



CORPORATE POLICY		CP.1.1.2.
Section	1	Administration
Subsection	1	General
Title/Subject/Chapter	2	Collection, Use, Disclosure and Destruction of Information
Approval Authority: CR-102.07	Effective Date: March 07, 2007	

**PURPOSE:**

To ensure that the Town of Innisfil complies with the intent and requirements of the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* and other privacy legislation by implementing practices that will facilitate open access to public records, while protecting the privacy of personal information.

**APPLICATION:** This policy applies to Members of Council and all Town employees, Committees, Affiliates, Agents and Contractors.

**POLICY STATEMENT/GUIDELINES:**

To provide guidelines to both elected officials and staff, regarding the collection, use, disclosure, and disposal of personal information. This policy shall establish principles which facilitate and promote an open and transparent government, while safeguarding personal information which is within the custody of the municipality.

**1.0 POLICY OBJECTIVES**

1. To ensure that the manner in which information is collected, used, retained, disclosed and destroyed by the Municipality is consistent with the requirements of legislation and the Town's Records Management Policy and Records Retention By-Law.
2. To ensure that exemptions applied pursuant to the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* are limited and specific.
3. To establish an accountability framework defining the roles and responsibilities of members of Council, senior officials and staff.

4. To ensure that processes are in place to protect the integrity and privacy of personal information within the custody and control of the Municipality.
5. To ensure there are uniform guidelines pertaining to the handling of routine disclosures and processing of formal access requests.

## 2.0 **DEFINITIONS**

**“Disposal”** refers to the process of eliminating or deleting data, documents and records so that the recorded information no longer exists;

**“Formal Access Request”** refers to the process of submitting a request for access to records in accordance with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

**“Personal Information”** as defined by MFIPPA, means recorded information about an identifiable individual, including:

- information relating to the race, national or ethnic origin, colour religion, age, sex, sexual orientation or marital or family status of the individual;
- information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
- any identifying number, symbol, or other particular assigned to the individual;
- the address, telephone number, fingerprints or blood type of the individual;
- the personal opinions or view of the individual except if they relate to another individual;
- 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;
- the views or opinions of another individual about the individual; and
- 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 Information Bank” (PIB)** A collection of personal information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual;

**“Record”** means any record of information, however recorded, whether in printed form, on film, by electronic means or otherwise, including correspondence, memoranda, plans, maps, drawings, graphic works, photographs, film, microfilm, microfiche, sound records, videotapes, e-mail, machine readable records, and any other documentary material, regardless of physical form or characteristics, and including “official records” and “transitory records”;

“**Records Management Manager**” means the Records Management Manager as designated by the Corporation;

“**Routine Access (Disclosure)**” refers to the process of providing requesters with a copy of records or providing a means in which the requester may examine or view records outside of the *Municipal Freedom of Information and Protection of Privacy Act* process.

### 3.0 **OVERVIEW OF LEGISLATION**

The Town of Innisfil has adopted business practices that standardize the way in which it collects, uses, discloses, and disposes of personal information. These practices have been developed in accordance with the requirements of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) as well as other privacy statutes and laws.

MFIPPA legislation came into effect on January 1, 1991 and is based on four (4) principles:

1. To provide a method of ensuring public access to government information.
2. That exempted information should be limited.
3. That there is an opportunity for an appeal process to an independent Information and Privacy Commission.
4. That privacy of personal information must be protected.

Advancements in technology and the way in which businesses collect, use, and maintain information has lead to the enactment of additional pieces of legislation including the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) as well as the *Personal Health Information Protection Act* (PHIPA). Any and all legislation must be considered when determining the impacts of collecting, using, disclosing and disposing of information and records.

### 4.0 **ROLES AND RESPONSIBILITIES**

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) stipulates that municipal councils may appoint a “**Head**” from amongst themselves to be responsible for overseeing the administration of the legislation within the municipality and for decisions made under the legislation.

At the Town of Innisfil, the **whole Council** is designated, by by-law, as the “**Head**” for the purposes of MFIPPA. To effectively carry out the requirements associated with MFIPPA, this responsibility has been delegated, by by-law, to the **Clerk**.

The **Records Management Manager** (on behalf of the Town Clerk) administers the day-to-day requirements of the program including the receipt and processing of formal requests, monitoring collection and disclosure of information, and providing assistance and guidance to staff on issues pertaining to MFIPPA and privacy legislation.

