FLOWER CITY

BRAMPTON.CA

Access & Privacy

A Manual

Working with the *Municipal Freedom of Information and Protection of Privacy Act*

City Clerk's Office

June, 2015

CONTENTS

FOREWORD

The *Municipal Freedom of Information and Protection of Privacy Act* ("the Act") came into effect January 1, 1991.

The purpose of this Manual is to assist the Staff of the City of Brampton to interpret and administer the legislation. The Manual is intended to serve as a practical guide in carrying out the requirements of the legislation. It should not be used as a substitute for the legislation. Where necessary, the legislation (along with the Regulations and related Orders) should be consulted.

The Manual contains the following 8 Parts:

1. Introduction to the Act
2. Administration of the Act
3. Access Procedures
4. Exemptions
5. Privacy Protection
6. Fees
7. Commissioner and Appeals
8. Offences and Liability

The Manual also contains sample Notification Letters as well as Appendices, a Section Index and Subject Index.

The City of Brampton is committed to a continually improving, effective access to information and privacy program as a corporate priority.

This manual can assist City of Brampton staff members that participate in responding to access to information requests under the Act. The Freedom of Information – Privacy Coordinator under the direction of the City Clerk manages the response to requests for access to information made in writing by members of the public under the Act. Each City division that has custody or control of the requested records is responsible for retrieving those requested records within the timeframes this manual sets out. The City Clerk has the final decision-making authority to grant or withhold access to records in response to formal access requests submitted under the Act.

PART 1: INTRODUCTION TO THE ACT

PURPOSE OF THE ACT (SECTION 1)

The *Municipal Freedom of Information and Protection of Privacy Act* (the Act) provides individuals with a right of access to certain records and personal information in the custody or under the control of institutions covered by the Act.

The purposes of the Act are as follows:

A) to provide a right of access to information under the control of institutions in accordance with the principles that:

- information should be available to the public,
- necessary exemptions from the right of access should be limited and specific,
- decisions on the disclosure of information should be reviewed independently of the institution controlling the information, and

B) to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

The *Municipal Freedom of Information and Protection of Privacy Act* can be accessed using the Provincial e-Laws Website.

ORGANIZATION OF THE ACT

The Act came into force on January 1, 1991, and it is divided into four parts:

Part I: Freedom of Information deals with the right of access to records, the exemptions to that right and access procedures (sections 4-26).

Part II: Protection of Individual Privacy concerns the collection, use and disclosure of personal information. This part also deals with an individual's right of access to his or her own personal information and the right to request correction of that information (sections 27-38).

Part III: Appeal deals with the right to appeal and the procedure involved in appealing a

decision made by an institution (sections 39-44).

Part IV: General covers general matters including the charging of fees, offences, regulations and the powers and duties of the Information and Privacy Commissioner (sections 45-55).

The remainder of this introductory section will discuss the scope of the Act and definitions of key terms within the Act.

WHAT THE ACT COVERS

The Act covers all municipal corporations in the Province of Ontario, including counties, metropolitan, district or regional municipalities, local boards and commissions. The term institution is defined in section 2 of the Act and is set out in the *Definitions* section.

This Act applies to any record in the custody or under the control of the City. This includes records that were created both before and after the Act came into force on January 1, 1991 [subsection 52(1)].

NON-APPLICATION OF ACT (SECTION 52)

The Act does not apply to:

- Records placed in archives by or on behalf of a person or organization other than the institution;
- Records relating to a prosecution if all proceedings in respect of the prosecution have not been completed; or,
- Records collected, prepared, maintained or used by or on behalf of the City in relation to any of the following:
    - Proceedings or anticipated proceedings before a court, tribunal or other entity relating to labour relations or to the employment of a person by the institution;
    - Negotiations or anticipated negotiations relating to labour relations or to the employment of a person by the institution between the institution and a person, bargaining agent or party to a proceeding or an anticipated

proceeding; and/or,

- Meetings, consultations, discussions or communications about labour relations or employment-related matters in which the institution has an interest.

Despite the above (non-application), the Act does apply to the following records [SEC.52(4)]:

- An agreement between the City and a trade union;
- An agreement between the City and one or more employees which ends a proceeding before a court, tribunal or other entity relating to labour relations or two employment-related matters;
- An agreement between the City and one or more employees resulting from negotiations about employment-related matters between the institution and the employee or employees;
- An expense account submitted by an employee of the City for the purpose of seeking reimbursement for expense incurred by the employee in his or her employment.

The Act does not impose any limitation on the information otherwise available by law to a party to litigation. Where an institution is required to produce documentary evidence pursuant to rules of court, the exemptions in the Act do not apply [subsection 51(1)]. The Act does not affect the power of a court or tribunal to compel a witness to testify or compel the production of a document [subsection 51(2)].

DEFINITIONS

In this part, the following key terms that appear throughout the Act are discussed:

- Head
- Information and Privacy Commissioner
- Institution
- Personal Information
- Personal Information Bank

- Record
- Machine Readable Record

Other terms are defined elsewhere in the manual with its related subject matter.

HEAD

The City of Brampton appointed the City Clerk as the Head for the purpose of administering the Act (By Law 191-2011). The head is responsible for decisions made under the Act by the City and for the administration of the Act within the City. In Part 2 a description of the head's responsibilities are discussed in detail.

INFORMATION AND PRIVACY COMMISSIONER

The Information and Privacy Commissioner is appointed by the Lieutenant Governor in Council. The Commissioner is an officer of the Legislature and is independent of the government.

The Commissioner 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 (Section 46). In Part 7, the role of the Commissioner is discussed in more detail.

INSTITUTION

Institution is the general term for local organizations, boards and other bodies covered by the Act. An institution is responsible for administering and adhering to the requirements of the Act. The Committee of Adjustment for the City of Brampton is included, as well as all Committees appointed by Council.

PERSONAL INFORMATION

Personal Information means recorded information about an identifiable individual,

including:

- information relating to the race, national or ethnic origin, religion, age, gender (sex), sexual orientation or marital or family status of the individual;
- information relating to the education or the medical, 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, e-mail address, fingerprints or blood type of the individual;
- the personal opinions or views of the individual except if they relate to another individual;
- the views or opinions of another individual about the 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; and,
- the individual's name if it appears with other personal information relating to the individual or where disclosure of the name would reveal other personal information about the individual.

Personal information must be about an identifiable individual, however, an individual's name need not be attached to the information to qualify as personal information. A physical description, photograph or video, or identifying number of a person attached to other personal information about that person is personal information although no name is ever indicated. This individual is *identifiable* and all personal information relating to the individual must be protected.

Generally, information about a property or specific municipal address, such as market value assessment, hydro-electric consumption or building permit information, is NOT personal information. However, records containing such property-related information may also contain an individual's name and personal information such as a home telephone number. Care should be taken to ensure that any disclosure of that personal information complies with the privacy protection provisions of the Act (see Part 5 for a discussion of sections 14 and 32 of the Act regarding the disclosure of personal information).

An individual's name on its own is not personal information. To be personal information

within the meaning of the act, the name must be associated with other personal information as defined in section 2 of the Act.

For example:

> An individual's name kept by a social services department would be personal information because the fact that the name on a record at the department might indicate that the person was, or is, in receipt of public assistance.

An individual, in the context of the Act, does NOT include a sole proprietorship, partnerships, unincorporated associations, corporations, trade unions or law firms or the names of officers of a corporation writing in their official capacity. However, records containing information about these business entities may also contain personal information about individuals and may warrant the protection of the Act.

Correspondence submitted to the City of Brampton by a representative of a group or association IS NOT the personal information of the author of the correspondence. If the correspondence submitted to an institution is on the letterhead of the organization and signed by an individual in his or her capacity as a spokesperson of the organization, the content of the letter does not qualify as the writer's personal information.

Personal information does not include information about an individual who has been dead for more than 30 years (subsection 2(2)).

The definition of personal information under the Act refers to **recorded** information about an identifiable individual. For the purposes of collecting personal information under part II of the Act (Protection of Individual Privacy), personal information includes personal information collected orally on behalf of an institution (section 28). This is discussed in Part 5.

PERSONAL INFORMATION BANK

A personal information bank is a collection of personal information that is organized and capable of being retrieved using an individual's name or other individual identifier. A collection of personal information in the custody or control of the City of Brampton would be a personal information bank if it has the following characteristics:

- it must contain personal information;
- information contained in the bank must be a collection of like or similar

information about individuals; and

- information must be linked to an identifiable individual; and the information must be capable of being retrieved by the individual's name or identifying symbol (such as a number of code name).

Examples:

- A public library's circulation records that contain the names, address and borrowing records of patrons would be a personal information bank.
- The City's Human Resources Files, including health, workers' compensation, grievances, etc.

The City will have collections of records which contain some personal information but these would not meet the criteria for the definition of personal information bank. The Act does not require the City to rearrange its personal information into personal information banks.

Collections of personal information that meet the characteristics of a personal information bank (as set out above) must be identified and described by the City. Generally, individuals have the right to obtain information about themselves contained in the personal information banks of an institution. These descriptions must be made available to assist the public in exercising privacy rights.

