ADMINISTRATIVE POLICY CONCERNING THE RULES OF GOVERNANCE IN MATTERS OF PROTECTION OF PERSONAL INFORMATION OF THE MUNICIPALITY OF THE TOWNSHIP OF WENTWORTH

CHAPTER I — APPLICATION AND INTERPRETATION

1. DEFINITIONS

For the purposes of this policy, the following expressions or terms shall have the meaning below:

CAI: Refers to the « **C**ommission d'**a**ccès à l'**i**nformation » created under the *Act respecting access*;

Council: Refers to the Municipal Council of the Municipality of the Township of Wentworth;

Life cycle: Refers to all the stages in the existence of information held by the Municipality, and more specifically its creation, modification, transfer, consultation, transmission, holding, archiving, anonymization or destruction;

Act respecting access: Refers to the *Act respecting access to documents held by public bodies and the protection of personal information*, RLRQ c. A -2,1;

Person concerned: Refers to any individual for whom the Municipality collects, holds, communicates to a thirs party, destroys or anonymizes personal information;

Related party: Refers to a natural person in a relationship with the Municipality in the course of its activities and, without limiting the generality of the foregoing, an employee or supplier;

PPI Governance Policy: Refers to the administrative policy concerning the Municipality's rules of governance with respect to the protection of personal information;

PPI : Refers to the protection of personal information;

Personal information (or PI) : Refers to any information concerning a natural person that enables that person to be identified directly or indirectly, such as a postal address, telephone number, e-mail address or bank account number, whether the data is personal or professional;

Sensitive personal information (or PI): Refers to any personal information that raises a high reasonable expectation of privacy for any individual, particularly because of the potential prejudice to the individual in the event of a condifentiality incident, such as financial information, medical information, biometric data, social insurance number, driver's license number or sexual orientation;

Responsible for access to documents (or RAD) : Refers to the person in charge who, in accordance with the *Act respecting access*, performs this function and responds to requests for access to the Municipality's documents;

Responsible for the protection of personal information (or RPPI) : Refers to the person in charge who, in accordance with the *Act respecting access*, performs this function and ensures the protection of personal information held by the Municipality.

2. OBJECTIVES

The PPI Governance Policy has the following objectives:

- Set out the orientations and guiding principles intended to effectively ensure PPI;
- To protect the PI collected by the Municipality throughout its life cycle;
- Ensure compliance with legal requirements applicable to PPI, including the *Act respecting access*, and with the best practices in this field;
- Ensure public confidence in the Municipality, demonstrate transparency regarding the processing of PI and the PPI measures applied by the Municipality, and provide access when required.

CHAPTER II — PERSONAL INFORMATION PROTECTION MEASURES

3. COLLECTION OF PERSONAL INFORMATION

3.1. The Municipality only collects PI necessary for the purposes of its activities.

3.2. Subject to the exceptions set out in the *Act respecting Access*, the Municipality will not collect PI without first obtaining the consent of the person concerned.

3.3. It is agreed that consent is given for **specific purposes**, for a **necessary period of time** to achieve the purposes for which it is requested. The person's consent must be :

a) **Manifest**: meaning that it is obvious and certain;
b) **Free**: meaning that is must be free of constraints;
c) **Enlightened**: meaning that it is made with full knowledge of the facts.

3.4. At the time of collection of any PI, the Municipality shall expressly obtain the free and informed consent of the person concerned. In particular, the Municipality must indicate:

- The purposes for which any PI is required;
- The mandatory or optional nature of the request to collect PI;
- The consequences for the person concerned of refusing to respond to the request;
- The consequences for the person concerned of withdrawing consent to the communication of use of PI following an optional request;
- Rights of access and rectification of collected PI;
- The means by which any PI is collected;
- Necessary details regarding (1) the use by the Municipality of a technology to collect any PI, including functions that allow the identification, location or profiling of the person concerned and (2) the means offered to the person concerned to activate or deactivate the functions;
- Details of the safekeeping period of any PI;

- The contact details of the person responsible for PPI within the Municipality.