## 5.0 **ACCOUNTABILITY**

In order to ensure that there is a collaborative approach to collecting, using, accessing, disclosing and destroying records and information, accountability guidelines have been established.

**The “Head”** shall be accountable and responsible for:

- ensuring overall compliance with all applicable privacy legislation.

**Town Clerk** shall be responsible for:

- overseeing administration of the Town’s MFIPPA Program (as delegated by the “Head”) and ensuring there is corporate compliance with all privacy legislation.

**CAO/Directors** shall be responsible for:

- ensuring that all departments/divisions within their area of responsibility are maintaining compliance with the Town’s Privacy Policy objectives as well as all privacy legislation.

**Managers** shall be responsible for:

- overseeing the routine disclosure of information and records associated with their area of responsibility. This would include informal requests from the public and requests from individuals wishing access to their own personal information;
- ensuring that proper notice is given to the public prior to the collection of any personal information;
- ensuring the accuracy of personal information collected and retained;
- ensuring that all personal information is managed and protected in accordance with this policy and all applicable privacy legislation;
- appointing a Freedom of Information (FOI) Contact person, within their department who will assume a lead role in coordinating and compiling information requested by the public and/or Records Management Manager.

**Records Management Manager** shall be responsible for:

- the receipt, coordination and formulation of responses for all formal access requests submitted under MFIPPA;
- providing advice and developing policies and guidelines to assist members of Council, staff, and the public on matters pertaining to the collection, use and disclosure of information;
- ensuring that legislative updates are incorporated into the Town’s collection and disclosure processes;
- ensuring that adequate disposal processes for personal information are in place and adhered to.

**Staff** shall be responsible for:

- ensuring that all personal information collected (s) is accurate and complete;
- protecting personal information to which they have access or custody of;
- assisting the public with requests for access to information and the routine disclosure of records and information;
- adhering to the disposal requirements contained in this and other records management policies of the Town.

## 6.0 **COLLECTION OF PERSONAL INFORMATION**

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) stipulates the provisions whereby personal information may be collected by a municipality. There are a number of Sections within MFIPPA that address this process:

At the Town of Innisfil:

- Personal information collected by Town staff shall be done in accordance with the provisions of MFIPPA and other privacy legislation.
- Personal information collected by Town staff shall be limited to only that information which is required in order to administer the programs and services of the Town.
- Wherever possible, personal information is to be collected directly from the individual to whom the information relates. If using an indirect or alternative manner of collection, staff must adhere to the guidelines stipulated in Section 29(1) of MFIPPA.
- Every attempt shall be made to ensure the accuracy and integrity of the personal information collected.
- Unless exceptions pertaining to collection are permitted as per Section 29(3) of MFIPPA, Departments will, when collecting personal information:
  - o inform individual(s) of the legal authority by which the information is being collected. This may require citing the applicable Section of MFIPPA and/or another piece of legislation. Such information will be included on all Town forms where personal information is being collected.
  - o state the principal purpose (or purposes) for which the personal information is intended to be used; and
  - o the title, business address and business telephone number of an appropriate staff member who will be able to answer questions from the public about the collection.
- Notice of collection may be done orally, in person, over the telephone, in writing (by way of an application form, posted signage, newspaper advertisement, Town website) or other manner which adequately informs the individual about the collection.

## **7.0 USE OF PERSONAL INFORMATION**

Personal information collected by the Town will be used for the purpose or activity for which it was originally collected or for a 'consistent purpose'. A 'consistent purpose' means that the individual to whom the information relates might reasonably have expected the use/disclosure.

The use of personal information for any other purpose shall only be permitted with the consent of the individual to whom the information relates, or in accordance with the provisions of Section 31 of MFIPPA.

### **7.1 Council Communications/Delegations**

The following process shall be applied when dealing with Council Communications/Delegations:

- Communications/delegations directed to the Town for the purposes of Council or Committee consideration shall include the name and/or address of the sender/delegate and shall be considered public record;
- The name of the sender, their signature, and the property address of the sender (if relevant) shall form part of the public record;
- Any additional personal information on communications (i.e. personal telephone numbers, personal e-mail addresses, etc.) shall be severed, prior to disclosure, unless the information belongs to a business entity or an individual acting in a business capacity;
- Such communications and information shall form part of Committee/Council agendas and be used to assist Council and Committee members with properly addressing and responding to individuals' requests or inquiries;
- Any communications presented to Council in public session shall be made available for public viewing by way of print and/or electronic means;
- Discretion pertaining to the disclosure of personal information may be exercised by the Town Clerk where the personal information relates to highly sensitive or confidential matters and/or relates to one of the designated criteria for a "closed" session;
- Where an individual has specifically expressed that the communication be treated as "confidential", the Clerk's Department shall contact the individual to request consent to disclose the communications in order to allow Council to deal with the matter.

