Eastern Ontario Regional Network (EORN) Privacy Policy

An initiative of the Eastern Ontario Wardens Caucus Inc.

March 05, 2020

POL- 2.2	Original Issued:	Supersedes:	Last Revised:
Date:	February 6, 2020	February 6, 2020	March 5 2020

2.2 Privacy Policy

2.2.1 Background

The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) provides a right of access to information under the control of institutions in accordance with the principles. It also works 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 and 32 of MFIPPA outline 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 or other application legislations, a privacy breach occurs.

Whereas, under Section 3, subsection (2) of the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990 c.M.56 the members elected or appointed to a board, commission or other body that is an institution under the Act may designate in writing from among its members an individual or committee of the body to act as head of the institution for the purposes of the Act; and

Whereas the Eastern Ontario Regional Network Board of Directors deems it necessary and expedient to designate a head for the purposes of the Act:

Now, therefore, the Eastern Ontario Regional Network Board of Directors resolves as follows:

1. **That the Eastern Ontario Regional Network Board of Directors hereby designates the EORN Chief Executive Officer (CEO) or designate as head for the purposes of the Municipal Freedom of Information and Protection of Privacy Act; and that**
2. **That this resolution come into force and effect on Thursday March 5, 2020; and further**
3. **That Privacy Policy # 2.2 be amended as necessary.**

2.2.2 Purpose

EORN is committed to protecting personal information in the control or custody of the municipality and comply with the privacy protection requirements as mandated by MFIPPA. The purpose of this policy is to ensure that all EORN employees, members of board, officers, volunteers, contractors, and agents comply at all times with privacy protection requirements.

This policy confirms EORN's obligation to protect personal information in the control or custody of the institution. Privacy breaches undermine public trust in an institution and may result in significant harm to EORN 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.

2.2.3. Purpose

This policy applies to all EORN employees, contractors, agents, and members of the Board.

2.2.4. Definitions

"Board" means members of the Board of Directors of EORN.

"EORN" means the Eastern Ontario Regional Network.

"Employee" means any employee, contractor, sub-contractor and volunteer of EORN engaged in EORN business, whether on a full-time, part-time, temporary or casual basis.

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

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

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

c) The telephone number, address, fingerprints or blood type of the individual;

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

e) 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;

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

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 an incident involving unauthorized disclosure of personal information, including it being stolen, lost, or accessed by, or disclosed to, unauthorized persons (including employee snooping or inadvertent disclosure through human error) that is not in accordance with MFIPPA.

2.2.5. Policy and Protection Procedures

Protection of Privacy and Personal Information Guiding Principles

EORN is required to protect privacy and personal information to meet its legislative and corporate obligations. Protecting privacy, including the proper stewardship of the personal information and only requesting necessary personal information, is fundamental to maintaining the public's trust and confidence.

Collecting and Maintaining Personal Information

EORN will:

- Collect only personal information that is relevant to and necessary for a particular purpose and will provide notice that the information is being collected. The notice shall state: the legal authority for the collection; the reason for the collection; how the institution plans to use the information; and, who to contact for more information;
- Ensure all personal information collected is maintained in a secure manner;
- Collect and process personal information fairly and lawfully; and
- Keep personal information accurate, complete and up to date.

Appropriate Measures for Availability and Access

EORN will:

- Make personal information available internally and externally only in appropriate circumstances (required by law or for a law enforcement purpose) or when consent by the individual has been obtained. When required by law, EORN will refer to the

Information and Privacy Commissioner of Ontario's ("IPC") fact sheet, "Disclosure of Personal Information to Law Enforcement" attached hereto as Appendix C;

- Only use the personal information collected for the purpose for which it was collected or for consistent purpose;
- Only disclose personal information if it is permitted for the purpose of complying with law;
- Provide individuals with appropriate access to personal information about themselves by providing a Freedom of Information request to the Privacy Officer.

Retention

EORN will:

- Retain personal information in accordance with EORN's Records Retention By-law;
- Retain all personal information, whether in paper or electronic form, in a safe and secure manner.

Safeguarding Information and Privacy Breaches

EORN will:

- Implement appropriate measures to safeguard personal information and instruct third parties processing personal information on behalf of EORN to process it only in a manner that is consistent with EORN procedures;
- Ensure that privacy protection measures are included in any contracts or agreements with third parties;
- Identify and report all privacy breaches as set out in this policy;
- When writing letters, reports, etc. try to avoid names and instead refer to "complainant" or "caller" and will refer to residential properties by address and not the owner's name;
- Educate employees in privacy awareness to reduce the risk for a breach or invasion of personal information.

Protection

Employees will protect personal information from unauthorized access, loss, theft, or inadvertent destruction or damage by implementing safeguards such as:

- Clean desk practices;
- Lock away personal information when unattended;

- Lock computer when unattended and follow the IT Privacy Policy;
- Lock desks and cabinets containing personal information;
- Coded file labels rather than descriptive text;
- Circulate personal information internally on a need to know basis; and
- Security provisions in contracts with external providers of storage or disposal of records.

