



CITY PROCEDURE

Safeguarding Personal Information

Procedure Title	Safeguarding Personal Information		
Procedure Number	507-5	Approved Date	2026-07-16
Department	Legislative and Legal Services	Last Amended	2026-10-06
City Manager Signature	"S. Bourke" (signed)	Last Reviewed	2026-10-06
		Signature Date	2026-10-09

1. Purpose:

- 1.1. The purpose of this procedure is to establish processes for safeguarding Personal Information in the custody and control of the City in accordance with Provincial Privacy Legislation and City policies.

2. Scope

- 2.1. This procedure applies to all Employees involved in the collection, access, Use, storage or Disclosure of Personal Information.

3. Definitions

The definitions in **Policy 507 Privacy Management** apply to this procedure. In addition, in this procedure:

- 3.1. **"Destroy"** means the permanent destruction of all copies of a Record so that they cannot reasonably be reconstructed or retrieved (such as by shredding, pulping or secure digital deletion).
- 3.2. **"Disclosure"** means to release, transmit, reveal, expose, show, provide copies of, verbally state the contents of or give Personal Information by any other means to someone. It includes oral transmission or information by telephone, or in person; provision of Personal Information on paper, by facsimile or in any other format; and electronic transmission through electronic mail, data transfer or the internet.
- 3.3. **"Department Head"** means the senior Employee in the highest level of authority of a department.
- 3.4. **"GIS and ITS"** means the City's GIS and ITS Department, responsible for maintaining and safeguarding the City's information technology systems.
- 3.5. **"Privacy Coordinator"** means the position responsible for operational administration, carrying out the powers, duties and functions related to Provincial Privacy Legislation that are delegated to the Privacy Coordinator by the City Manager.
- 3.6. **"Supervisor"** means the person in the City who is immediately responsible for or in charge of the Employee.



CITY PROCEDURE

Safeguarding Personal Information

- 3.7. **"Use"** means employing Collected information to accomplish the City's purposes such as using the information to administer a program or activity, provide a service or determine eligibility for a benefit. Access to a file or database by program staff or contract agent constitutes "use" as defined under POPA.

4. Procedure & Guidelines

4.1. Classification of Personal Information

- 4.1.1. All Personal Information is classified Confidential unless this section provides otherwise. Classification is applied at the time of Collection or creation and reviewed where the sensitivity or Use of the information changes.
- 4.1.2. Personal Information is classified using the following levels:
- a. **Restricted**
 - i. Personal Information whose loss or unauthorized access or Disclosure could result in significant harm to an individual, including Personal Information of high sensitivity (such as financial or biometric information, or information about minors or other vulnerable individuals), law enforcement and investigation information, and any Personal Information designated Restricted by a Privacy Impact Assessment.
 - ii. Access is limited to individuals specifically authorized
 - b. **Confidential**
 - i. All other Personal Information. This is the default classification.
 - ii. Access is limited to Employees who require the information to perform their duties.
 - c. **Public**
 - i. Personal Information that is publicly available or that has been approved for active dissemination (for example, the names of members of Council).
 - ii. No confidentiality restrictions apply, but accuracy, integrity and Records management requirements continue to apply.
- 4.1.3. Where the appropriate classification is unclear, Employees must apply the higher classification under consideration and consult the Privacy Coordinator for final determination.
- 4.2. **Apply Safeguards**
- 4.2.1. Department Heads must ensure their departments apply administrative, physical and technical safeguards that are appropriate and proportional to the classification level of the Personal Information in their custody or control, for example:
- a. Physical safeguards (e.g., locked storage, restricted access areas);
 - b. Technical safeguards (e.g., access controls, encryption, and storage and transmission methods approved by GIS and ITS); and



CITY PROCEDURE

Safeguarding Personal Information

- c. Administrative safeguards (e.g., standard operating procedures, training and oversight).

4.2.2. Department Heads must ensure safeguards are reviewed at least annually and following any Privacy Incident affecting their department.

4.2.3. Safeguards must protect Personal Information throughout its lifecycle, from Collection to destruction or transfer.

4.3. Control Access

4.3.1. Access to Personal Information must be limited to Employees who require it to perform their duties, and only to the extent necessary to enable the City to carry out its purpose in a reasonable manner.

4.3.2. Supervisors must ensure access is granted on the basis of role and documented authorization, and that access credentials are not shared.

4.3.3. Supervisors must ensure access permissions are removed or updated, with the support of GIS and ITS, when an Employee's role changes or employment ends.