## **8.0 DISCLOSURE AND PROTECTION OF PERSONAL INFORMATION**

### **8.1 Protecting Personal Information**

Protecting the privacy of individuals and any personal information which has been collected and used by the Municipality is a requirement of privacy legislation and a primary focus of the Town of Innisfil.

Section 3 of R.R.O. 1990, Regulation 823, *Amended To O. Reg. 480/97*, stipulates:

- (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.
- (2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.

To ensure that every precaution is taken to protect the privacy of personal information, the following processes shall be adhered to:

- o Access to personal information shall be restricted to 'only' those employees requiring access in order to carry out their duties.
- o No personal information shall be disclosed to members of the public, Council or other staff without the consent of the individual to whom the information relates (except where permitted by legislation or within this policy).
- o Personal information shall not be discussed in public areas where it may be overheard by others who are not otherwise authorized to have such information.
- o Personal information should not be left exposed or visible on desks or computer screens. Staff should minimize computer screens and put records

- containing [third party] personal information away when not in use.
- Records/files containing personal information should not be removed from Town worksites. If it is necessary to have records leave the worksite, the records should be copied first. Originals should remain on-site at all times.
- Records/files leaving the worksite that contain personal information should be signed out. Sign-out cards/forms should include employee's name, description of records, file number and file name, date of removal and date of return and be kept within the department/location where the records were removed from.
- Any records leaving the site that contain personal information should be secure (packaged in envelopes or folders and placed in a locked briefcase or sealed box).
- Documents shall not be opened or reviewed in public places unless the personal privacy of the individuals contained in the records is protected.
- System, software and e-mail passwords shall not be shared or disclosed to others.
- Sensitive personal or confidential information should, wherever possible, be sent by regular mail or courier. If transmitting such information by e-mail or fax, ensure that e-mail addresses and fax numbers are accurate prior to sending the information.
- Confidentiality and privacy statements shall be included on all e-mail and fax transmissions.
- Cabinets or storage locations containing personal or confidential information should be locked or secured at the end of each day and when not in use.

## **8.2 Access to one's own personal information**

MFIPPA further provides that individuals have the right to access and correct their own personal information if they believe there is an error or omission. This applies to information contained in Town Personal Information Banks to which the individual has been granted access.

Once access has been granted to their personal information, an individual has the right to:

- request a correction of their personal information
- require that a statement of disagreement be attached to the information reflecting any correction that was requested but not made; and
- require that notification be sent to any person or body to whom the personal information has been disclosed (within the year before) advising them of the correction or statement of disagreement

Access to one's own personal information shall be at the discretion of the Head (or delegate). Certain exemptions affecting access may be applied pursuant to Section 38 of MFIPPA.

## **8.3 Routine Disclosure**

There are a number of records and types of information which are available via Routine Disclosure, meaning that a formal access request is not necessarily required in order to obtain or view the information.

Access to Town information and records will, wherever possible, be made available to the public via Town kiosks, the Town website, orally, or through public inspection at the Town's Municipal Offices.

The following are examples of such records where routine disclosure may be permitted:

- Information related to Town-owned Surplus Lands
- Corporate Policies
- Demographic and statistical information
- By-Laws
- Agendas
- Minutes
- Reports
- Resolutions
- General community information (i.e. licensing, permits, waste disposal information, etc.)
- Annual (approved) budgets
- Audited Financial Statements
- Summary of total tender results
- Tax Certificates
- Committee of Adjustment Notices and Decisions
- Planning related documents and development records (as per the *Planning Act*)
- Subdivision / Site Plan Agreement Information
- Construction information
- Building Services reports or compiled statistics
- Recreational programming and facility rental information
- Information pertaining to leisure events and activities

Prior to the disclosure of any records, Town staff should consult with their manager/supervisor and where uncertain about disclosure, contact the Town Clerk or Records Management Manager.