RECORD

A record is any record of information however recorded, whether in printed form, in film, by electronic means or otherwise, and includes:

- correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a video whether on tape, DVD or any other electronic device, a machine-readable record, any other documentary material regardless of physical form or characteristics, and any copy thereof; and
- subject to the regulations, any record that is capable of being reproduced from a machine-readable record under the control of an City by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution.

The definition of record is very broad and includes virtually every form of information held by an institution. The definition is not restricted to actual physical documents, but includes records that can be created from existing data in a computer bank. Email, voicemail messages, text messages and social media posts are all considered to be records.

Handwritten notes or other notations on records form a part of the records. Working copies and drafts of reports and letters are also records and all are subject to the Act if they exist.

The Act does not apply to records placed in the archives by or on behalf of a person or organization other than the institution [subsection 52(2)]. Manuscripts such as diaries and letters donated by a member of the general public to a municipal archive, would not be covered by the Act. However, if the City places its records in an archive, either its own archive or the archive of another institution, these records are subject to the Act. The City of Brampton transfers it archival records to the Region of Peel Archives.

MACHINE READABLE RECORD

In cases where a request is for information that does not currently exist, but is capable of being produced from a machine readable record, the Act gives the requester the right (subject to the regulations) to the information which would answer all or part of a request.

If the process of producing a record from a machine readable format would unreasonably interfere with the operations of an institution, the machine readable record would not be included in the definition of a record as outlined above. Unreasonable interference with operations could include instances where normal business activities would have to stop or change in order to produce the record. It may include instances where the cost of producing the record would result in the inability of an institution to meet its other obligations.

Reg. 823 of the Act (Regulations) speaks to this further.

PART 2: ADMINISTRATION OF THE ACT

INTRODUCTION

The *Municipal Freedom of Information and Protection of Privacy Act* sets requirements that must be met by each institution. In the City of Brampton, the head of the institution is responsible for fulfilling these requirements. The requirements concern:

- Responding to requests for access to records;
- Protecting personal privacy;
- Providing specific information to the Information and Privacy Commissioner (IPC); and,
- Making information available to the public.

This part provides an overview of the administrative responsibilities of the head, and other issues dealing with the administration of the Act.

HEAD OF AN INSTITUTION

The head of an institution is responsible for decisions made under the Act and for overseeing the administration of the Act within the institution.

The Council of the City of Brampton by by-law has designated the City Clerk to be the head as per section 3 of the Act (By Law 191-2011). The City Clerk in turn can delegate, in writing, the responsibility to another staff person.

To revoke the designation, Council would have to revoke the by-law appointing the City Clerk.

Employees who issue notices required by the Act must ensure that they have the delegated authority to do so. Where an employee of the City denies partial access to records and does not have the written authority to do so, the City is deemed to have refused complete access to the records at issue. The City must adhere to the delegation of authority. Where circumstances change, the City must revise the delegation of authority.

RESPONSIBILITIES OF THE HEAD (CITY CLERK)

The Act places certain administrative and reporting requirements on heads of institutions. These include:

- Meeting time limits and notification requirements;
- Considering representations from third parties who may be affected by the disclosure of the records;
- Making decisions about the disclosure of records and responding to access requests;
- Determining the method of disclosing records;
- Responding to requests for correction of personal information;
- Calculating and collecting fees;
- Where necessary, defending decisions made under the Act at an appeal; and
- Administering the privacy provisions of the Act.

Each of these duties will be discussed in more detail elsewhere in this Manual. The following administrative requirements are discussed below:

- Preparing and making available descriptions of the general types of records and personal information banks maintained by the City;
- Filing of an annual report with the Information and Privacy Commissioner.

INFORMATION AVAILABLE TO THE PUBLIC (SECTIONS 25 AND 34)

The City must prepare and make available descriptions of the City's records and personal information banks. These descriptions are intended for use by the public to determine the information generally maintained by the City. Accurate record descriptions enable a requester to submit a more detailed request, thus simplifying the response process.

The records descriptions should be made available in a publicly available place or a variety of places such as at the City Clerk's Office, at City libraries and on the City's

web page.

The City must ensure that the descriptions of records and personal information banks are amended as required to ensure that the information is accurate (subsections 25(2) and 34(2) of the Act.

The description of records and personal information banks must include:

- A description of the organization and responsibilities of the City;
- A listing of the general types or classes of records in the custody or control of the City;
- An index describing all the personal information banks in the custody or control of the City including:
    - the name and location of the personal information bank;
    - the legal authority for it;
    - a description of the types of personal information in the bank;
    - how the information is used on a regular basis;
    - to whom the personal information is disclosed on a regular basis;
    - the categories of individuals about whom personal information is maintained; and
    - the policies and practices about the retention and disposal of the personal information.
- the title, address and telephone number of the head; and
- the address to which a request for access to records should be made.

The records descriptions required by the Act need not be complex or lengthy and existing descriptions can be used, such as a file plan.

REPORT TO THE COMMISSIONER

Section 26 of the Act requires the head to provide an annual report to the Information and Privacy Commissioner. The report must set out:

- the number of requests received by the City;

- the number of refusals by the head to disclose a record, the provisions of the Act under which disclosure was refused and the number of occasions on which each provision was invoked;
- the number of uses or purposes for which personal information is disclosed if the use or purpose is not included in the statements of uses and purposes set out in the Personal Information Bank Index;
- the amount of fees collected under Section 45 of the Act; and
- any other information indicating an effort by the City to put into practice the purposes of the Act.

FREEDOM OF INFORMATION COORDINATOR

The City Clerk has designated the Freedom of Information Coordinator, under the direction of the Manager, Records & Information Management, to coordinate access and privacy activities. At the City of Brampton, this responsibility includes training of staff, the development of procedures for the administration of the Act, collecting the necessary information for the General Classes of Records and Personal Information Bank indices and making decisions on requests under the Act.

RECORDS MANAGEMENT

Improvement in records management systems throughout municipalities, local boards and commissions, is one of the major long term benefits of the Act. The public has a right to expect that each institution knows what records are in its custody or control and where the records are located so that they can easily be retrieved.

The Information and Privacy Commissioner has stressed the need for institutions to develop and maintain up-to-date retention schedules. Search time can be reduced significantly when it can be determined if a record has been destroyed by means of a records destruction certificate or other such document.

Section 3 of this Manual further addresses records management topics such as custody and control of records, including political and other elected officials' records.

SECURITY AND CONFIDENTIALITY OF RECORDS

Regulation 823, Section 3 requires measures to prevent unauthorized access to the City's records and to protect against inadvertent destruction of records. The regulation and guidelines are intended to apply to access and security considerations in the day-to-day administration of the City's records, rather than access to records in response to requests under the Act.

ACCOUNTABILITY

An important first step to establish reasonable measures is to assign responsibility and accountability for the security of the institution's records. In the City of Brampton, this responsibility rests within each department. The assignment as to who is responsible for security of records should be documented, and appropriate training and awareness should be provided to affected staff.

DETERMINING SECURITY REQUIREMENTS

Before measures to protect records from unauthorized access can be established, the City must determine the degree to which access to its records should be controlled.

Although it may be necessary to determine appropriate levels of access to individual documents or files, usually this determination is on the basis of record series. When considering access controls for record series, the level of security must be appropriate for the most sensitive information in the series.

All relevant factors must be taken into account in determining whether access to records should be controlled, and the scope and extent of those controls, including:

- whether or not exemptions are likely to apply to the records;
- the nature of the exemptions (mandatory or discretionary) which may apply;
- the circumstances under which the records were supplied to or created by the institution;
- possible harms which may result from unauthorized access;
- the need to protect the record from tampering; and

- the need to protect unique or original records.

SECURITY MEASURES

In identifying security measures, the head must balance the cost and complexity of such measures against the possible harms resulting from unauthorized access. Security measures should be appropriate to the nature of the record and to the level of security required.

For paper records, security measures can include:

- clean desk policies – desks should be locked when unattended;
- locking file cabinets, which are locked when unattended and where key distribution is limited and documented;
- central file stations with log-in and log-out procedures for files, accompanied by restriction on the making of copies;
- locked file room with access controlled by file room staff;
- coded file labels, labels using numeric or alpha-numeric codes rather than descriptive texts;
- inclusion of security provisions in contracts with outside suppliers of records storage and disposal services;
- record distribution/circulation policies which limit the production and circulation of records to staff on a need-to-know basis; and
- policies and procedures for using facsimile machines, including policies on types of information which should not be faxed, staff access to, and physical placement of fax machines. Checking procedures such as ensuring that the document is being sent to the correct number prior to sending documents should also be developed.

For electronic records, security measures should include:

- positioning terminals in such a manner that passers-by cannot read information displayed on the screen;
- logging off when leaving desk unattended;
- password protection for electronic systems, with policies in place governing the assignment, use and deletion of user identification and passwords;
- encryption of transmitted data or developing guidelines for transmitting confidential information, for example, guidelines for

the use of e-mail;

- tracking systems which monitor the use of data, and which identify system user; and
- inclusion of security provisions in contracts with outside suppliers of information technology services.

The head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it. This applies not only to paper records, but to all electronic data. The City must determine which groups of staff need to have access to a particular class or series of records in the performance of duties and take steps to ensure that access is limited to those groups.

