



**Administrative policy concerning the rules of governance for the  
protection of personal information of the  
Municipality of Pontiac**

**REGULAR** meeting of the municipal council of the Municipality of Pontiac, held on May 13, 2025, at 7:30 p.m., at the Breckenridge Community Center located at 1491, Highway 148, Pontiac, at which meeting was present:

**THE MAYOR:** Roger Larose

**THE COUNCIL MEMBERS:**

Dr. Jean Amyotte

Diane Lacasse

Caryl McCann

Garry Dagenais

Serge Laforest

Some members of the council and forming a quorum.

**WHEREAS** the Municipality of Pontiac (hereinafter the “Municipality”) is a public body subject to the Act respecting access to documents held by public bodies and the protection of personal information, CQLR c. A-2.1 (hereinafter the “Access to Information Act”);

**WHEREAS** the Municipality is committed to protecting the personal information it collects and processes in the course of its activities, in accordance with applicable laws and regulations;

**WHEREAS** in 2022, the Municipality employed, on average, 50 employees or fewer, and is therefore not subject to the obligation to establish a committee on access to information and the protection of personal information pursuant to the Regulation exempting certain public bodies from the obligation to establish a committee on access to information and the protection of personal information;

**WHEREAS** in order to fulfill the obligations set out in the Access to Information Act, this administrative policy on governance rules regarding the protection of personal information is hereby established;

**THEREFORE**, the Council decrees as follows:

## CHAPTER I - APPLICATION AND INTERPRETATION

### 1. DEFINITIONS

For the purposes of this policy, the following expressions or terms shall have the meanings set forth below:

**CAI:** Refers to the Commission d'accès à l'information (Access to Information Commission) created under the Access to Information Act;

**Council:** Refers to the municipal council of the Municipality of Pontiac;

**Life Cycle:** refers to all the stages in the existence of information held by the municipality, specifically its creation, modification, transfer, consultation, transmission, retention, archiving, anonymization, or destruction;

**Access to Information Act:** Refers to the *Act respecting access to documents held by public bodies and the protection of personal information*, CQLR c. A-2.1;

**Concerned Individual:** Refers to any natural person whose personal information is collected, held, disclosed to a third party, destroyed, or anonymized by the Municipality;

**Stakeholder:** Refers to any natural person who is in a relationship with the Municipality in the context of its activities, including, without limiting the generality of the foregoing, an employee or a supplier;

**PRP Governance Policy:** Refers to the administrative policy concerning the governance rules regarding the protection of personal information of the Municipality;

**PRP:** Refers to the protection of personal information;

**Personal Information (or PI):** Refers to any information about a natural person that allows that person to be identified, directly or indirectly, such as mailing address, telephone number, email address, or bank account numbers, whether personal or professional data of the individual;

**Sensitive Personal Information (or Sensitive PI):** Refers to any personal information that gives rise to a high degree of reasonable expectation of privacy, particularly due to the potential harm to the individual in the event of a confidentiality incident, such as financial information, medical information, biometric data, social insurance number, driver's license number, or sexual orientation;

**Access to Documents Officer (or ADO):** Refers to the person who, in accordance with the *Access to Information Act*, performs this function and responds to requests for access to documents of the Municipality;

**Personal Information Protection Officer (or PIPO):** Refers to the person who, in accordance with the *Access to Information Act*, performs this function and ensures the protection of personal information held by the Municipality.

## 2. OBJECTIVES

The PRP Governance Policy aims to achieve the following objectives:

- To set out the orientations and guiding principles to effectively ensure the protection of personal information (PRP);
- To protect personal information (PI) collected by the Municipality throughout its entire life cycle;
- To ensure compliance with the legal requirements applicable to personal information protection, including the *Access to Information Act*, as well as best practices in this area;
- To maintain public trust in the Municipality, demonstrate transparency in the handling of personal information, explain the protection measures applied by the Municipality, and provide access when required.

## CHAPTER II - PRIVACY PROTECTION MEASURES

### 3. COLLECTION OF PERSONAL INFORMATION

- 3.1 The Municipality collects only the personal information (PI) necessary for the purposes of its activities;
- 3.2 Subject to the exceptions provided under the *Access to Information Act*, the Municipality does not collect PI without first obtaining the consent of the individual concerned;
- 3.3 It is understood that consent must be given for **specific purposes** and for the **duration necessary** to achieve those purposes. The consent of the individual concerned must be:
  - a) **Explicit:** meaning it is clear and certain;
  - b) **Freely given:** meaning it must be provided without coercion;
  - c) **Informed:** meaning it is given with full knowledge of the relevant facts.
- 3.4 At the time of collecting any PI, the Municipality ensures that it obtains the Individual's free, informed, and express consent. The Municipality must specifically indicate:

- a) The purposes for which the PI is required;
- b) Whether the request for PI is mandatory or optional;
- c) The consequences for the individual of refusing to provide the requested information;
- d) The consequences for the individual of withdrawing their consent to the communication or use of the PI following an optional request;
- e) The individual's rights of access to and rectification of the collected PI;
- f) The methods by which the PI is collected;
- g) Relevant details regarding (1) the Municipality's use of any technology to collect PI, including functions that enable identification, location tracking, or profiling of the individual, and (2) the options available to the individual to activate or deactivate such functions;
- h) Details regarding the retention period for any PI;
- i) The contact information of the person responsible for PI protection within the Municipality.

