# CORPORATE POLICY AND PROCEDURE

| | |
|---|---|
| POLICY | **Access and Privacy Policy** |
| CATEGORY | Corporate Services |
| AUTHORITY | City Clerk's Office |
| RELATED POLICIES | Video Surveillance Policy, Records and Information Management Policy, Acceptable Use Policy, Bring Your Own Device (BYOD), Code of Conduct for Council and Local Boards, Accountability and Transparency Policy |
| APPROVED BY | Executive Team |
| EFFECTIVE DATE | March 23, 2017 |

## POLICY STATEMENT

The City of Guelph is committed to being open, accessible and transparent while protecting the privacy of individuals.

City records are public documents, subject to legislative exemptions, and are available for review in accordance with established procedures.

The protection of personal information is a legislated obligation under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), and the Personal Health Information Protection Act (PHIPA).

## PURPOSE

The purpose of this policy is to ensure compliance with the requirements of MFIPPA and PHIPA by establishing principles and practices that facilitate access to public records while protecting the privacy of personal and confidential information.

This policy is designed to ensure fair and equitable access to corporate records and information in the custody and control of the City. It also establishes the roles, responsibilities, and operational requirements around how personal information is collected, used, disclosed and disposed of by the City.

## SCOPE

This policy applies to all City employees, including full-time, part-time, casual, contract, volunteer and co-op placement employees.

This policy applies to all corporate records and all personal information managed by the City, and is not limited to the scope of any individual statute or regulation.

This policy applies to the records and information of the Office of the Mayor and members of Council that are created and used for the purpose of carrying out City business.

## POLICY

### Access to information

The City recognizes the public's right to access information in corporate records within its custody and control as an essential function of open government, accountability and transparency.

Access to information can be provided under one of the following procedures:

1. Public record request - Employees will provide access to, or give a copy of, a record that has been created or maintained as part of a public process.
2. Routine disclosure request - Employees will provide access, to or give a copy of, a record that is clearly outlined as part of a department level routine disclosure plan.
3. Freedom of information request - The City Clerk or delegated employees provide access to, or give a copy of, a record that contains personal or sensitive information and requires legislative review not otherwise public or set out under routine disclosure in accordance with the formal freedom of information procedure.

See related procedures for more information on the three access processes.

In order to facilitate access to corporate records, the City acknowledges the role that strong records and information management (RIM) practices play in preventing records from being lost or inappropriately deleted, reducing search times and fees associated with mishandled information and reducing the risk of privacy breaches.

<u>Identity of requestors</u>

Requestors' identities are protected and are only disclosed when there is a clear need in order to facilitate an access to information request or as required by legislation.

Access decisions in response to requestors exercising their right to access City information will be made in a consistent manner regardless of the requestors' identity.

Duty to assist

Employees have a duty to ensure every reasonable effort is made to assist requestors, by providing complete, accurate and timely responses to their request using the appropriate access to information process. This includes working with City Clerk's staff and responding to requests for records as part of the Freedom of Information process in a timely manner.

Obstructing right of access

In accordance with MFIPPA, it is an offence to willfully alter, conceal, destroy/ delete, or cause any person to do so, with the intention of denying access to a record or information contained in a record.

## Protection of privacy

Collection of personal information

MFIPPA and PHIPA govern the circumstances under which personal information may be collected. The City has adopted the following practices to standardize how the City collects personal information.

1. Personal information collected by employees is limited to only that which is required in order to administer the programs and services of the City.

2. When collecting personal information employees will:

    - Collect personal information directly from the individual to whom the information relates, with limited exceptions;
    - Make every attempt to ensure the accuracy and integrity of the personal information collected;
    - Prior to collection, provide notice or obtain the necessary consent as prescribed by the relevant legislation;
    - Inform individual(s) of the legal authority by which the information is being collected. This information is to be included on all City forms where personal information is being collected;
    - State the principal purpose(s) for which the personal information is to be used; and
    - Provide the contact information of the appropriate employee position that will be answer questions regarding the collection.

Use of information

Personal information collected by the City is used for the purpose or activity for which it was originally collected or for a consistent purpose. The use of personal information for any other purpose is permitted with the consent of the individual to whom the information relates, or in accordance with the legislation.

Protection of information

To protect the personal information within the custody and/or control of the City the following standards apply:

1. Access to personal information is restricted to only those employees requiring access in order to carry out their duties.
2. Personal information is not disclosed to members of the public, Council or other employees without the consent of the individual to whom the information relates, or in accordance with legislation.
3. Personal information is not discussed in public areas where it may be overheard by others who are not otherwise authorized to have such information.
4. Personal information is not left exposed or visible on desks or computer screens. Employees should lock computer screens and put physical records containing personal information away when not in use.
5. Records and files containing personal information are not removed from City worksites, unless required to complete duties and responsibilities of the position.
6. If documents are opened or reviewed in public places, the personal information contained in the records is protected.
7. System, software and email passwords allowing access to personal information are not shared or disclosed to others.
8. Cabinets or storage locations containing personal or confidential information are secured at the end of each day or when not in use.
9. External storage devices, such as USB sticks or external drives, are appropriately protected by being locked in a drawer or cabinet and/or are password encrypted.
10. Keys to secure storage areas are not left in open or obvious places.
11. Documents containing personal or confidential information are retrieved from the printer or fax machine in a timely manner.
12. Secure destruction is done by securely shredding sensitive documents or wiping digital storage devices. Records or digital storage devices are not placed in the garbage or recycle bin.
13. When a meeting is completed all personal or confidential materials are removed from the room, wiped from boards and flipcharts and computers signed out of.