Regulation 823 also requires institutions to ensure that reasonable measures to protect the records from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

If records are inadvertently destroyed before their proper disposal date, as specified in the City's Retention Schedule (By-law 307-2010) requesters are deprived of their right of access under the Act to those records. The head must take all reasonable steps to protect the records from accidental destruction.

In determining reasonable steps, the following factors should be considered:

- the media of the record (protective measures appropriate for paper records, for instance, may not be appropriate for other media);
- whether copies of the record exist;
- whether the original of the record is inherently valuable (such as archival records or signed documents);
- how vital the record is to the functions of the City;
- the cost of replacing or recreating the record; and
- the cost of available protective measures.

Some steps which might be considered to protect records from inadvertent destruction include:

- making regular back-up copies (disks, photocopies, microfilm), with a copy stored at a site separate from the original working copy;
- ensuring that a copy of all the City's vital records (by-laws, Council minutes,

etc.) are stored at an off-site facility regardless of the media;

- using fire-resistant file cabinets;
- locating record storage/computer operations away from areas where fire or water damage is more likely to occur (for instance, away from exposed pipes);
- raising records and records-producing equipment off the floor to prevent flood damage;
- installing smoke detectors and fire extinguishing equipment (it should be noted that some automatic fire extinguishing systems such as water sprinklers, may themselves pose a hazard to records and computers; and
- ensuring that storage facilities and maintenance practices are appropriate to the record's media (magnetic media, for instance, are especially vulnerable to inadvertent destruction or damage through improper storage). Similarly because magnetic media is often tied to a particular operating system and set of hardware, data stored on that media may not be usable if the operating system or hardware is no longer available. Steps should be taken to ensure that data on such systems can be migrated to newer systems.

PART 3: ACCESS PROCEDURES

INTRODUCTION

This part discusses general information about access, requests under the Act, and how to process requests for access to records. It is divided into the following sections:

- Right of Access
- Confidentiality Provisions
- Existing Information Practices
- Copyright Act
- Obligations to Disclose
- Requests under the Act
- Processing Requests
- Locating and Reviewing the Records
- Granting and Denying Access
- Access to Own Personal Information
- Checklist of Steps in Processing a Request

RIGHT OF ACCESS

OVERVIEW

The right of access applies to an existing record which is defined in Section 1. There is no obligation to create a record in response to a request under the Act, except in certain circumstances involving information maintained on electronic systems.

Other points to note regarding the right of access:

- The right of access is not restricted by residency, age or citizenship. An individual need not reside in a particular municipality in order to have a right of access to the records of that municipality;
- The Act is retroactive. It applies to any record that exists regardless of whether or not it was created prior to the Act taking effect on January 1, 1991 [subsection 52(1)]. This subsection also implies that the Act recognizes that although different requirements concerning disclosure of records may have been imposed pursuant to earlier legislation, once the *Municipal Freedom of Information and Protection of Privacy Act* came into force, these records were also subject to the Act; and

- The Act does not apply to records placed in the archives by private donors other than institutions defined in the Act.

CONFIDENTIALITY PROVISIONS

Subsection 53(1) of the Act provides that the *Municipal Freedom of Information and Protection of Privacy Act* prevails over a confidentiality provision in any other Act unless the other Act or this Act specifically provides otherwise.

The following confidentiality provisions prevail over this Act:

- ***Municipal Elections Act,* R.S.O. 1990, c.M.53, s.105.**

  "No person shall be allowed to inspect the contents of a ballot box in the custody of the clerk except under the order of a judge."

- ***Assessment Act,* R.S.O. 1990, c.A31, s.53(1)**

  "Every assessment commissioner or assessor or any person in the employ of a municipality or school board who in the course of the person's duties acquires or has access to information furnished by any person under section 10 or 11 that relates in any way to the determination of the value of any real property or the amount of assessment t hereof or to the determination of the amount of any business assessment, and who willfully discloses or permits to be disclosed any such information not required to be entered on the assessment roll to any other person not likewise entitled in the course of that person's duties to acquire or have access to the information, is guilty of an offence and on conviction is liable to a fine of not more than $2,000 or to imprisonment for a term of not more than six months, or both."

As a result, on January 1, 1991, all statutory confidentiality provisions ceased to be effective as non–disclosure provisions with the exception of those provisions cited in subsection 53(2) of MFIPPA.

EXISTING INFORMATION PRACTICES

A head may provide information without a formal request under the Act [subsection 50(1)]. The Act is not intended to replace the normal process of providing information. Providing information in response to informal oral or written inquiries will continue. The Act should only be used by the public in cases where information is not available through usual channels. However, when a request is made in writing under the Act for records that are not available through normal channels, the time limits and procedures

in the Act for responding must be followed.

The Act preserves access to information (except personal information) that was available to the public by statute, custom or practice immediately before the Act took effect [subsection 50(2)]. In other words, any information that was available to the public before January 1, 1991, continues to be available.

For example:

> Section 253 of the *Municipal Act* provides that the clerk shall maintain certain official records of the City. Section 254 states that the clerk shall provide access to the records specified in section 73 to any member of the public, subject to the *Municipal Freedom of Information and Protection of Privacy Act*. This means that given subsection 50(2) of the Act, preexisting access continues except in respect of personal information. Therefore, if a record falls under the pre-existing access provision, a formal request under the Act is not necessary.

Personal information is excluded from the pre-existing access provision. Disclosure of personal information is governed by sections 14, 32, and 38 of the Act.

COPYRIGHT ACT

Subsection 32(1)(i) of the federal *Copyright Act* provides that the disclosure of a record pursuant to a freedom of information request is not a violation of copyright. Therefore, this provision means that copies of architects' plans, drawings or specifications may be provided in response to a request under MFIPPA, unless another exemption applies to the record.

The person to whom the record is provided is still bound by copyright. When providing access to architects' records, an institution should:

- Stamp all plans released under the Act with the phrase "Copyright Act applies to use and reproduction"; and
- Ensure the author is associated by name with the document by including the title block or other indication of authorship on copies of documents released.

OBLIGATIONS TO DISCLOSE

GRAVE ENVIRONMENTAL, HEALTH, OR SAFETY HAZARD (SUBSECTION 5(1))

The Act requires the head to disclose a record that reveals a grave environmental, health, or safety hazard to the public, and where it is in the public interest to do so. In this provision:

- Grave means serious, likely to produce great harm or danger;
- Public interest includes the interests of the local community in general and not of any particular individual or group of individuals; and
- The information must be in record form.

If these conditions are met, the record must be disclosed as soon as possible. There is no requirement that a request under the Act be made before the head is required to act.

For example:

> Where the head possesses records indicating that a beach is unsafe because of high levels of pollution, he or she is obliged to alert the public to the danger.

Before disclosing a record, the head must give notice to any person to whom information in the record relates if it is reasonable to do so in the circumstances [subsection 5(2)]. The notice need not be in writing. Due to the urgency of the circumstances contemplated, the head is not required to wait for any prescribed period before disclosing the record or obtaining any representations.

This section applies despite any other provision of the Act.

COMPELLING PUBLIC INTEREST (SECTION 16)

Where certain exemptions apply to a record, disclosure may be required if a compelling public interest in the disclosure of the records clearly outweighs the purpose of the exemption. This provision applies to the following exemptions:

- Advice or recommendations (section 7);
- Relations with governments (section 9);
- Third party information (section 10);
- Economic and other interests (section 11);

- Danger to safety of health (section 13); and
- Personal privacy (section 14).

This section does not apply to exemptions dealing with records of closed meetings (section 6), law enforcement (section 8), solicitor-client privilege (section 12) or published information (section 15).

The interest in disclosure must be compelling, i.e. strong or overwhelming. The public interest must also clearly outweigh the purpose of the exemption. There is a balancing required by weighing the public interest against the purpose of the exemption. The results of that balancing test must be clear and definitive.

A compelling public interest has been found to exist, where, for example:

- The records relate to the economic impact of Quebec separation (Order P-1398), upheld on judicial review in *Ontario (Ministry of Finance) v. Ontario (Information and Privacy Commissioner);*
- The integrity of the criminal justice system has been called into question (Order P-1779);
- Public safety issues relating to the operation of nuclear facilities have been raised (Order P-1190), upheld on judicial review in *Ontario Hydro v. Ontario (Information and Privacy Commissioner);*
- The records contain information about contributions to municipal election campaigns (*Bombu v. Ontario (Assistant Information and Privacy Commissioner);*

A compelling public interest has been found NOT to exist where, for example:

- A significant amount of information has already been disclosed and this is adequate to address and public interest considerations (Orders P-532, P-568);
- There has already been wide public coverage or debate of the issue, and the records would not shed further light on the matter (Order P-613).

Both the head and the Information and Privacy Commissioner can determine if the compelling public interest provision applies to the disclosure of a record.

WHAT IS A REQUEST?

Under the Act, a request for access to records must be made in writing and must provide sufficient detail to enable an experienced employee of the City to identify he record(s) requested [subsection 17(1)].

If an individual is seeking access to his or her own personal information, the request must also identify the personal information bank or the location of the personal information being requested [subsection 37(1)]. If, after a thorough search, the City cannot locate the requested personal information and the requester cannot provide any credible evidence to support the existence of records, the records are deemed not to exist in a personal information bank.