#### **4. RETENTION AND USE OF PERSONAL INFORMATION**

- 4.1. The Municipality restricts the use of any personal information (PI) to the purposes for which it was collected and for which the Municipality has obtained the express consent of the individual concerned, subject to the exceptions provided under the *Access to Information Act*;
- 4.2. The Municipality limits access to any PI it holds to only those individuals whose access is required for the performance of their duties within the Municipality;
- 4.3. The Municipality applies equivalent security measures regardless of the sensitivity of the PI it holds, in order to prevent breaches of its confidentiality and integrity, subject to the exceptions provided under the *Access to Information Act*;
- 4.4. The Municipality retains data and documents containing PI:

- a) For the duration necessary for the use for which they were obtained  
Or
  - b) In accordance with the timeframes set out in its records retention schedule.
- 4.5. When using any PI, the Municipality ensures the accuracy of the PI. To do so, it regularly validates its accuracy with the individual concerned and, if necessary, at the time of its use;
- 4.6. The Municipality applies the same high standard of reasonable expectation of protection for confidentiality and integrity to all PI it collects, retains, and uses, whether the PI is sensitive or not.

## **5. PERSONAL INFORMATION FILE**

The Municipality establishes and maintains an up-to-date inventory of its personal information files.

This inventory must include the following information:

- 5.1 The designation of each file, the categories of information it contains, the purposes for which the information is retained, and the management method for each file;
- 5.2 The source of the information entered into each file;
- 5.3 The categories of individuals concerned by the information contained in each file;
- 5.4 The categories of individuals who have access to each file in the performance of their duties;
- 5.5 The security measures taken to ensure the protection of personal information.

Any person who makes a request has the right to access this inventory, except with respect to information whose existence may be denied in accordance with the provisions of the *Access to Information Act*.

## **6. DISCLOSURE TO THIRD PARTIES**

- 6.1. The Municipality may not disclose any personal information (PI) to third parties without the express consent of the individual concerned, except in cases provided for by the *Access to Information Act*;

- 6.2. The Municipality records in the registers required by the *Access to Information Act* all information related to the transmission of any PI to a third party, regardless of the purpose.

## **7. DESTRUCTION OR ANONYMIZATION**

- 7.1. When PI is no longer necessary for the purposes for which it was collected and the retention period specified in the records retention schedule has expired, the Municipality must irreversibly destroy the PI or render it anonymous;
- 7.2. The destruction procedure must be approved by the Clerk-Treasurer and the Personal Information Protection Officer (PIPO) to ensure, among other things, compliance with section 199 of the *Municipal Code*;
- 7.3. The anonymization must serve a serious and legitimate purpose, and the process must be irreversible;
- 7.4. Upon the recommendation of the PIPO, any anonymization procedure must be approved by the Clerk-Treasurer.

## **CHAPITRE III - ROLES AND RESPONSIBILITIES WITH REGARD TO THE PROTECTION OF PERSONAL INFORMATION**

### **8. COUNCIL**

The Council approves this Policy and ensures its implementation, in particular by:

- 8.1 Making the necessary decisions within its jurisdiction to implement and enforce this Policy;
- 8.2 Ensuring that the Municipality's General Management and Department Directors promote an organizational culture based on the protection of PI and foster behaviours that prevent any confidentiality incidents;
- 8.3 Ensuring that the PIPO and the ADO can independently exercise their powers and responsibilities.

### **9. GENERAL MANAGEMENT**

General Management is responsible for the quality of PI protection management and the use of all technological infrastructure of the Municipality for this purpose.

In accordance with the *Regulation exempting certain public bodies from the obligation to establish a committee on access to information and the protection of personal information* (Decree 744-2023, May 3, 2023), General Management assumes the responsibilities normally assigned to the Committee on Access to Information and the Protection of Personal Information:

- 9.1 Defining and approving the governance rules related to PI protection within the Municipality;
- 9.2 Defining and approving the orientations related to PI protection within the Municipality;
- 9.3 Providing guidance on initiatives involving the acquisition, deployment, or redesign of information systems, or any new electronic service delivery by the Municipality that involves the collection, use, retention, disclosure to third parties, or destruction of PI—both at the implementation stage and when these initiatives are modified.