#### **8.4 Disclosure of Information**

Although a primary focus of MFIPPA is to facilitate access to government information, there are limitations to that access. These limitations are in place to protect personal information, as well as sensitive information, in the custody and control of government.

Under MFIPPA, there are two types of exemptions that must be considered when assessing whether information is to be disclosed:

- (1) **Mandatory exemptions** – requiring the institution to refuse disclosure of the record. Such records include:
  - information pertaining to intergovernmental relations; if the information was received in confidence;
  - third party information that reveals a trade secret or scientific, technical, commercial, financial or labour relations information, if supplied in confidence, and where disclosure could prejudice the interests of a third party;
  - personal information about individuals other than the requester.
- (2) **Discretionary exemptions** – requiring an institution to apply discretion and good judgment when determining whether or not to disclose the record. Such records include:
  - draft by-laws, records of closed meetings where such are authorized by statute;
  - advice or recommendations within the organization;

- law enforcement records;
- information which could prejudice the financial or other specified interests of the organization;
- solicitor-client privileged information;
- information which could endanger the health or safety of an individual;
- information already available to the public or soon to be published

Although the above noted exemptions provide direction as to what must or may be considered when assessing whether or not to disclose, there are times when the above exemptions do not apply.

Certain exemptions (above) do not apply:

- (a) if a compelling **public** interest outweighs the purpose of the exemption; or
- (b) if there is a **grave** environmental, health or safety hazard, regardless of whether or not a formal request for information has been made

### **8.5 Disclosure of Personal Information**

Under MFIPPA, there are limited circumstances where disclosure of personal information is permitted:

- 1) With the consent of the individual to which the information pertains;
- 2) Where disclosure to another employee is required in order for he/she to carry out the duties of their position (where the disclosure is necessary and proper in the discharge of the employee's functions);
- 3) For the purpose for which the information was obtained or compiled or for a 'consistent purpose';
- 4) For the purposes of complying with an Act of the Legislature or an Act of Parliament, an agreement or arrangement under such Act or a treaty;
- 5) To an institution or a law enforcement agency in Canada to aid in an investigation;
- 6) In compelling circumstances affecting the health and safety of an individual;
- 7) In compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased;
- 8) To the Minister;
- 9) To the Information and Privacy Commissioner;
- 10) To the Government of Canada or the Government of Ontario in order to facilitate the auditing of shared cost programs (R.S.O. 1990, c.M.56, s. 32).

Members of the public seeking access to records which contain another individual's personal information must complete and submit a formal Access Request in accordance with the *Municipal Freedom of Information and Protection of Privacy Act*.

## **9.0 DISPOSAL OF PERSONAL INFORMATION**

Section 3 of R.R.O. 1990, Regulation 823, *Amended To O. Reg. 480/97*, stipulates:

- (3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

- Records containing personal information, collected by the Town, shall be retained in accordance with the retention periods set out in the Town's Records Retention By-Law and disposal shall be in the manner prescribed within the Town's Records Management Policy.
- Staff shall ensure that all records containing personal information are disposed of by means of shredding or by placing records in waste disposal containers within Town office buildings.
- No personal information is to be discarded in recycle bins or in waste baskets where public access is permitted.

## **10.0 FORMAL ACCESS REQUESTS**

### **10.1 General Guidelines:**

- Members of the public may obtain access to information or records held by the municipality by first contacting the Town of Innisfil Administration offices to see if the records are subject to routine disclosure.
- Records containing third party personal information must be requested by way of a formal access request.
- Requests for copies of Engineering or Architectural type drawings as well as any technical reports, assessments, analysis, etc., produced by external entities, which are in the custody of the municipality, must be requested by way of a formal Access Request. This process shall be adhered to in order to ensure that the Town remains compliant with the provisions of the *Copyright Act*.

## **11.0 PRIVACY BREACHES**

Breaches of privacy result in a loss of credibility, damage to the Municipality's reputation, appeals and/or potential litigation.

A privacy breach occurs whenever a person has contravened a provision of privacy legislation by purposely or inadvertently disclosing the personal information of another individual.

If any employee, elected official, or affiliated individual or entity acting on behalf of the Town believes that a privacy breach has occurred, they are asked to contact the Town Clerk or Records Management Manager immediately so that all necessary action can be taken to mitigate any damage which may arise as a result of the breach.