Sometimes a request might be in the form of a question. For example, a requester might write, "Does the municipality have any information about municipal swimming pools?" In this situation, it is unlikely that the City could determine what information the requester wants. For this reason, requests in the form of questions are not generally acceptable and should be clarified with the requester before proceeding to process the request.

There is a prescribed form for access requests, but a letter that makes reference to the Act is considered a request.

A request for access to hardcopy records must be for records that exist at the time a request is received. There is no requirement to compile information from a number of records to create a new hardcopy record in response to a request.

If the City receives a request for access to a record that was destroyed according to the retention by-law, the requester would be advised that the record does not exist.

A request may also be made for access to records that are capable of being produced from a machine-readable record using the hardware, software and technical expertise normally used by the City. Requests for machine readable records are subject to R.R.O.1990, Reg. 823, Sec. 1.

TRANSLATING REQUESTS

The Act does not require that records be translated into the language of the requester.

CLARIFYING REQUESTS

The City is obligated to assist the requester to clarify the request where the request does not sufficiently describe the record sought. Clarifying a request is helpful to both the City and the requester. After a request has been clarified, it should be clear to each party what records are being requested [subsection 17(2)].

Appendix 1 contains a sample letter that can be sent to a requester when a request needs to be clarified.

WHO CAN MAKE A REQUEST?

Any person can make a request for access to records. In this instance, a person includes individuals and organizations such as corporations, partnerships and sole proprietorships. The right of access is not limited by citizenship or place of residence.

There are situations where one person represents another person. The Act provides that any right or power conferred on an individual by the Act may be exercised by:

- The personal representative of a deceased person only if the exercise of the right or power relates to the administration of the person's estate. The personal representative would be the executor named in a will or if there is no will, the administrator appointed by a court [subsection 54(a)];
- A committee for a person if one has been appointed or the Public Trustee. A committee can be appointed by a court for a person who is incapable of managing his or her own affairs. The Public Trustee may become a person's committee under the *Mental Health Act* or the *Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act, 2008* [subsection 54(b)];
- The person having lawful custody of a child under the age of 16 [subsection 54(c)]; or
- A person with the written consent of the individual.

The rights and powers which an individual may exercise include the right to make access requests, the right to consent to the collection, use and disclosure of personal

information and the right to request correction of personal information.

PROCESSING REQUESTS

A records management system that includes a filing system and storage, retrieval and records retention procedures is necessary to process requests for access to information.

TIME LIMITS

In general, requests for access to records must be dealt with within 30 calendar days from the date a complete request is received (section 19). A complete request is one which has been clarified or one which provides sufficient detail to allow the institution to understand what information is being requested. The 30-day time period does not start to run until the day after the complete request is received. If a time limit under the Act expires on a Sunday or statutory holiday the time limit is extended to the next day which is not a Sunday or statutory holiday.

Where a broad request is received which is subsequently narrowed by the requester, the 30-day time period begins on the date the original broad request was received.

Where the original broad request provided sufficient detail regarding the nature of the records being requested, the request is deemed to be merely narrowed, not clarified.

For example:

> An individual requests the results of a police investigation, including all correspondence between the police agency and an outside organization relating to a specific case. The requester later limits his request to one specific report regarding the case. This request would be considered narrowed and not clarified. The original request contained sufficient detail for a staff person to identify the records. In this case, the 30-day time limit would begin on the day the first (broad) request was received.

The time limit for responding to a request is automatically extended where notice is given to a third party under section 21.

It should be noted that courier companies cannot deliver to a post office box. A street address is required.

RECEIPT OF REQUEST AND OPENING REQUEST FILE

- Written access request received [17(1)];
- Sufficient detail [s. 17(1)];
- Should request be reformulated [s. 17(2)]; and
- Date stamp request, open file, begin tracking.

The first step when a request is received is to stamp the date on the request. This is important because of the time limits in the Act. Requests should be routed quickly to the Freedom of Information – Privacy Coordinator to ensure time is not wasted while the request works its way through to the appropriate person. A notice should be sent to the requester acknowledging receipt of the request.

The Freedom of Information – Privacy Coordinator will open a file.

A tracking and recording form should be used to record the actions taken to process a request. This form will indicate at a glance how a request was processed and what decisions were made with respect to the file.

DO WE HAVE THE RECORD?

- Does record exist? [s.17(1)]
- If machine readable record, can record be produced? [s. 2];
- Does the City have custody or control/greater interest in record? [s.18(2)(3)]; and
- Transfer request if necessary [s.18(2)(3)].

The Act applies only to records in the custody or control of the City.

In determining whether the City has custody or control of the record, consideration should be given to all aspects of the creation, maintenance and use of the particular record.

Custody of a record includes the keeping, care, watch, preservation or security of the record. While physical possession may not always constitute custody, it is the best evidence of custody.

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

Examples:

Records of the Works and Transportation Department are both in the custody and under the control of the City.

Political records belonging to a councillor may come within the custody and control of the City if these records are integrated with other files held by the City. When no steps are taken to separate the maintenance and storage of political records from the City's records and an employee has responsibility for their care, these records would be subject to the Act.

City of Brampton councillors are responsible for the maintenance and control of their own records, therefore, are not subject to the Act. However, where a record in the custody and control of a councilor is communicated to an officer or employee of the City, the record is now considered to be in the custody and control of the City.

The Mayor is considered to be an officer of the City and therefore, the Mayor's records are subject to the Act.

The following questions can be used to determine custody or control. This list is not exhaustive:

- Was the record created by an officer or employee of the City?
- What was the intended use of the record;
- Does the City have possession of the record either because it has been voluntarily provided by the creator or pursuant to a mandatory, statutory or employment requirement;
- If the City does not have possession of the record, is it being held by an officer or employee of the City for the purpose of his or her duties as an officer or employee?
- Does the City have a right to possession of the record?
- Does the content of the record relate to the City's mandate and functions?
- Does the City have the authority to regulate the use of the record?
- To what extent has the record been relied upon by the City?
- How closely is the record integrated with other records of the City?
- Does the City have the authority to dispose of the record?

Once custody or control has been determined, the Freedom of Information – Privacy Coordinator will proceed to gather and review the records to determine what will, or will not be released.

FORWARDING REQUESTS

If a request is received that would be more properly handled by another institution, depending on the circumstances, the Freedom of Information – Privacy Coordinator will either forward or transfer the request to the second institution.

If the City does not have the record(s) that were requested in its custody or control, reasonable inquiries must be made to determine if another institution has the record(s) (section 18).

For example:

> If the City receives a request for records about a program run by the Region of Peel, the City will contact the Region to see if it is appropriate to forward the request to the Region.

Under the Act, a request can also be forwarded to an institution covered by the provincial *Freedom of Information and Protection of Privacy Act* and vice versa. Institutions covered by that Act include provincial ministries, agencies, boards, corporations and commissions, community colleges and district health councils.

If the City does not know where to forward a request, the requester will be informed of this and advised what steps were taken to make the inquiries.

If it is determined that another institution has custody or control of the record(s), the request must be forwarded within 15 days of the date the request was received. The requester must also be notified that the request has been forwarded to another institution [subsection 18(2)(b)].

TRANSFERRING REQUESTS

There are cases where more than one institution has copies of the requested record(s). It may be determined that another institution has a greater interest in the record and in that case, the request may be transferred to the second institution. This includes provincial entities (section 18). An institution is under no obligation to transfer the request but may do so if it wishes.

Another institution has a greater interest in the record if:

- The record was originally produced in or for another institution; or
- If the record was not originally produced in or for another institution, the other institution was the first institution to receive the record or a copy of it.

For example:

> Both the City and a provincial government ministry might have a copy of an environmental impact study that was originally prepared for the provincial government. In such a case, the City could decide to transfer the request to the provincial ministry.

If it is decided to forward or transfer a request, it is important to act quickly as the 30-day time limit begins when the request is received by the first institution and continues to run before it is forwarded or transferred to the second institution. Due to time constraints, when transferring or forwarding a request, the Freedom of Information – Privacy Coordinator should immediately telephone the second institution. The second institution has the remainder of the 30-day period to respond [subsection 18(5)]. The time for responding does not stop running while the request is in transit, however, the second institution may send a notice to an affected third party; require a time extension or issue a fee estimate, all of which change the original deadline.

The City cannot forward or transfer a request to a federal department. The requester must be instructed to resubmit the request under the federal *Access to Information Act* or the *Privacy Act.*

For example:

> All records of indictable criminal convictions, supported by fingerprints are held by the RCMP. While Provincial and Municipal police agencies have access to Criminal History Information, an individual requiring an official copy of their own history must be directed to submit such a request to the RCMP, supported by their fingerprints. If the request was made to a municipal or provincial police agency, it cannot transfer such request. It must be resubmitted to the federal department.

The City must notify a requester if it forwards or transfers a request to another institution [subsection 18(3)]. Documentation of such transfer must be retained.

- Potential exemption? [s.6-15];
- Third party notices and representations required? [s.21];
- Extension (and notice) required?[s.20];
- Fee estimate over $100? [s.45(3)];
- Deposit required?; and
- Suspend 30-day count?.