Personal information is protected at all times against unauthorized access, loss, theft, and inadvertent destruction or damage. Security measures include administrative, technical and physical safeguards.

Records are stored in a manner that prevents loss through misplacement, deterioration, accidental destruction, theft and unauthorized or inappropriate access.

Security provisions are included in contracts with outside providers of records and information storage or disposal services.

Disclosure of information

The disclosure of personal information is administered in accordance with MFIPPA, PHIPA and City procedures. Where disclosure is not clearly authorized under legislation, the City will get consent to disclose prior to doing so.

Retention of information

The City will not retain any personal information for longer than is required for the provision of City programs and services, in accordance with the records retention by-law or subject to legislation.

## RESPONSIBILITY

The Chief Administration Officer (CAO) will:

- Provide oversight and compliance with this policy by all City employees.

Deputy Chief Administration Officers (DCAO's) will:

- Administer and communicate this policy broadly to all employees in their service areas;
- Promote a culture and business practices that ensure City information is shared and accessible to the greatest extent possible, while respecting privacy requirements of personal information and other confidentiality obligations; and
- Integrate the protection of personal and confidential information into the development, implementation, evaluation and reporting activities of service area programs and services.

The City Clerk and delegated employees will:

- Act as the Head under MFIPPA and as provided for through Council delegation;
- Be accountable for overseeing the administration of MFIPPA and PHIPA within the municipality and for decisions made under the above legislation;
- Ensure oversight of and compliance with this policy;
- Develop and implement policies, programs and services to ensure awareness of access to information processes and protection of personal information based on Access by Design and Privacy by Design principles;
- In partnership with service areas, ensure implementation of this policy, review practices for collecting and managing personal information, and consult with employees to meet privacy requirements as identified in this policy, applicable legislation, privacy standards and procedures;

- Investigate and respond to complaints regarding the misuse of personal information or reports of privacy breaches following the City's Privacy Breach Protocol;
- Provide recommendations and sign-off on any privacy impact assessments prior to the implementation of a new application, system, program or service involving the collection or use of personal information or personal health information;
- Develop standards, procedures, guidelines, training material and other tools as required, to assist members of Council, employees and the public on matters pertaining to the collection, use and disclosure of information;
- Ensure that legislative updates are incorporated into the City's collection, use and disclosure processes;
- Ensure that adequate disposal processes for personal information are in place and adhered to;
- Be responsible for the receipt, coordination, response and sign off for all formal freedom of information requests received pursuant to MFIPPA and PHIPA in collaboration with all departments; and
- Assist the public with requests for access to information as required.

The General Manager Human Resources will:

- In partnership with the City Clerk, establish a training and education plan, including the development of online and in person learning opportunities to improve awareness of access and privacy requirements; and
- Build access and privacy awareness into all new employee orientation programs.

The General Manager Technology and Innovation will:

- In partnership with the City Clerk, implement Access by Design and Privacy by Design principles in enterprise architecture, IT policies, standards, procedures and technologies where appropriate;
- Create privacy and security standards for technologies that will ensure adequate safeguards and compliance for those technologies or technical processes that collect, use, disclose or retain personal information; and
- Ensure privacy impact assessments are conducted on all new systems or applications involving the collection or use of personal information prior to implementation.

General managers, managers and supervisors will:

- Ensure personal information is collected, used disclosed and disposed of in accordance with legislation and in compliance with this policy;
- Implement this policy and communicate requirements to the employees under their direction;
- Receive public record or routine disclosure requests from the public and from individuals wishing access to or correction of their own information;
- Respond to requests for records from the City Clerk's Office in relation to freedom of information requests;

- Ensure proper notice is given and/or the required level of consent is obtained prior to the collection or use of all personal information;
- In collaboration with the City Clerk and Procurement/Purchasing staff, require vendors and contractors comply with this policy and that privacy rules and concerns are referenced in all procurement documents;
- Require employees, vendors and/or contractors maintain a level of privacy awareness appropriate to their responsibilities;
- Inform employees of the legal and administrative consequences of any inappropriate or unauthorized access to, or collection, use, disclosure or disposition of, personal information related to a particular program or activity;
- Ensure programs and services within their departments integrate protection of personal privacy requirements into development, implementation, evaluation and reporting activities;
- Ensure privacy impact assessments are conducted on any new programs, services or technologies involving the collection or use of personal information prior to implementation; and
- Promote a culture and business practices that ensures City information is shared and accessible to the greatest extent possible while respecting security and privacy requirements of personal information.