4. SAFEKEEPING AND USE OF PERSONAL INFORMATION

4.1. The Municipality restricts the use of any PI to the purposes for which itw as collected and for which the Municipality has obtainted the express consent of the person concerned, subject to the exceptions set out in the *Act respecting access*.

4.2. The Municipality limits access to any PI held to those persons for whom said access is required to perform their duties within the Municipality.

4.3. The Municipality applies equivalent security measures, regardless of the sensitivity of the PI held, in order to prevent breaches of confidentiality and integrity, subject to the exceptions provided for in the *Act respecting access*.

4.4. The Municipality shall keep information and documents containing PI:

a) For the necessary period of time for the use for which they were obtained

or

b) In accordance with its safekeeping schedule.

4.5. When using any PI, the Municipality ensures that the PI is accurate. To this end, it validates its accuracy with the person concerned on a regular basis and, if necessry, at the time of use.

4.6. The Municipality shall provide the same high level of reasonable expectation of protection, in terms of confidentiality and integrity, for any PI it collects, safekeeps and uses, whether the PI is sensitive or not.

5. PERSONAL INFORMATION FILE

The Municipality establishes and maintains a register of its personal information files.

This register must contain the following information:

a) the designation of each file, the categories of information it contains, the pruposes for which the information is kept and the management method for each file;

b) the origin of the information in each file;

c) the categories of persons concerned by the information contained in each file;

d) the categories of persons who have access to each file in the performance of their duties;

e) the security measures taken to ensure the protection of personal information.

Any person who requests it has a right of access to this register, except for information whose existence may be refused under the provisions of the *Act respecting access*.

6. DISCLOSURE TO THIRD PARTIES

6.1. The Municipality may not disclose any PI to third parties without th express consent of the person concerned, except as provided for in the *Act respecting access*.

6.2. The Municipality shall indicate, in the registers required by the *Act respecting access*, all information relating to the transmission of any PI to a third party for any purposes whatsoever.

7. DESTRUCTION OU ANONYMISATION

7.1. When PI is no longer required for the purposes for which it was collected, and when the period specified in the safekeeping schedule has expired, the Municipality must irreversibly destroy it or render it anonymous.

7.2. The destruction procedure must be approved by the Clerk-Treasurer and the RPPI to ensure compliance with Section 199 of the *Municipal Code.*

7.3. Anonymization serves a serious and legitimate purpose, and the procedure is irreversible.

7.4. On the recommendation of the RPPI, any anonymization procedure must be approved by the Clerk-Treasurer.

CHAPTER III — ROLES AND RESPONSIBILITIES WITH REGARD TO THE PROTECTION OF PERSONAL INFORMATION

8. COUNCIL

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

a) Take the necessary decisions within its jurisdiction to ensure the implementation of and compliance with this Policy;

b) That the Municipality's general management and department directors promote an organizational culture based on the protection of PI and the necessary behaviours to avoid any confidentiality incidents;

c) That the RPPI and RAD are able to exercise their powers and responsibilities autonomously.

9. GENERAL MANAGEMENT

The General Management is responsible for the qulity of PPI management and for the use of all the Municipality’s technological infrastructure for this purpose.

In this regard, it must implement this present Policy by:

a) Ensuring that the RPPI and RAD can exercise their powers and responsibilities autonomously;

b) Ensuring that PPI values and orientations are shared and conveyed by all managers and employees of the Municipality;

c) Providing the necessary financial and logistical support for the implementation of and compliance with this Policy;

d) Exercising its investigative powers and applying sanctions appropriate to the circumstances for non-compliance with this Policy.

10. RESPONSIBLE FOR THE PROTECTION OF PERSONAL INFORMATION

The RPPI, in collaboration with the RAD, contributes to ensuring sound management of the PPI within the Municipality. It supports the Council, General Management and all municipal staff in implementing this Policy. In accordance with the *By-Law excluding certain public bodies from the obligation to form a committee on access to information and the protection of personal information* (Decree 744-2023, May 3rd, 2023), the PPI assumes the duties and obligations of the Committee on Access to Information and the Protection of Personal Information provided for in section 8.1 of the *Act respecting access*.