Once it is determined by the Freedom of Information – Privacy Coordinator that it is appropriate to respond to a request, the search for the requested records starts; records are examined and a decision made as to what will be released. During the review of the records, the Freedom of Information – Privacy Coordinator may find it necessary to extend the time period to respond to a request, notify the affected parties and/or issue a fee estimate. In these instances the time period for processing the request is suspended or extended.

SEARCH FOR RECORDS

Searches for records responsive to a request should include, where practicable, enquiries of staff responsible for the issue(s) the records concern at the time the records were created or might have been created. Enquiries should also be made for any briefing materials relevant to the issue.

The following should also be considered when searching for records:

- Identify the specific files and data banks that should be searched;
- Determine whether records and/or types of records the requester claims should exist within the City's files, are contained in the files that were searched; and
- Identify and assess whether other files and data banks might contain records responsive to a request.

Steps taken to locate a record can be verified by affidavit evidence and by the tracking sheets prepared by persons who conducted the search.

TIME EXTENSIONS

A head can extend the 30-day time limit for responding to requests for a period that is "reasonable" in the circumstances (section 20), if one of two conditions exist:

- The request is for a large number of records or necessitates a search through a large number of records and meeting the time limit would unreasonably interfere with the operations of the City; or
- Consultations with persons outside the City are necessary to comply with the request and cannot be completed within the time limit.

Under the first condition for extending time, interference with the operations of the City must relate to a request for a large number of records or require an extensive search through a large number of records.

Under the second condition, the City may need to consult with persons outside such as the provincial government to possibly determine if the exemption from disclosing records under section 9 (relations with governments) applies to the requested records.

The 30-day time limit can only be extended once.

An institution cannot combine numerous requests and deal with them en bloc rather than individually as requested and then request a time extension because a search through numerous records or consultation is necessary.

The Act provides a clear and relatively short time limit for responding to requests. The time limit can be extended only in the circumstances set out in section 20.

There are two legitimate courses of action that can be considered when compliance with the time limit set out in the Act places an excessive strain on resources. They are as follows:

- Negotiate with requesters who file numerous requests to prioritize responses (possibly in sequence).
- If at all possible, allocate resources in such a way that it can import on an emergency basis additional staff to assist the Freedom of Information – Privacy Coordinator in situations in which there is a sudden influx of requests.

Each request should be considered separately and a decision made on a case-by-case basis, whether a request's volume justified a section 20 extension.

If the time limit is extended, the requester must be given written notice [subsection 20(2)] that sets out:

- The length of the extension;

- The reason for the extension;
- The fact that the requester can ask the Information and Privacy Commissioner to review the decision to extend the time period.

NOTICES TO AFFECTED THIRD PARTIES

There will be records that contain information concerning a person other than the requester. In this instance, a person may be another individual or a corporation, partnership or other legal entity considered to be a person. Before granting access to a record that affects a third party, written notice must be given to third parties to whom the information relates. The information is considered to affect a third party if:

- There is reason to believe that the record contains third party information referred to in subsection 10(1); or
- The record contains personal information the City has reason to believe might, if released, constitute an unjustified invasion of personal privacy [subsection 14(1)(f)]. (See Section 4, Exemptions)

A notice to an affected party gives that part an opportunity to make representations about the proposed disclosure of records that affect them.

If the records are going to be released, then the affected party will be given a notice [subsection 21(2)]. The notice must contain:

- A statement that the head intends to disclose a record or part of a record that may affect the interests of the person;
- A description of the contents of the record or the part that relates to the third party; and
- A statement that the person may, within 20 days after the notice is given, make representations to the head as to why the record or part of the record should not be released.

The notice must be given within the initial 30-day period after a complete request is received or, if there has been an extension of time under subsection 20(1), within that extended period.

The third party has 20 days after the notice is given to make representations to the head [subsection 21(5)]. Representations are to be in writing. After the representations are made (or after the 20-day period for representations has elapsed), the head must

decide within 10 days whether or not to disclose the record.

If affected third parties have been notified, this will delay the processing of a request. The requester must be notified of this delay [subsection 21(4)]. It is advisable to do this at the same time that the affected third party is notified. The notice to the requester must state:

- That the disclosure of the record or part may affect the interests of a third party;
- That the third party has an opportunity to make representations concerning the disclosure;
- That a decision will be made within 30 days if the record or part will be released.

FEE ESTIMATES/INTERIM NOTICES

In processing a request, it may become clear that fees will be involved. If it appears that the costs of processing the request will be over $100, the requester must be given a fee estimate before access is given to the records [subsection 45(3)]. Section 19, however, requires that the requester be notified within 30 days of his or her decision regarding access to the requested records.

Therefore, both the fee estimate notice and a notice of decision on access must be issued within the 30-day period (unless there has been a time extension or a third party notice issued). This can be handled in two ways:

- Where the number of records is not large or unduly expensive to retrieve, it will be a relatively straightforward matter to review the records and provide the requester with both a detailed fee estimate and a section 19 decision about the disclosure within the 30-day period. In this case, the fee estimate amounts to the same as a final fee statement, and no records would be severed, copied or released until the fee is paid or waived.
- There may be cases where it would be unduly expensive to gather and review the records to make a decision before a fee estimate is agreed to and deposit paid. There may be, for instance, requests involving large volumes of records or records housed in a variety of locations.

In such a case, the requester is provided with a notice containing an interim decision on access under section 19 and a fee estimate under subsection 45(3). The decision on access is an interim decision because it has not been possible to fully determine whether and how exemptions will apply. Both the interim decision and fee estimate are based on one of the following methods:

- Consulting with a staff member who is familiar with the type and contents of the records; or
- Basing the interim decision and fee estimate on a representative (as opposed to haphazard) sampling of the records.

The interim decision lets the requester know that certain exemptions may apply to the records. Since this is not a final decision, it is not binding on the City and is not subject to appeal. However, the fee estimate may be appealed [subsection 45(5)].

The time period for responding to a request is suspended after the notice containing the interim decision and fee estimate is issued. The time begins to run again once a deposit is received from the requester of a fee waiver is granted, or the issue of fees has been resolved after an appeal to the Information and Privacy Commissioner.

In all cases, the fee estimate should be based on an examination of the records and should provide the requester with as much information as possible about the costs that will be incurred in processing the request. The estimate should also indicate that the requester may ask for a fee waiver.

Section 6 deals with chargeable costs, calculation of fees, deposits and fee waivers.

GRANTING AND DENYING ACCESS

- Retrieve records
- Do exemptions apply?
- Compelling public interest/ [s. 16]
- Determine access method (original vs. copy) [s.23]
- Sever records where required [s.4(2)]
- Determine fee [s.45]
- Fee to be waived? [s.45(4)]
- Provide notice re access, exemptions and fee [s.19,22(3)]
- Collect fee where applicable;
- Provide record or part of record to requester, or
- Provide notice that access is denied or record does not exist [s.22(1)]
- Close file

Once a decision has been made about access, written notice of the decision must be given to the requester and any affected third parties. The notice must be given within the 30-day time period (or within the extended time period, if any).

If third party notices have been given, the notice of a decision on disclosure cannot be given until:

- A response from a third party has been received; or
- After the 20-day period in which a third party can respond to a third party notice has elapsed [subsection 21(7)]

If a decision has not been given to the requester within the 30 days (or within the timeframes extended under section 20, or subsection 21(7), third party notice procedure), the head is deemed to have refused access to the record. The requester may then appeal to the Information and Privacy Commissioner.

METHODS OF SEVERING RECORDS

If part of a record that has been requested falls within one of the exemptions and other information in the record can be disclosed, the City must disclose as much of the record as possible [subsection 4(2)].

Exempt material can be severed using electronic redaction or by using removable tape.

Whenever records are severed, copies of the severed records must be kept on file as a record of what parts of records were released. Un-severed (i.e. original) records must also be kept on file.

GRANTING ACCESS TO RECORDS WHERE THERE IS AN AFFECTED THIRD PARTY

If, after representations have been received and considered (or the time period for making representations has expired), it is decided under subsection 21(7) to release a record in whole or in part that affects a third party, the requester and third party must be notified that:

- The person to whom the information relates may appeal the decision to the Commissioner within 30 days; and
- The requester will be given access to the record unless an appeal is filed within the 30 days after the notice is given [subsection 21(8)].

The notice should be very clear that the requester will be given access to the record or part unless the affected third party appeals to the Commissioner within the 30-day time

limit.

MAKING THE RECORD AVAILABLE

A requester who is granted access to a record (in whole or in part) is given a copy unless the requestor has specified the preference to review the original record.

ACCESS TO ORIGINAL AND COPYING

Sometimes a requester may ask to examine the original record or part rather than have a copy. This shall be allowed if it is feasible [section 23].

Once the requester has examined the original or part and wants parts of it copied, the requester must be given a copy of what is wanted, unless it would not be reasonable to reproduce the record or part because of its length or nature.

If access to the original record compromises the security of the record, it may not be reasonable to provide access to the original.

For example:

> Archives might have genealogical records in the original form and on microfiche. Given the age and condition of the original documents, it might not be practicable to give access to them.

Requesters are charged for photocopies.

GRANTING ACCESS TO RECORDS IN THEIR ENTIRETY

If a record is to be released in its entirety, a requester is informed of the decision to grant access [subsection 19(1)].