Employees will:

- Understand their responsibilities to provide access to information, as well as, protect privacy in executing their operational duties;
- Take access and privacy awareness training for the appropriate handling of personal information to understand their responsibilities;
- Be aware of their access and privacy responsibilities noted in the other City policies;
- Assist the public with access to information requests under the public record or routine disclosure procedures as required;
- Respond to requests for records from the City Clerk's Office in relation to freedom of information requests; and
- Adhere to information management requirements contained in records and information management policies and procedures of the City, including the records retention by-law.

## MONITORING AND REPORTING

The City Clerk's Office monitors compliance, engagement and awareness of this policy with:

- access to information reporting documents under the routine disclosure and freedom of information processes;
- the results of audits;
- training and education session evaluations; and
- employee surveys.

This policy is reviewed a minimum of once per calendar year to ensure its effectiveness and compliance with legislation and current business processes or as required based on legislative changes.

For further information regarding this policy please contact the Program Manager Information, Privacy and Elections at 519-822-1260 extension 2605 or privacy@guelph.ca.

## REFERENCE MATERIAL

Municipal Freedom of Information and Protection of Privacy Act
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm

Personal Health Information and Protection Act
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm

Information and Privacy Commissioner
http://www.ipc.on.ca/english/Privacy/

## APPENDIX A: DEFINITIONS

**Access by design** is the access standard developed by the Information and Privacy Commissioner of Ontario that the City utilizes to embed access to information into the design and development of new applications, systems, programs and services in order to facilitate compliance with access to information principles.

**City** means the Corporation of the City of Guelph.

**Consistent purpose** means personal information collected by the City of Guelph is used for the purpose for which it was collected or similar consistent purposes when carrying out City business. The individual to whom the information relates might reasonably expect the use/disclosure of their personal information for those consistent purposes.

**Control (of a record)** means the power or authority to make a decision about the use or disclosure of a record.

**Custody (of a record)** means the keeping, care, watch, preservation or security of a record for a legitimate business purpose. While physical possession of a record may not always constitute custody, it is the best evidence of custody.

**Destruction** is the physical or electronic disposal of records or data by means of shredding, recycling, deletion or overwriting. This also includes the destruction of records or data residing on computers and electronic devices supplied or paid for by the Corporation.

**Freedom of information request-** means a formal request for access to records made under the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

**Head** refers to the City Clerk.

**Information and Privacy Commissioner** means the Information and Privacy Commissioner of Ontario (commonly referred to as the IPC). The IPC hears appeals of decisions made by Heads of institutions, issues binding orders, conducts privacy investigations, and has certain powers relating to the protection of personal privacy as set out in the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

**Institution** means the Municipality.

**Integrity Commissioner** means the City Council appointed official responsible for addressing requests to investigate and recommend penalties for suspected contraventions of the Code of Conduct for Council and Local Boards.

**Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)** means legislation that governs access to and the privacy of municipal records.

**Personal information** means recorded information about an identifiable individual including:

a) Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation, or marital or family status of the individual;
b) Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to the financial transactions in which the individual has been involved;
c) Any identifying number, symbol, or other particular assigned to the individual;
d) The address, telephone number, fingerprints or blood type of the individual;
e) The personal opinions or views of the individual except if they relate to another individual;
f) Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;
g) The views or opinions of another individual about the individual, and
h) 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.

**Personal health information** means identifying information about an individual in oral or recorded form, if the information:

a) Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family;
b) Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual;
c) Is a plan of service within the meaning of the *Home Care and Community Services Act, 1994* for the individual;
d) Relates to payment or eligibility for health care, or eligibility for coverage for health care, in respect to the individual;
e) Relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part of bodily substance;
f) The individual's health number; or
g) Identifies the individual's substitute decision maker.

**Privacy breach** means an incident involving unauthorized disclosure of personal information, including it being stolen, lost or accessed by unauthorized persons.

**Privacy by design** is the privacy standard developed by the Information and Privacy Commissioner of Ontario that the City utilizes to embed privacy and data protection into the design and development of new applications, systems, programs and services, in order to facilitate compliance with privacy and data protection principles.

**Privacy Impact Assessment (PIA)** is the process for identifying, assessing and mitigating privacy risks. The City develops and maintains privacy impact assessments for all new or modified programs that involve the use of personal information or personal health information for an administrative or operational purpose.

**Public record request** means a request for records or information that has passed through an open public process, thereby making them public documents, that can be provided to the requestor without needing to go through a routine disclosure or freedom of information process.

**Record** means any unit of information however recorded, whether in printed form, on film, by electronic means, or otherwise, and includes correspondence, memoranda, plans, maps, drawings, graphic works, photographs, film, microfilm, sound recordings, videotapes, machine readable records, an e-mail and any other documentary material regardless of physical form or characteristics, made or received in the course of the conduct of City business.

**Records retention by-law** means the most recent by-law passed that contains the schedule and the length of time City business records must be retained for before it may be disposed of in order to meet business needs and legislative requirements.

**Routine disclosure request** means a request for routine records, listed in a department routine disclosure plan, that can be made and released at the department level without the requirement of a Freedom of Information Request pursuant to MFIPPA.