Namely, the RPPI ensures:

a) Defining and approving PPI orientations within the Municipality;

b) Determining the type of PI to be collected by the various departments of the Municipality, its safekeeping, communication to third parties and destruction;

c) Suggesting the necessary adaptations in the event of amendments to the *Act respecting access*, its related regulations or the interpretation of the courts, as the case may be;

d) Planning and carrying out PPI training activities for municipal employees;

e) Formulating opinions on initiatives for the acquisition, deployment and redesign of information systems or any new electronic delivery of services by the Municipality requiring the collection, use, safekeeping, communication to third parties or destruction of PI, both at the time of implementation of these initiatives and at the time of any modification thereto;

f) Formulating on special measures to be taken for surveys that collect or use PI, or for video surveillance;

g) Ensuring that the Municipality is aware of the orientations, directives and decisions formulated by the CAI with regard to PPI;

h) Evaluating the level of PPI within the Municipality;

i) Recommending that the Clerk-Treasurer proceed with the anonymization of PI rather than destroying PI that is no longer useful to the Municipality;

j) Reporting annually to the Council and General Management on the application of this Policy.

11. RESPONSIBLE FOR ACCESS TO DOCUMENTS

In the course of this function, the Responsible of conformity must:

a) Receive all requests that are in the nature of a request for access to documents withing the meaning of the *Act respecting access*, including requestes for information;

b) Respond to requestes for access to documents in accordance with the requirements of the *Act respecting access*.

12. DEPARTMENT DIRECTOR

Each department director is responsible for ensuring PPI within the department he/she leads, as well as for the technological infrastructures required for this purpose, to which he/she and the department's employees have access as part of their duties at the Municipality.

As such, each department director must:

a) Communicate this PPI Policy to employees in his/her department and ensure its application and compliance by them;

b) Ensure that the safety measures determined and implemented are applied systematically in the course of his/her employment and that of the employees he/she manages in the department for which he/she is responsible;

c) Participate in raising the awareness of each employee on his/her team about PPI issues;

d) Designate, within its department, the employee(s) whose duties specifically include overseeing the collection, safekeeping, retention or destruction of PI and its protection;

e) In the absence of a designated employee, the department director assumes the duties and responsibilities set out in Article 13.

13. RESPONSIBLE FOR PPI IN THE DIFFERENT DEPARTMENTS OF THE MUNICIPALITY

Each department director of the Municipality must identify the person responsible for PPI within his/her department at the RPPI. The employees of each department of the Municipality thus designated are responsible within their department for certain stages in the life of PPI, i.e. collection and safekeeping.

Each person in charge within the above-mentioned departments works closely with the RPPI to compile and maintain an up-to-date register of the various categories of personal information collected, held, transferred to third parties, destroyed or anonymized, as the case may be. The person in charge must also ensure that the department's employees obtain any consent required from any individual for the purposes of collecting, holding or transferring to third parties, as the case may be. The person in charge must ensure that all consents collected are kept and filed in such a way that they can be easily traced.

14. EMPLOYEES

Each employee must:

a) Take all necessary measures to protect PI;

b) Make every effort to comply with the applicable legal framework and the measures set out in the Municipality's various policies and directives relating to the protection of PI;

c) Only access PI that is necessary for the performance of its duties;

d) Report any incidents of confidentiality or irregular processing of PI to the RPPI;

e) Participate actively in any awareness-raising or training activities relating to PPI;

f) Collaborating with the RPPI and RAD.

15. TRAINING FOR MUNICIPAL STAFF TRAINING REGARDING THE PROTECTION OF PERSONAL INFORMATION

The RPPI establishes the content and choice of training offered to all employees of the Municipality, and determines the frequency with which employees must attend any established training.