2.2.6. Roles and Responsibilities

Privacy Officer

The Privacy Officer or designate shall handle all inquiries with respect to privacy breaches and the actions of EORN in response to an alleged or confirmed breach. The Privacy Officer 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.

For the purposes of this policy the Privacy Officer shall be the EORN Director of Communications and Stakeholder Relations.

Directors, Officers and Managers

Directors, Officers and Managers shall be responsible for becoming familiar with this policy and providing training to their staff and new hires. Directors and Managers shall ensure compliance with this policy, address non-compliance and report any suspected privacy breach to the Privacy Officer.

Employees & Contractors:

Employees & Contractors shall:

- Collect only personal information that is relevant to and necessary for a particular purpose;
- Familiarize and comply with this policy, and related policies and procedures; and
- Alert a Director, Manager or Privacy Officer of a suspected privacy breach.

2.2.7. Privacy Breach Procedure

Procedure

When a privacy breach is alleged to have occurred, EORN employees shall undertake immediate action in accordance with the Information and Privacy Commissioner of Ontario's 'Privacy Breaches – Guidelines for Public Sector Organizations' attached hereto as Appendix B.

In all instances of a privacy breach or alleged breach the following procedure, conducted in quick succession, or concurrently, shall be followed.

Step 1: Identify and Alert

If a complaint has been received or you suspect that a privacy breach has occurred, contact the Privacy Officer or designate immediately. The Privacy Officer will then investigate the validity of the complaint or suspicion. The "Risk Assessment Chart," attached hereto as Appendix C, can be used to assist in determining if a privacy breach occurred. If a privacy breach is confirmed, the Privacy Officer or designate will assess the severity of the breach and proceed accordingly.

The Privacy Officer or designate shall handle all inquiries with respect to privacy breaches and the actions of EORN in response to an alleged or confirmed breach. The Privacy Officer 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.

Step 2: Contain

The Privacy Officer shall, in cooperation with other employees, carry out the following actions to contain the alleged privacy breach:

- Determine what personal information is involved;
- Where appropriate and conditional 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;
- Take corrective action to:
    - Ensure no personal information has been retained by an unauthorized recipient and get their contact information for any future follow up;
    - Ensure the breach does not allow other unauthorized access to personal information; ex. change passwords, or temporarily shut down a system
    - In a case of unauthorized access by a member of the Board or an employee, consider suspending their access rights or appropriate discipline; and
    - Retrieve hard copies of any personal information that has been disclosed; and
- Take any other action necessary to contain the alleged breach.

Step 3: Notify

The Privacy Officer shall advise the Information and Privacy Commissioner of Ontario of significant breaches, such as those that may involve sensitive personal information or large numbers of individuals, or when having difficulties containing the breach.

The Privacy Officer shall notify all individuals affected by a privacy breach as soon as possible if it is determined that the breach poses a real risk of significant harm to the individual. The Privacy Officer will take into consideration the sensitivity of the information and whether it is likely to be misused.

Notification to individuals should be direct, such as telephone, email or in person, along with a formal letter that includes the following information:

- Details of the extent of the breach and the specifics of the personal information that was compromised;
- The steps taken and planned to address the breach, both immediate and long term;
- If the information is financial, a suggestion to contact their bank, monitor their bank and credit card activity and obtain a copy of their credit report;
- Contact information for the Privacy Officer (or designate) for information and assistance; and
- A statement that they have a right to make a complaint to the Information and Privacy Commissioner and how they can do so.

Step 4: Investigate

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

- Identify and analyse the events that led to the breach;
- A timeline of the events that led to the breach and the nature and sensitivity of the personal information disclosed;
- The source of the breach, including any policies or procedures responsible for the breach. Review policies and practices in protecting personal information, privacy breach response plans and employee training to determine whether changes are needed;
- Take corrective action to prevent similar breaches in the future and ensure employees are adequately trained; and
- Any other factors relevant to the circumstances.

Step 5: Report and Follow-Up

Following the completion of the investigation, a report shall be prepared by the Privacy Officer or designate outlining the results of the investigation, including any recommendations to mitigate future incidents. If the Information and Privacy Commissioner was notified, a copy of

the report shall be sent to them. A copy of the report to all individuals who were affected by the privacy breach.

The report will also be included on the EORN Board of Director's Agenda when:

- More than five (5) individuals are affected by a confirmed breach; or,
- In the opinion of the Privacy Officer it is determined that it is in the public interest to provide such a report.

Any recommendations from the report will be reviewed and where appropriate, implemented.

2.2.8. Review Cycle

This Policy will be reviewed at a minimum of once every three (3) years.