General Management must also implement this Policy by:

- a) Ensuring that the PIPO and ADO can independently exercise their powers and responsibilities;
- b) Ensuring that PI protection values and orientations are shared and promoted by all managers and employees of the Municipality;
- c) Planning and delivering training activities for Municipal employees on PI protection;
- d) Ensuring that the Municipality is aware of the orientations, directives, and decisions issued by the CAI regarding PI protection;
- e) Evaluating the level of PI protection within the Municipality;
- f) Providing the necessary financial and logistical support to implement and uphold this Policy;
- g) Exercising investigative authority and applying appropriate sanctions depending on the circumstances in cases of non-compliance with this Policy.

## **10. PERSONAL INFORMATION PROTECTION OFFICER**

The PIPO, in collaboration with the ADO, helps ensure sound management of PIP within the Municipality. The PIPO supports the Council, General Management, and all Municipal staff in implementing this Policy.

Specifically, the PIPO is responsible for:

- 10.1 Defining, in collaboration with General Management, the orientations related to PIP within the Municipality;
- 10.2 Determining the types of PI to be collected by the various Municipal departments, as well as their retention, disclosure to third parties, and destruction;
- 10.3 Recommending necessary adjustments in the event of amendments to the *Access to Information Act*, its related regulations, or court interpretations, as applicable;
- 10.4 Planning and ensuring, in collaboration with General Management, the delivery of training activities for Municipal employees regarding PIP;
- 10.5 Providing General Management with guidance on initiatives involving the acquisition, deployment, or redesign of information systems or any new electronic service delivery by the Municipality that requires the collection, use, retention, disclosure to third parties, or destruction of PI, both at the launch and during any subsequent modification of such initiatives;
- 10.6 Advising on specific measures to be observed for surveys that collect or use PI, and on matters relating to video surveillance;
- 10.7 Ensuring that the Municipality is aware of the orientations, directives, and decisions issued by the CAI regarding PIP;
- 10.8 Evaluating, in collaboration with General Management, the level of PIP within the Municipality;
- 10.9 Recommending to the Clerk-Treasurer the anonymization of PI instead of its destruction, where the information is no longer useful to the Municipality;
- 10.10 Reporting annually to the Council and General Management on the application of this Policy.

## **11. ACCESS TO DOCUMENT OFFICER**

As part of this role, the officer must:



- 11.1 Receive all requests related to access to documents under the *Access to Information Act*, including requests for information;
- 11.2 Respond to requests for access to documents in accordance with the provisions of the *Access to Information Act*.

## **12. DEPARTMENT DIRECTOR**

Each department director is responsible for ensuring PI protection within the department they lead, as well as managing the technological infrastructure necessary for this purpose, which is accessible to both the department's employees and the director as part of their duties within the Municipality.

In this regard, each department director must:

- 12.1 Ensure that the employees in their department are familiar with this PI protection policy and ensure its application and compliance;
- 12.2 Ensure that the security measures determined and implemented are systematically applied in the course of their work and that of the employees under their supervision in the department they are responsible for;
- 12.3 Participate in raising awareness among each employee in their team about PI protection issues;
- 12.4 Appoint one or more employees within their department whose duties specifically include ensuring the collection, retention, storage, or destruction of PI and its protection;
- 12.5 If no employee is designated, the department director assumes the tasks and responsibilities outlined in section 13.

## **13. PERSON RESPONSIBLE FOR PI PROTECTION WITHIN THE MUNICIPALITY'S DEPARTMENTS**

Each department director within the Municipality must identify the person responsible for PI protection in their department to the PIPO. The employees designated in each department are responsible for certain stages of the PI lifecycle within their department, namely collection and retention.

Each person responsible within the department works closely with the PIPO to inventory the various categories of personal information collected, retained, disclosed to third parties

(if applicable), destroyed, or anonymized, and to keep this inventory up to date. The responsible person must also ensure that department employees obtain any necessary consent from individuals to collect, retain, or transfer personal information to third parties, as appropriate. The responsible person must ensure that the collected consents are stored and organized so that they can be easily traced.

#### **14. EMPLOYEES**

Each employee must:

- 14.1 Take all necessary measures to protect PI;
- 14.2 Make every effort to comply with the applicable legal framework and the measures outlined in the Municipality's various policies and guidelines related to PI protection;
- 14.3 Access only the PI necessary for the performance of their duties;
- 14.5 Report any confidentiality incidents or irregular handling of PI to the PIPO;
- 14.6 Actively participate in any awareness or training activities related to PI protection;
- 14.7 Collaborate with the PIPO and ADO.

#### **15. TRAINING OF MUNICIPALITY STAFF ON PERSONAL INFORMATION PROTECTION**

The RPRP and/or the general management establishes the content and selection of training offered to all Municipality employees and determines the frequency at which employees must undergo the established training.

