MATTAWA REGIONAL OPP DETACHMENT BOARD
CONSEIL DU DÉTACHEMENT RÉGIONAL DE MATTAWA DE LA POLICE PROVINCIALE

NORTH BAY OPP DETACHMENT
DÉTACHEMENT DE NORTH BAY DE LA POLICE PROVINCIALE

| #2026-02 | |
|---|---|
| **Policy: Protection of Privacy Policy** | |
| **Date of Board Approval:** 07/06/2026 | **Date of Next Review:** 07/06/2031 |

## 1. POLICY PURPOSE

The Mattawa Regional OPP Detachment Board's Protection of Privacy Policy establishes guidance and principles for the responsible management of Personal Information by the Board.

This policy outlines privacy management accountabilities and oversight mechanisms to enable Board staff to comply with the privacy requirements identified in the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

## 2. POLICY STATEMENT

In accordance with its obligations under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), the Mattawa Regional OPP Detachment Board will ensure the protection of individuals' personal information in its custody or control by complying with the appropriate methods for collection, use, retention and disposition of personal information, as much reasonably possible.

## 3. DEFINITIONS

**"Act"** means the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M56 (MFIPPA).

**"Consistent Purpose"** means a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.

**"Personal Information"** means recorded information about an identifiable individual. To quality as personal information:

- It must be about an individual in a personal capacity
- It is reasonable to expect an individual may be identified if the information is disclosed

Examples of personal information include:

- Home address, personal email address, home telephone number, identification numbers e.g. Social Insurance Number or employee number

- Correspondence between the individual and the Board that directly or indirectly relates to private or confidential matters
- Ethnic origin, religion, age, gender, sexual orientation, marital status,
- Educational, medical, criminal history, employment history, or personal financial transactions
- 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

Some of the above examples do not constitute Personal Information on their own; however, when combined with other information, it may constitute Personal Information (for example, a poll or survey may not contain a person's name or address but may include information that could potentially identify an individual).

This policy definition is a guideline for the benefits of understanding personal information. The Specific legislative definition of "Personal Information" in MFIPPA applies to this policy.

**"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.

**"Privacy Breach"** occurs when personal information is collected, retained, used or disclosed in a way that is not in accordance with MFIPPA.

**"Secondary Purpose"** means a purpose that is not consistent with the original purpose.

## 4. SCOPE

- This policy applied to all Boar Employees and volunteers engaged with the Mattawa Regional OPP Detachment Board.
- This policy applies to all Personal Information that is under the custody or control of the Board.

## 5. COLLECTION OF PERSONAL INFORMATION

5.1. Personal Information will not be collected by Board staff unless it is essential for business purposes, authorized for collection under legislation, or permitted under Board policy or by-law, and applicants should be informed of the principal purpose of collection at the time the personal information is collected during an application process.

5.2. Personal Information will not be collected without the knowledge or consent of the individual to whom the information relates except in certain conditions under S.29 of MFIPPA or when providing emergency care or treatment.

5.3. Personal Information of minors (under 16) will not be collected without express or implied authorization of a parent/guardian.

5.4. All Personal Information collected will be complete and accurate.

5.5. Personal Information will only be used for the purpose for which it was collected unless used for a Consistent Purpose the individual to whom the information relates might reasonably expect, or unless authorized under statute or policy.

5.6. Access to Personal Information will be restricted to only those employees requiring access in order to carry out their duties.

5.7. Records containing Personal Information shall not be removed from the workplace unless authorized under policy, statute or with manager approval. Any records containing Personal Information that are removed from, or access electronically outside of the workplace will be always secured. Store physical records in a secure location that you have sole access to and avoid leaving documents unattended when visible. External and mobile devices containing or accessing Personal Information will be kept secure.

5.8. In accordance with Section 34(1) of MFIPPA, the Board will make available a Personal Information Bank to assist the public in identifying and locating where their personal information is being kept, the legal authority of the collection, what is being collected and what it is being used for.

5.9. When implementing new programs or services, department heads must consider the impact on individuals' privacy and ensure that Personal Information is collected, used and managed in accordance with legal and regulatory requirements.