4.4. Secure Handling and Storage

4.4.1. Employees must store Personal Information in systems or locations that meet the safeguards for its classification level. Systems used to store Personal Information must be approved by GIS and ITS.

4.4.2. Employees must not make or retain copies of Personal Information beyond what is necessary to perform their duties.

4.4.3. Employees must protect Personal Information against such risks as unauthorized access, collection, Use, Disclosure or destruction.

4.5. Transmission

4.5.1. The authority to Disclose Personal Information is governed by the [Collection, Use and Disclosure Procedure \(507-1\)](#) and the [Access to and Correction of Personal Information Procedure \(507-2\)](#). This section governs how Personal Information is transmitted once a Disclosure or transfer is authorized, and Employees must not transmit Personal Information externally except under an authorized Disclosure or transfer.

4.5.2. Employees must send Personal Information only by a method approved for its classification level, as set out in [Schedule "A"](#) to this procedure.

4.5.3. Before transmitting, Employees must confirm the identity of the intended recipient and the accuracy of the address, number or account being used.

4.5.4. This section does not prevent an authorized oral Disclosure, provided the Employee takes appropriate care to prevent Disclosure to any person other than the intended recipient.



CITY PROCEDURE

Safeguarding Personal Information

4.6. Retention and Disposition

- 4.6.1. Personal Information must be retained in accordance with the **Records Management Bylaw C-1348**, POPIA (including the one-year retention requirement for Personal Information Used to make a decision that directly affects an individual) and any applicable City policies or procedures.
- 4.6.2. Personal Information must be Destroyed using methods approved under the City's Records management program when retention requirements have been met, and must not be Destroyed while it is subject to a legal hold, an outstanding access or correction request, or the retention requirement in section 4.6.1.

4.7. Privacy Incident Reporting

- 4.7.1. Employees must report any suspected or confirmed Privacy Incident to the Privacy Coordinator without unreasonable delay and follow the **Privacy Incident Response and Notification Procedure (507-6)**.

4.8. Training and Assistance

- 4.8.1. Employees must complete the privacy and information security training required for their role.
- 4.8.2. An Employee who is uncertain how to safeguard Personal Information must consult the Privacy Coordinator.

5. Roles and Responsibilities

- 5.1. The City Manager will review and approve this procedure and any amendments.
- 5.2. Employees will comply with this procedure.
- 5.3. Supervisors approve and manage Employee access to Personal Information within their areas of responsibility, including ensuring access is removed or updated on role change or departure.
- 5.4. The Privacy Coordinator coordinates privacy training and awareness activities and maintains records of training completion.
- 5.5. Departments must consult GIS and ITS before implementing a system or technical safeguard involving Personal Information.

6. Attachments

- 6.1. See **Schedule "A"**, Approved Methods for Sending Personal Information



CITY PROCEDURE

Safeguarding Personal Information

7. Version History

Action	Date	Description
New Procedure	2026-07-16	
Amendment	2026-10-06	Addition of Schedule "A" and reference to it added to 4.5.2.



CITY PROCEDURE

Safeguarding Personal Information

Schedule "A": Approved Methods for Sending Personal Information

1. How to Use

- 1.1. Find the sensitivity level of what you are sending, then use a method marked "Yes".
- 1.2. Whatever method you use:
 - 1.2.1. Check the address, number or recipient before you send.
 - 1.2.2. Send only what the recipient needs or has requested.
 - 1.2.3. Share information only with individuals who have a need to know.
 - 1.2.4. If it goes to the wrong person, follow the process set out in [City Procedure 507-6](#).

2. Classification

- 2.1. **Restricted:** Health, financial, biometric or law enforcement information, and information about children or vulnerable people.
- 2.2. **Confidential:** All other personal information. This is the default.
- 2.3. **Public:** Personal information that is already public or approved for release.

Method	Restricted	Confidential	Public
City-issued email to a person you have confirmed	Yes	Yes	Yes
City-managed cloud collaboration platforms (OneDrive, SharePoint, Teams) shared with a person you have confirmed	Yes	Yes	Yes
SMS text to a person you have confirmed	Yes	Yes	Yes
A link from those platforms that is open to anyone with the link	No	No	Yes
Mail, courier, or hand delivery in a sealed envelope to a confirmed address	Yes	Yes	Yes
In person or by telephone, after confirming who you are speaking to	Yes	Yes	Yes
Fax to a number you have confirmed	Yes	Yes	Yes
Personal email, personal cloud storage, messaging apps, or a USB drive not issued by the City	No	No	Yes
Posting or publishing publicly — website, social media, open data, or other publications	No	No	Yes