The training or awareness activities include, in particular:

- 15.1 Training upon hiring on the importance of protecting personal information (PRP) and the appropriate actions to take in the course of their duties;
- 15.2 Training for all employees on the implementation of this policy;
- 15.3 Training for employees using new computer tools involving personal information;
- 15.4 Training on updates to this policy or security measures for personal information, as applicable.

## **CHAPTER IV - ADMINISTRATIVE MEASURES**

### **16. SURVEYS**

Before conducting, or allowing a third party to conduct, a survey of individuals for whom the Municipality holds, collects, or uses PI, the RPRP must first evaluate the following:

- 16.1 The necessity of conducting the survey;
- 16.2 The ethical aspect of the survey, particularly considering the sensitivity of the personal information collected and the purpose for which it is used.

Following this evaluation, the RPRP must make recommendations to the council and the general management.

### **17. ACQUISITION, DEVELOPMENT, OR REVAMPING OF AN INFORMATION SYSTEM OR ELECTRONIC SERVICE DELIVERY**

- 17.1. Before proceeding with the acquisition, development, or revamping of personal information management systems, the Municipality must conduct a privacy impact assessment;

For this assessment, the Municipality must consult, from the outset of the project, with general management;

- 17.2. As part of the implementation of the project described in Section 17.1, general management may, at any stage, suggest PI protection measures, including but not limited to:
  - a) The appointment of a person responsible for implementing privacy protection measures;
  - b) PI protection measures in any document related to the project, such as a specification document or contract;
  - c) A description of the responsibilities of project participants regarding PI protection;
  - d) Conducting training on PI protection for project participants.

- 17.3. The Municipality must also ensure that, as part of the project described in Section 17.1, the personal information management system allows for any computerized PI collected from the concerned individual to be communicated to them in a structured, commonly used technological format;

- 17.4. Conducting a privacy impact assessment must be proportional to the sensitivity of the information concerned, the purpose for which it is used, its quantity, its distribution, and its medium.

## **18. CONFIDENTIALITY INCIDENTS**

The unauthorized access, use, disclosure, or loss of any PI constitutes a confidentiality incident within the meaning of the *Access to Information Act*.

The Municipality manages all confidentiality incidents in accordance with its incident management procedure, which includes the following rules:

:

- 18.1 Any confirmed or potential confidentiality incidents must be reported as soon as possible to the RPRP by any person who becomes aware of it;
- 18.2 The RPRP must review the reported information to determine whether it qualifies as a confidentiality incident and, if so:
  - a) Enter the relevant information in the Municipality's confidentiality incident registry;
  - b) Notify the CAI and any individuals affected by the confidentiality incident;
  - c) Identify and recommend the implementation of appropriate mitigation measures, if necessary.

## **19. HANDLING OF COMPLAINTS**

Any individual who believes that the Municipality is not protecting PI in accordance with the *Access to Information Act* may file a complaint as follows:

- 19.1. A complaint will only be considered if it is submitted in writing by an identified individual;
- 19.2. Such a request must be addressed to the Municipality's RPRP;
- 19.3. The RPRP shall notify the complainant in writing of the date the complaint was received and indicates the timeline for a response;
- 19.4. The RPRP shall address the complaint diligently and no later than twenty days after its receipt;

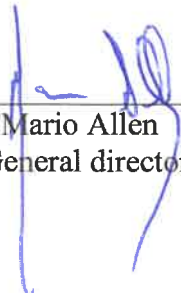
- 19.5. If it appears impossible to process the complaint within the time limit set out in Article 19.4 without interfering with the normal operations of the Municipality, the RPRP may, before the expiry of the initial period, extend the deadline by a reasonable period and shall inform the complainant by any means of communication capable of reaching them;
- 19.6. In processing the complaint, the RPRP may contact the complainant and conduct an internal investigation;
- 19.7. Upon completing the review of the complaint, the RPRP shall send the complainant a final written and reasoned response;
- 19.8. If the complainant is not satisfied with the response or the handling of the complaint, they may contact the CAI in writing.

## **20. SANCTIONS**

Any employee of the Municipality who violates this Policy or applicable laws and regulations related to PI protection is subject, in addition to legal penalties, to disciplinary action, which may include disciplinary measures up to and including dismissal. General management, in consultation with the Human Resources Department, is responsible for determining whether disciplinary action is appropriate. The Municipality may also forward to any judicial authority the information collected about an employee if there is reason to believe that a violation of applicable PI protection laws or regulations has occurred.

## **21. FINAL PROVISION**

This Policy comes into effect on May 13, 2025, following the decision of the Council and resolution 25-05-5583.

  
\_\_\_\_\_  
Roger Larose  
Mayor  
\_\_\_\_\_  
Mario Allen  
General director