## 6. USE AND DISCLOSURE OF PERSONAL INFORMATION

The Board is permitted to use personal information:

6.1. If the individual has consented to the particular information to be used;

6.2. For the purpose of which it was obtained or compiled;

6.3. For a consistent purpose (i.e. the individual might reasonably expect the use);

6.4. For a purpose permitted by MFIPPA or other legislation; or

6.5. For the purpose for which the information was collected by the Board under MFIPPA.

**7.** The Board is only permitted to disclose personal information in the following circumstances:

7.1. In compliance with Part I of the Act – Right of Access, or other provisions of MFIPPA;

7.2. If the individual has consented to its disclosure;

7.3. For the purpose for which it was collected;

7.4. For a consistent purpose (i.e. the individual might reasonably expect the disclosure);

7.5. Disclosure is made to an employee, consultant or agent of the Board who needs the record in the performance of their duties, and if the disclosure is necessary and proper in the discharge of the Board's functions;

7.6. To comply with federal legislation or to assist a law enforcement agency in Canada to aid an investigation;

7.7. In compelling circumstances affecting personal health or safety or in compassionate circumstances ( to contact next of kin or friend of an injured, ill or deceased person);

7.8. To a provincial or federal government department for auditing of cost-shared programs; and

7.9. As specifically permitted by legislation.

The Board does not use or retain Personal Information provided for any secondary purposes unless the individual in questions has been notified and has provided permission to do so.

Board staff (employees, volunteers, agents, or contractors) shall take all reasonable measures to protect against theft, loss, unauthorized use, and mistaken disclosure of any Personal Information.

Every employee shall ensure that any records containing Personal Information are disposed of in a safe and secure manner and in accordance with the Board's policies and procedures and any relevant Acts.

## 8. PRIVACY BREACH GENERAL PROCEDURE

In the event of a Privacy Breach, the Board will take the following steps:

8.1. **Identify**

If a complaint is received or there is a suspicion that there is a Privacy Breach, contact the department supervisor who will contact the Board Secretary-Treasurer.

8.2. **Contain**

The first priority after a confirmed Privacy Breach is to contain the damage as much as reasonably expected. The Secretary-Treasurer will work with the necessary departments to identify the scope of the breach and will take steps to contain it by:

8.2.1. Retrieving any hard or electronic copies of Personal Information that has been disclosed;

8.2.2. Ensure there are no unauthorized duplicates or Personal Information

8.2.3. Prevent unauthorized access to more files by taking the necessary steps (such as changing keys, resetting passwords, suspend access, system shut down, etc.)

8.3. **Notify**

8.3.1. The Secretary-Treasurer will proceed to notify all individuals involved or affected by the breach via the most appropriate means related to the breach. The content will include the following information:

- Any relevant information surrounding the nature of the alleged, or confirmed breach;
- Details of the breach that are available at the time of notification;
- Specific areas that were affected;
- Procedures that are underway to contain, control and reduce the harm of the breach;
- Steps an individual should take to protect themselves;
- Future steps to prevent a similar incident; and
- Contact information about the Information Privacy Commissioner's Officer in case of further questions.

8.4. **Investigate**

8.4.1. Once the breach has been contained and all individuals notified, the Secretary- Treasurer will work to undertake an investigation to establish:

- The extent of damage of the Privacy Breach (sensitivity, number of individuals affected, etc.);
- The source of the breach, including future preventative measures, if able;
- A timeline of events that has led to the breach; and
- Any other relevant information relating to the circumstances, before or after.

8.4.2. The Secretary-Treasurer may report the breach to the Information Privacy Commissioner and, depending on the breadth of the damage, may

work in consultation with the Information Privacy Commissioner office to investigate.

8.5. **Report and Follow-Up**

8.5.1. Following the completion of the investigation, the Secretary-Treasurer may develop a report outlining the results of the investigation. This report will include recommended steps to prevent another breach for the future as well as steps on how to mitigate damage. The report will be forwarded to the Information Privacy Commissioner, individuals who were affected and to the Board.

8.5.2. Any recommendations within the report will be reviewed and implemented if appropriate.

8.5.3. The Secretary-Treasurer shall prepare an annual statistical report containing the number and general type of privacy breaches for the Board, if required.

8.6. **Privacy Complaints and Investigations**

8.6.1. Individuals may submit a complaint to the Information and Privacy Commissioner of Ontario (IPC) if they believe that the Board has improperly collected, used, disclosed or disposed of their personal information. The Board shall receive notice from the IPC in the event an individual has lodged a complaint, and an investigation is being undertaken.

## 9. APPROVAL

This policy is approved by resolution of the Mattawa Regional OPP Detachment Board and may be amended by majority vote at any official meeting of the Board.