If access is granted to someone who has requested his or her own personal information, the identity of the person must be confirmed to ensure that the personal information is disclosed only to the person to whom it relates or to that person's representative.

DENYING ACCESS TO RECORDS OR PARTS OF RECORDS

If the records or part of the records fall within an exemption, the head must refuse to disclose the information if the records or parts are subject to a mandatory exemption. The head may refuse to disclose them if they fall within a discretionary exemption, but

does have the option of releasing the records. A notice of refusal [section 22] must state:

- If the record does not exist, that the record does not exist and the requester may appeal the question of whether or not the record exists to the Information and Privacy Commissioner;
- If the record exists:
    - The specific provision of the Act under which access is refused;
    - The reason the provision applies to the record;
    - The name and position of the person responsible for making the decision; and
    - That the requester can appeal the decision to the Information and Privacy Commissioner.

The withheld record must be described sufficiently to allow a requester to make a reasonably informed decision whether or not to appeal. This should include a detailed description of the withheld record(s) or an index. Care should be taken not to disclose any names when describing the withheld records).

FRIVOLOUS REQUEST [SECTION 20.1][SECTION 4(1)(B)][5.1 OF REGULATION 823]

If the City decides to refuse a request for access to a record because it is of the opinion that the request for access is frivolous or vexatious, the notice under section 19 shall state:

- That the request is refused because the head is of the opinion that the request is frivolous or vexatious;
- The reasons for which the head is of the opinion that the request is frivolous or vexatious; and
- That the person who made the request may appeal to the Commissioner under subsection 39(1) for a review of the decision.

The City shall conclude that the request is frivolous or vexatious if:

- The City is of the opinion on reasonable grounds that the request is part of a pattern of conduct that amounts to an abuse of the right of access or would interfere with the operations of the institution; or
- The City is of the opinion on reasonable grounds that the request is made in bad

faith or for a purpose other than to obtain access.

REFUSING TO CONFIRM OR DENY THE EXISTENCE OF A RECORD

In certain circumstances when access to records has been refused, an City may also refuse to confirm or deny the existence of a record, if the record relates to law enforcement [subsection 8(3)], or if disclosure of the records would constitute an unjustified invasion of personal privacy [subsection 14(5)].

The notice of refusal [subsection 22(2)] to the requester must state:

- That the City refused to confirm or deny the existence of the record;
- The provision of the Act (either subsection 8(3) – law enforcement – or subsection 14(5) – unjustified invasion of personal privacy, on which the refusal is based;
- The name and office of the person responsible for making the decision;
- That the requester may appeal the decision to the Information and Privacy Commissioner.

There may be instances where acknowledging that a record exists could hamper law enforcement matters or invade and individual's privacy.

Examples:

A social services department that acknowledges that a record about a particular individual exists may invade that individual's personal privacy because the acknowledgement would be a strong indication that the person was, or is, in receipt of social assistance.

A police agency that acknowledges that a record exists about a particular individual may compromise an investigation before a decision is made to lay a charge.

ACCESS TO OWN PERSONAL INFORMATION [SUBSECTIONS 36(1) AND 37(1)]

The Act provides an individual with a right of access to his or her own personal information, whether or not the information is held in a personal information bank.

A request must be in writing and must identify the personal information bank where the record is held or the location of the personal information. The personal information bank index will assist the requester in locating the specific personal information bank that contains his or her information.

IDENTIFICATION REQUIRED FOR ACCESS

When releasing personal information upon request, the requester's identity must be verified and it must be ensured that the records are safely transmitted. It is up to the institution, on a case by case basis to satisfy itself as to a requester's identity before releasing personal information to the individual. This can be done by various means, for example:

- Ask for photo ID – driver's licence or a passport;
- Spelling of names, address, telephone number, signature, handwriting, etc. should be reviewed and compared with the information the institution has on file;
- Question the requester on unique personal information contained in the record itself; ie, a Health Unit may ask for an Ontario Health Card Number.

Personal attendance should not be the standard form of verification used as many individuals do not possess photo ID.

COMPREHENSIBLE FORM

Personal information must be provided to the individual in a comprehensible form and in a manner which indicates the general terms and conditions under which the information is stored and used [subsection 37(3)].

Personal information may be stored in such a manner that it would not be readily understood by the individual. For instance, information produced in coded form is meaningless without providing the key to the code. Information provided in response to a request under the Act, should be decoded, or the code or key provided so the information can be understood by the person.

CORRECTION OF PERSONAL INFORMATION [SUBSECTION 36(2)]

Every individual who is given access to his or her own personal information has the right to request correction of the personal information if he or she believes that the information contains errors or omissions [subsection 36(2)].

The right of correction applies only to personal information to which an individual is given access. The meaning of the word *correction* incorporates three elements:

- The information at issue must be personal information; and
- The information must be inexact, incomplete or ambiguous; and
- The correction cannot be substitution of opinion.

If the correction sought is merely a substitution of opinion, then it will not qualify as a correction to personal information. A statement of disagreement may be attached. The Access/Correction Request form may serve as a statement of disagreement.

Once the City has been asked to correct personal information, the City must consider whether or not the information submitted for correction can be verified. In some cases, documentary proof should be requested, especially if the information impacts on an individual's financial status or eligibility for a benefit.

If a requested correction of personal information is not made, the individual should be informed of the reasons the correction was not made and that the individual has the right to:

- Appeal the decision to the Information and Privacy Commissioner
- Require that a statement of disagreement be attached to the information; or
- Have any person or body to whom the personal information was disclosed within the last twelve months notified of the correction or statement of disagreement [subsection 36(2)].

The Act does not specify the time period within which a response must be provided to a request for correction. The general 30-day period is considered reasonable.

EXERCISE OF RIGHTS OF DECEASED PERSONS, CHILDREN, ETC. [SECTION 54]

Any right, including the right of access to information, conferred on an individual by MFIPPA may be exercised by another person in the following circumstances:

- Deceased individuals by the individual's personal representative if it relates to administration of the individual's estate;
- Individuals under Power of Attorney: by the individual's attorney or guardian of person or property; or
- Individuals under age of 16: by a person who has lawful custody of the individual

CHECKLIST FOR PROCESSING A REQUEST

A REQUEST IS RECEIVED

1. Is the request in writing? [subsection 17(1)]
2. Does it provide sufficient detail to enable identification of the requested record(s)?

   If not, assist the requester to rewrite the request [subsection 17(2)].
3. Date-stamp the request, open a file and prepare a tracking form.

DO THE REQUESTED RECORDS EXIST?

1. Do the records exist or are they capable of being reproduced from a machine-readable record?

   If not, notify the requester that the records do not exist [subsection 22(1)(1)]
2. Do we have custody or control of the records?

   If not, make reasonable inquiries to determine where to forward the request, and forward it within 15 days of receipt. Notify the requester if the request is forwarded [subsection 18(2)].

   If you do not know where to forward the request, notify the requester that the records do not exist and that the requester can appeal to the Information and Privacy Commissioner [subsection 22(1)].
3. If the City and another institution have copies of the records, determine which one has a greater interest in the record and if appropriate, transfer the request to the other institution within 15 days of receiving the request. Notify the requester of the transfer [subsections 18(3) and (4)].

LOCATING AND REVIEWING THE RECORDS

1. Gather the records (or a sample of the records) along with a completed tracking form from the appropriate department and review them.
2. Determine if any exemptions apply.

3. Determine if more time is needed to process the request and if so, notify the requester [section 20].
4. Determine if the records affect the interests of a third party or parties and if so, send notices and give affected third parties an opportunity to make representations about the disclosure of records that affect them [section 21]. This will affect the deadline for responding to the request.
5. Determine if there will be a cost for processing the request and if the fee will be over $100, the requester must be given a fee estimate [subsection 45(3)].

PROCESSING THE REQUEST

1. Retrieve the records.
2. Determine what exemptions apply [sections 6-15].
3. Determine if the override provisions apply [sections 5, 16].
4. If required, sever exempt material from the records.
5. Determine what the final fee will be and if the fee will be waived [section 45].

GRANTING OR DENYING ACCESS TO THE RECORDS

1. If access to a record or part of a record is granted, determine the method of access (copy of original) [section 23].
2. If access is granted, give the requester notice regarding access [section 19].
3. If an affected third party is involved, give notice regarding access to third party and requester [subsection 21(8)].

   Note that the affected party has 30 days in which to appeal your access decision to the Commissioner. Access is not granted until the 30 days have expired and an appeal has not been filed.
4. Collect fee where applicable and provide record(s), together with an Index of Records.

OR

Give the requester a *notice of refusal,* if:

- The record does not exist;
- All or part of the record is exempt from disclosure; or
- The decision is to refuse to confirm or deny the existence of the records [section 22].

CORRECTING PERSONAL INFORMATION

1. If an individual requests the correction of personal information, verify the information to be corrected, correct it or permit a statement of disagreement to be filed.
2. If requested, notify recent users of the personal information of the correction or statement of disagreement [subsection 236(2)].

