieve and secure any records associated with the alleged breach;
- Where appropriate and depending on circumstances, isolate and suspend access to any system associated with the alleged breach (i.e. an electronic information system, change passwords, etc.);
- Suspend processes or practices which are believed to have served as a source for the alleged breach; and
- Take any other action necessary to contain the alleged breach.

6.3 Step 3: Notify

The CAO/Clerk shall notify the Information and Privacy Commissioner of Ontario (IPC) of all alleged and confirmed privacy breaches.

The CAO/Clerk shall notify all individuals affected by a privacy breach as soon as possible, via telephone followed with a formal letter that shall include the following information:

- Information surrounding the nature of alleged, or confirmed, privacy breach;
- The details of the breach (as understood at the time of notification);
- The specific personal information affected;
- Steps, if any, taken so far to control or reduce the harm;
- Future steps planned to prevent future privacy breaches;
- Steps the individuals can take to protect themselves; and
- Contact information for municipal staff and the Information and Privacy Commissioner of Ontario should they have any questions.

The CAO/Clerk or designate shall handle all inquiries with respect to privacy breaches and the actions of the municipality in response to an alleged or confirmed breach. The CAO/Clerk or designate will determine if other authorities or organizations, such as law enforcement, privacy commissioner's office, and/or professional/regulatory bodies should be informed of the breach.

6.4 Step 4: Investigate

After all efforts have been exhausted to contain the alleged privacy breach and notifying the affected individuals, the CAO/Clerk or designate shall undertake an investigation in an attempt to establish:

- Whether a privacy breach occurred;
- A time line of the events that led to the breach;
- The source of the breach, including any policies or procedures responsible for the breach;
- The nature and sensitivity of the personal information disclosed;
- The number of individuals affected; and
- Any other factors relevant to the circumstances.

6.5 Step 5: Report and Follow-up

Following the completion of the investigation, a report shall be prepared by the CAO/Clerk or designate outlining the results of the investigation, including any recommendations to mitigate future incidents. Consistent with the privacy best practices, a copy of the report shall be forwarded to the IPC, as well as to all individuals who were affected by the privacy breach.

7. Risk Assessment Chart

The "Risk Assessment Chart" can be used to assist in determining if a privacy breach occurred. If you answer "No" to all risk factors, there is a low probability that personal information has been compromised and it's not likely a reportable breach. Regardless, the CAO/Clerk will make the determination.

	Risk Assessment	Yes or No
1.	**Risk of identity theft** Is there a risk of identity theft or other fraud? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's licence numbers, personal health numbers, debit card numbers with password information or any other information that can be used for fraud by third parties (e.g. financial information).	
2.	**Risk of physical harm** Does the loss of information place any individual at risk of physical harm, stalking or harassment?	
3.	**Risk of hurt, humiliation, damage to reputation** Could the loss of information lead to hurt, humiliation or damage to an individual's reputation? This type of harm can occur with the loss of information such as medical or disciplinary records.	
4.	**Risk of loss of business or employment opportunities** Could the loss of information result in damage to the reputation of an individual, affecting business or employment opportunities?	