Training or awareness-raising activities include, namely:

For example:

- Hiring training on the importance of the PPI and the actions to be taken on the job;
- Training for all employees on the implementation of this Policy;
- Training on updates to this Policy or PPI safety measures where applicable.

CHAPTER IV — ADMINISTRATIVE MEASURES

16. SURVEYS

Before conducting, or allowing a third party to conduct a survey towards persons concerned for whom the Municipality holds, collects or uses PI, the RPPI must first evaluate the following points:

- the need to conduct a survey;
- the ethical aspect of the survey, particularly in light of the sensitivity of the personal information collected and the purpose for which it will be used.

Following this evaluation, the RPPI will make recommendations to the Council and General Manager.

17. ACQUISITION, DEVELOPMENT OR RESTRUCTURING OF AN ELECTRONIC INFORMATION OR SERVICE SYSTEM

17.1. Before proceeding with the acquisition, development or restructuring of PI management systems, the Municipality must carry out a privacy impact evaluation.

For the purposes of this evaluation, the Municipality must consult its RPPI at the very beginning of the project.

17.2. As part of the implementation of the project provided for in Article 17.1, the RPPI may, at any stage, suggest measures to protect PI, including in particular:

a) the nomination of a person responsible for the implementation of PPI measures;

b) PPI mesures in any project document, such as a specification or contract;

c) a description of the PPI responsibilities of project participants;

d) PPI training activities for project participants.

17.3. The Municipality must also ensure that, as part of the project provided for in Article 17.1, the personal information management system allows a computerized PI collected from the person concerned to be communicated to the latter in a structured and commonly used technological format.

17.4. The conduct of a privacy impact evaluation shall be proportionate to the sensitivity of the information concerned, the purpose for which it is to be used, its quantity, distribution and medium.

18. CONFIDENTIALITY INCIDENTS

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

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

- Any actual or potential confidentiality incident must be reported as soon as possible to the RPPI by anyone who becomes aware of it;
- The RPPI must review the reported information to determine if it is a confidentiality incident and if so:
  - Enter relevant information in the Municipality's confidentiality incident register;
  - Notify the CAI and anyone else involved in the confidentiality incident;
  - Identify and recommend the application of appropriate mitigation measures, where necessary.

19. HANDLING COMPLAINTS

Any individual who considers that the Municipality does not ensure the protection of PI in accordance with the *Act respecting access* may file a complaint in the following manner:

19.1. A complaint can only be considered if it is made in writing by a natural person who identifies him/herself.

19.2. Such a request is addressed to the RPPI of the Municipality.

19.3. The RPPI notifies the complainant in writing of the date on which the complaint is received and indicates the deadlines for dealing with the complaint.

19.4. The RPRP will respond diligently to a complaint and no later than twenty days from the date of receipt.

19.5. If it appears impossible to deal with the complaint within the time limit set out in section 19.4 of this Policy without interfering with the normal conduct of the Municipality's activities, the RPRP may, before the expiry of this time limit, extend it for a reasonable period of time and notify the complainant, by any means of communication by which the latter can be reached.

19.6. As part of the complaint process, the RPRP may contact the complainant and conduct an internal investigation.

19.7. Once the complaint has been examined, the RPPI will send the complainant a final written response, with reasons.

19.8. If the complainant is not satisfied with the response or handling of his/her complaint, he/she may write to the CAI.

20. PENALTIES

Any employee of the Municipality who contravenes the present Policy or the laws and regulations in force applicable to PPI is liable, in addition to the penalties provided for by law, to disciplinary action, which may include dismissal. General Management, in conjunction with the Human Resources Department, is responsible for deciding whether or not to apply the appropriate sanction. The Municipality may also forward to any judicial authority any information gathered on any employee which leads it to believe that a breach of any law or regulation in force relating to PRP has been committed.

21. FINAL PROVISION

The present Policy comes into effect upon adoption by the Council.

Jason Morrison Mayor	Natalie Black General Manager, Clerk-Treasurer

Adoption of the Policy: November 6th, 2023