COMPLETE THE FILE

1. Complete documentation of the request and all actions taken.
2. Close the file, unless an appeal is commenced.

PROCESSING A REQUEST

STEP 1: RECEIPT OF REQUEST

- Written access request received [s.17(1)]
- Sufficient detail? [s.17(1)]
- City to assist in reformulating request? [s.17(2)]
- Date stamp request, open file, begin tracking

STEP 2: LOCATE RECORD

- Does record exist? [s.17(1)]
- If machine readable record, can record be produced? [s2]
- Does City have custody or control/greater interest in record? [s.18(2)(3)]

- Transfer request if necessary [s.18(2)(3)]

STEP 3: PRELIMINARY REVIEW

- Potential exemption? [s.6-15]
- Third party notices and representations required? [s.21]
- Fee estimate over $100? [s.45(3)]
- Deposit required?
- Suspend 30-day count?

STEP 4: PROCESS REQUEST

- Retrieve records
- Do exemptions apply?
- Compelling public interest? [s.16]
- Frivolous or Vexatious? [20.1]
- Determine access method (original vs. copy) [s.23]
- Redact records where required [s.4(2)]
- Determine fee [s.45]
- Fee to be waived? [s.45(4)]

STEP 5: GRANT/DENY ACESS

- Provide notice re access, exemptions and fee [s.19,22(3)]
- Where appropriate, provide third party notice and wait 30 days
- Collect fee where applicable

STEP 6: END

- Provide record or part of record to requester

Or

- Provide notice that access is denied or record does not exist [s.22(1)]
- Document request
- Close file

THIRD PARTY NOTICE AND REPRESENTATION PROCESS SECTION 21

REQUEST RECEIVED

Day 0	1. Where the City intends to release a record affecting the interest of a third party, the City must notify the affected third party within the original 30 days (unless the deadline has been extended under sec. 20).

NOTICE TO THIRD PARTY

Day 0	2. Once notice is given, a new timeframe begins. The third party has up to 20 days to make representations.
Day 20	3. After the 20 day representation period, the City has 10 days in which to make a decision. This brings the total number of days since the third party notice to 30.

NOTICE OF DECISION

Day 0	4. If the City decides not to release the record processing is finished and notice of decision is sent to requester and third party. If the City decides to release the record, the City must wait an additional 30 days to allow the third party to appeal to the Commissioner. If no appeal is filed in 30 days, the record is Released.

PART 4: EXEMPTIONS

INTRODUCTION

The exemptions to access are set out in sections 6 to 15, and 38. The City bears the burden of proving that an exemption is justified in the event of an appeal to the Commissioner [section 42].

Exemptions in sections 6 to 13 and section 15 apply to requests for general records. Exemptions in sections 14 and 38 apply to requests for access to personal information. The exemption in section 14 (personal privacy) applies for requests for access to another individual's personal information. The exemption in section 38 applies to a request by an individual for his or her own personal information. More than one exemption may apply to a requested record.

Some exemptions contain exceptions. Exceptions are provisions that limit the applicability of that particular exemption.

For example:

> Subsection 7(1) provides an exemption for advice and recommendations, however, subsection 7(2) provides exceptions to this exemption; a list of records that cannot be exempted under subsection 7(1).

Exceptions outlined in a section apply only to that section. However, another exemption may apply to the record.

SEVERABILITY

Where an exemption applies to only part of a requested record, the City must make available as much of the record as possible without disclosing the exempt portions [subsection 4(2)]. This is done by severing (redacting) the exempt portions from the record before it is released. Information not described in or pertinent to the request may also be severed before the remainder is made available.

MANDATORY AND DISCRETIONARY EXEMPTIONS

There are two types of exemptions in the Act: mandatory and discretionary. Mandatory exemptions impose a duty on the head to refuse to disclose a record. Mandatory exemptions begin with the words "a head shall refuse to disclose…". The head must determine whether facts exist or may exist that bring the record within the exemption. If grounds for the exemption exists, the head must refuse access, unless a compelling

public interest clearly outweighs the purpose of the exemption [section 16]. There are three mandatory exemptions:

- Relations with governments [section 9]
- Third party information [section 10]; and
- Personal privacy [section 14].

The remainder of the exemptions, sections, 6, 7, 8, 11, 12, 13, 15 and 38, are discretionary. Discretionary exemptions permit the head to disclose a record despite the existence of the exemptions. Discretionary exemptions are introduced by the words "a head *may* refuse to disclose…".

The Act requires a two stage process in determining whether a discretionary exemption is to be applied. First, the head must determine whether the record falls within the exemption; second, the head must decide whether he or she is willing to release the record, despite the existence of grounds for the exemption. A decision by a head to disclose information falling within an exemption is an exercise of discretion.

The compelling public interest provision must be considered in the case of the discretionary exemptions in section 7 (advice or recommendations), section 11 (economic and other interests) and 13 (danger to safety or health), if the head has decided not to exercise his or her discretion in favour of disclosure.

Discretionary exemptions may be applied by the head alone. In an appeal situation, if a head chooses not to claim a discretionary exemption, no other party to the appeal may claim one.

DRAFT BY-LAWS, RECORDS OF CLOSED MEETINGS [SECTION 6]

Subsection 6(1)(a) is a *discretionary* exemption which permits the head to deny access to a draft by-law unless the draft has been considered in an open meeting. The term *considered* involves examination or deliberation.

Subsection 6(1)(b) permits the head to prevent disclosure of a record which reveals the substance of deliberations of a closed meeting of council, board, commission or other body or a committee of one of them. There must be statutory authority to hold the meeting in the absence of the public.

If the subject matter of the deliberations is later considered in an open meeting, this exemption no longer applies to the record.

The exemption in 6(1) cannot be relied on if the records mentioned in subsection 6(1)(a) or (b) are over 20 years old. Unless another exemption applies, the record must be released upon request.

The compelling public interest override in section 16 does not apply to this exemption.

ADVICE OR RECOMMENDATIONS [SECTION 7]

Subsection 7(1) provides a *discretionary* exemption for records where disclosure would reveal the advice or recommendations of officers or employees of City or of consultants retained by the City. Officers or employees include those persons who work for the City or who perform duties under a contract of employment. The advice of an officer or employee of another institution cannot be exempted under this section, nor can advise of a volunteer.

The exemption is for advice or recommendations. There is some overlap between the terms advice and recommendations. *Recommendations* refer to formal recommendations about courses of action to be followed which are usually specific in nature and are proposed mainly in connection with a particular decision. *Advice* refers to less formal suggestions about particular approaches to take or courses of action to follow. The advice or recommendations must be communicated from one employee to another and must be made in the course of the deliberative process of decision-making and policy-making. An employee's memo to file has not been communicated and would not be included in this exemption.

Subsection 7(1) is not restricted to advice or recommendations given to the head.

Subsections 7(2) and (3) provide **exceptions** to the exemption in subsection 7(1).

Discussed immediately below are the types of records and information listed in subsections 7(2) and (3). A report or study in the following list means a completed document ready for presentation and would not include working papers used in preparation such as notes or preliminary drafts. For the types of records listed in subsection 7(2)(b) through (k), the record or part of it cannot be exempted under subsection 7(1), even if it contains advice or recommendations.

FACTUAL MATERIAL [SUBSECTION 7(2)(A)]

Records or parts of records containing essentially factual material must be disclosed.

Factual material means a coherent body of facts which can be separated from the rest of the advice or recommendations, for example, an appendix of factual information

supporting a policy document. Where factual material and advice or recommendations are contained in the same record, the advice or recommendations may be severed and withheld. However, it may not be possible to sever advice and recommendations and still leave meaningful factual information. In this circumstance, severing may not be appropriate, and the information would not be disclosed.

STATISTICAL SURVEY [SUBSECTION 7(2)(B)]

A statistical survey must be disclosed unless another exemption applies.

A statistical survey is a record showing the collection, analysis, interpretation and presentation of aggregate data in relation to a topic or issue which is the object of study, for example, a poll. Any information identifying individuals must be removed before the record is disclosed.

VALUATOR'S REPORT [SUBSECTION 7(2)(C)]

A valuator is someone with specific expertise appointed to determine or estimate the value, price or merit of an article. He or she need not be an officer of the institution. A valuator's report would include an appraisal of the value of real property.

ENVIRONMENTAL IMPACT STATEMENT [SUBSECTION 7(2)(D)]

An environmental impact statement or similar record must be disclosed.

An environmental impact statement is a record containing a technical assessment, including findings and conclusions respecting the social, cultural, economic and environmental consequences of projects such as buildings and highways.

REPORT ON PERFORMANCE [SUBSECTION 7(2)(E)]

A report or study on the performance or efficiency of the City is not exempt under subsection 7(1).

For example:

A final audit report, including its findings and conclusions would not be exempt.

FEASIBILITY STUDY [SUBSECTION 7(2)(F)]

A feasibility or other technical study, including cost estimate, relating to a policy or project is not exempt under subsection 7(2)(F)..

For a record to qualify as a feasibility study, it must be a study which is practicable, possible, capable of being done or accomplished and has a reasonable assurance of success.

For example:

A feasibility study for a micrographics program would not be exempt.

FIELD RESEARCH REPORT [SUBSECTION 7(2)(G)]

The exemption in subsection 7(1) does not apply to a report setting out the findings and conclusions of field research on an issue or problem which is undertaken before the formulation of a policy proposal.

