

Council Policy No.:	CP2026-017
Council Policy Name:	Confidentiality of Information Policy
Date Approved by Council:	March 24, 2026 CR2026-091
Date revision approved by Council:	

### Policy Statement and Rationale:

It is important for the Corporation to set out a policy to protect the confidentiality of corporate records of the City of Kawartha Lakes. It is acknowledged that Members of Council, Committees, Task Forces and staff have access to corporate records which are confidential in nature. It is also acknowledged that these individuals do not complete all City work in a conventional office space within City owned facilities and that City documents may have to be taken off-site to allow work in other locations such as home, meetings, or other public places.

### Scope:

This policy applies to any person conducting City business and applies to all Members of Council, all employees and appointed volunteers.

### Definitions:

This policy should be read in conjunction with all applicable Corporate Policies and Management Directives Policy, Procedure and Implementation:

#### 1. MFIPPA, PHIPA, PIPEDA and QCIPA

1.1 The City of Kawartha Lakes, its Council, staff and appointed volunteers shall comply with the MFIPPA, PHIPA, PIPEDA and QCIPA.

#### 2. Sale or Release of Information

2.1 The City of Kawartha Lakes will not sell personal and/or confidential information.

2.2 The City of Kawartha Lakes will not release personal and/or confidential information unless required by or otherwise in accordance with law and relevant City Policy.

### 3. Collection of Information

- 3.1 The collection of information by the City will be governed by legislation, the Records Retention By-law and adopted City Policies.

### 4. Disclaimer

- 4.1 The following disclaimer (or similar) shall be placed at the bottom of all emails and fax cover letters being sent externally:

**This message, including any attachments, is privileged and intended only for the addressee(s) named above. If you are not the intended recipient, you must not read, use or disseminate the information contained in this email/fax. If you have received this email/fax transmission in error, please notify the sender immediately by telephone, fax or email and permanently delete this email from your computer/shred this fax, including any attachments, without making a copy. Access to this email/fax by anyone else is unauthorized. Thank you.**

- 4.3 The City website shall have a disclaimer relating to any links to other websites, Access to Information, and Privacy matters . The City shall not be responsible for the privacy practices of such linked websites.

### 5. Personal or other Confidential Information

- 5.1 If it is necessary to photocopy or electronically transmit personal or other confidential information, Council and employees shall do so directly and/or it shall be delegated to a staff member who is authorized to handle confidential materials and who has signed a confidentiality agreement.
- 5.2 All members of Council, and employees shall sign a confidentiality agreement as a condition of appointment/employment.
- 5.3 Council and/or employees shall only send personal or other confidential information by email when there is no other option available. The preferred option will be hand delivery. If sending personal or other confidential information by email, the email shall be classified as confidential using the confidential sensitivity tag. For internal email, the word **Confidential** shall be placed on the subject line in addition to the confidential classification.
- 5.4 Confidential information shall be prominently labeled **Confidential** on each page. (Example by using a watermark or the header option).
- 5.5 Only orange (salmon) coloured paper is to be used for copies of confidential documents. Members of Council and Senior Staff who receive confidential information on orange paper shall provide the copies to the City Clerk at the end of the Council session where the matter was dealt with unless they are responsible for following through on a matter of action, and the Clerk shall ensure that the information is shredded.

- 5.6 When bulk physical records (i.e. paper copies or an electronic memory device) containing confidential or personal information (i.e. reporting to a third party, relating to vital statistics, or financial reporting) are to be delivered externally, staff or Council shall use a traceable courier to protect the integrity of the delivery. Letters being sent directly to individual residents are permitted to be mailed by regular post, unless registered mail is required.
- 5.7 Where staff, members of Council, or City volunteers inadvertently receive personal or confidential information that they should not have received from other City Staff or Staff of Institutions under MFIPPA or FIPPA (due to error or otherwise), the staff who received the information shall:
- Notify the sender as soon as possible that information was sent to them in error;
  - Notify a supervisor or manager of the incident;
  - Refrain from discussing the inappropriate circulation with co-workers or other unaffected people; and
  - Delete or return and not record or retain a copy of any of the information that they received or viewed in error.

## **6. Off-Site Work on Files Containing Personal Information**

- 6.1 Records containing personal information shall only be removed from the office if it is absolutely necessary to carry out work responsibilities. When possible, original documents shall remain in the office and only copies of information shall be removed. Employees shall notify other departmental staff (preferably a supervisor or manager) when removing records containing personal information from the office.
- 6.2 Paper records containing personal or confidential information shall be kept in a secure location and under the constant control the member of Council or employee. Transitory paper records used off-site or in a remote office shall be shredded at a municipal office. Paper records shall be filed and stored in accordance with the City's Records Retention By-law and Policies.
- 6.3 Work-related records shall be kept separately in only one secure location of a personal premises.
- 6.4 Memory devices containing personal information shall be kept under constant control while in transit and when working away from the office.
- 6.5 Staff and members of Council shall prohibit any other person at their off-site work location from using or viewing a corporate device that contains personal or confidential information for personal purposes.

## **7. Loss or Theft**

It is the responsibility of every member of Council, staff or volunteer to complete the actions outlined in this section to ensure protection of corporate records.

- 7.1 Any breach of security shall be reported to the employees immediate supervisor. In the case of Members of Council, breaches of security should be reported to the City Clerk or their delegate.
- 7.2 In the event of a lost or stolen laptop, mobile phone, or memory device containing personal and confidential information, it should be reported immediately to the IT Division as well as the City Clerk or their delegate.
- 7.3 If necessary, the City Clerk will contact the Information and Privacy Commissioner (where a real risk of significant harm has been identified), and the police (if necessary) and follow all appropriate privacy breach policy and procedures.
- 7.4 Every member of Council and all employees shall assess control of personal or confidential information and records and improve controls wherever possible, in consultation with the City Clerk's Office.

**8. Policy Compliance**

- 8.1 Compliance with this policy is mandatory for all members of Council, and employees.
- 8.2 The contact person for this policy is the City Clerk or Deputy Clerk.

**Revision History:**

Proposed Date of Review:

Revision	Date	Description of Changes	Requested By
1	March 24, 2026	Approved to replace CP2022-005	