PROPOSAL TO CHANGE OR ESTABLISH A PROGRAM [SUBSECTION 7(2)(H)]

This subsection requires disclosure of a final plan or proposal to change or establish a program, including a budgetary estimate, whether or not the plan or proposal is subject to approval.

Subsection 7(2)(h) must be considered in relation to the exemption in subsection 11(f). Subsection 7(20(h) refers to a final plan or proposal to alter or establish a program which provides a service to the public and which is developed or implemented to carry out the City's responsibilities. Subsection 11(f) relates to internal administrative arrangements relating to personnel which do not fundamentally alter the nature and content of the programs being delivered to the public.

COMMITTEE REPORT [SUBSECTION 7(2)(H)]

A report of a City committee must be disclosed unless another exemption applies to the record.

REPORT OF A BODY ATTACHED TO INSTITUTION [SUBSECTION 7(2)(J)]

The type of body referred to in this subsection is one that undertakes inquiries and makes reports or recommendations to the City and consists primarily of representatives from outside the institution. The phrase *attached to an institution* indicates that the body has been appointed or invited to meet and deliberate by someone in an institution with appropriate authority.

For example:

> A local grants committee established to make recommendations regarding the awarding of grants would be one such body.

REASONS FOR A FINAL DECISION SUBSECTION 7(2)(K)]

Unless another exemption applies, this exception requires the disclosure of the reasons for a final decision, order or ruling by an officer or employee of the City. This exemption applies regardless of whether or not the reasons are recorded in an internal memorandum or external correspondence.

RECORD MORE THAN 20 YEARS OLD [SUBSECTION 7(3)]

The City must release a record that is more than 20 years old. This subsection does not place an obligation on the City to retain a record for 20 years.

The compelling public interest provision in section 16 applies to this exemption.

LAW ENFORCEMENT [SECTION 8]

Section 8 provides a *discretionary* exemption for records relating to police and by-law enforcement investigations and certain other investigative, adjudicative and protective functions.

Subsection 8(1) provides an exemption where disclosure could reasonably be expected to interfere with law enforcement and certain other activities. Subsection 8(2) exempts certain types of law enforcement records. Subsection 8(3) provides that a head may refuse to confirm or deny the existence of records in subsections 8(1) and (2).

Subsections 8(4) and (5) set out exceptions to the exemptions.

Law enforcement is defined in subsection 2(1) of the Act. The phrase not only includes records relating to policing activities and prosecutions, but also records in respect of investigations, or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed. This definition encompasses records relating to the enforcement of federal and provincial statutes and municipal by-law.

For example:

> The enforcement of a property standards by-law by a municipality or the enforcement of a non-smoking by-law by a transit authority would constitute a law enforcement activity.

The term *could reasonably be expected to* as used in this section requires that the expectation of the harm coming to pass should the record be disclosed, not be fanciful, imaginary or contrived, but based on reason. By virtue of section 42, an institution must provide evidence to substantiate the reasonableness of the expected harm.

LAW ENFORCEMENT MATTER [SUBSECTION 8(1)(A)]

This exemption applies if disclosure could reasonably be expected to interfere with a law enforcement matter. To interfere with a law enforcement matter means that the disclosure would have the effect of hindering or impeding the conduct of a proceeding or the carrying out of a law enforcement activity.

Law enforcement matter refers to a proceeding or an activity that is within the scope of law enforcement as defined in subsection 2(1).

LAW ENFORCEMENT INVESTIGATION [SUBSECTION 8(1)(B)]

The City may refuse to disclose a record where the disclosure could reasonably be expected to interfere with an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

To interfere with an investigation does not mean that disclosure would altogether prevent a law enforcement investigation from taking place but rather that disclosure would frustrate or impede the carrying out of an investigation.

REVEAL INVESTIGATIVE TECHNIQUES [SUBSECTION 8(1)(C)]

The purpose of this exemption is to preclude access to information about the application of technology to investigate techniques where disclosure would undermine or jeopardize the effectiveness of such techniques.

REVEAL A CONFIDENTIAL SOURCE [SUBSECTION 8(1)(D)]

The City may refuse to disclose a record where the disclosure would reveal the identity of a confidential source of information in respect of a law enforcement matter, or disclose information furnished only by the confidential source.

For example:

> A person who complains against his or her neighbor in respect of a municipal by-law infraction is a source protected under the exemption.

SAFETY OF A LAW ENFORCEMENT OFFICER [SUBSECTION 9(1)(E)]

The City may refuse to disclose a record that would endanger the safety of a law enforcement officer or any other person.

Please see section 13, danger to safety or health for further information.

FAIR TRIAL OR IMPARTIAL ADJUDICATION [SUBSECTION 8(1)(F)]

This exemption prevents premature disclosure of information that could deprive a person of a fair trial or impartial adjudication. Once the proceeding has been completely disposed of (including appeals), the exemption no longer applies.

This subsection does not contain a reference to law enforcement and, accordingly, the exemption applies to proceedings that do not fall within the definition of law enforcement such as tribunals established by legislation to adjudicate individual or collective rights.

An example of such a tribunal would be the Social Assistance Review Board. To rely on this exemption, however, there must be evidence that the disclosure of the records would result in unfairness.

INTELLIGENCE INFORMATION [SUBSECTION 8(1)(G)]

This subsection exempts from disclosure records where the disclosure could reasonably be expected to interfere with the gathering of or reveal law enforcement intelligence information respecting organizations or persons.

CONFISCATED RECORDS [SUBSECTION 8(1)(H)]

This exemption applies where disclosure could reasonably be expected to reveal records confiscated by a peace officer in accordance with an Act or regulation.

ENDANGER THE SECURITY [SUBSECTION 8(1)(J)]

The City may refuse to disclose a record where the disclosure could reasonably be expected to endanger the security of a building or the security of a vehicle carrying items, or of a system or procedure established for the protection of items, for which protection is reasonably required.

For example:

A security audit is a record where disclosure would endanger the security of a system or procedure established for the protection of items.

FACILITATE ESCAPE [SUBSECTION 8(1)(J)]

Records are exempt where the disclosure could reasonably be expected to facilitate escape from custody of a person who is under lawful detention. Custody indicates that an individual is not free to leave a place of confinement without restriction. In general, any person held in custody pursuant to a valid warrant or other authorized order is under lawful detention.

CENTRE FOR LAWFUL DETENTION [SUBSECTION 8(1)(K)]

This provision exempts records where disclosure could reasonably be expected to jeopardize the security of a centre for lawful detention. This includes records containing details of previous investigations of escape attempts and details of security measures in place.

UNLAWFUL ACT [SUBSECTION 8(1)(L)]

Records are exempt where the disclosure could reasonably be expected to facilitate the commission of an unlawful act or hamper the control of a crime. Unlawful act means a contravention of a statute or regulation or of a municipal by-law.

OTHER LAW ENFORCEMENT EXEMPTIONS

Subsection 8(2) specifies certain records that the institution may refuse to disclose in response to a request. These records are described immediately below.

LAW ENFORCEMENT REPORT [SUBSECTION 8(2)9A) AND 8(4)]

Subsection 8(2)(a) exempts from disclosure a report prepared in the course of law enforcement inspections or investigations by an agency responsible for enforcing and regulating compliance with a law. Reports include internal memoranda, complaint processing records and proposed witness statements. Agency includes organizations acting on behalf of or as agents for law enforcement agencies.

Subsection 8(2)(a), however, is modified by subsection 8(4) which does not allow the institution to exempt a routine inspection report. Routine inspections are carried out when there are no specific allegations that standards have been breached. Routine inspections include random inspections as well as those done on a regular basis. While the standards are frequently set out in a by-law or regulation, the statute provides the

authority for enforcement and compliance.

For example:

The *Fire Marshals Act* authorizes the Fire Chief to enforce compliance with fire safety standards through routine inspections. These standards are set out in the *Fire Marshals Act* and the *Ontario Fire Code* (R.R.O. 1990, Reg. 454). These inspections need not take place as a result of a complaint. The records of these routine inspections would not be exempt under subsection 8(2)(a).

ACT OF PARLIAMENT [SUBSECTION 8(2)(B)]

This subsection exempts a law enforcement record where disclosure would be an offence under an Act of Parliament.

For example:

> Section 46 of the *Young Offenders Act* makes it an offence to knowingly disclose certain court, police and government records relating to young offenders, except as authorized by that Act.

CIVIL LIABILITY [SUBSECTION 8(2)(C)]

Subsection 8(2)(c) exempts a law enforcement record where disclosure could reasonably be expected to expose the author of the record, or any person who had been quoted or paraphrased in the record to civil liability.

The purpose of this exemption is to provide protection for law enforcement officials who might be sued for defamation as a result of disclosure of records made while carrying out their duties.

CORRECTIONAL AUTHORITY [SUBSECTION 8(2)(D)]

Subsection 8(2)(d) exempts records that contain information relating to an individual's correctional history while the individual is under the control or supervision of a correctional authority.

REFUSAL TO CONFIRM OR DENY THE EXISTENCE OF A RECORD [SUBSECTION 8(3)]

Subsection 8(3) provides that a head may refuse to confirm or deny the existence of a record to which subsections 8(1) or 8(2) apply. Situations may arise in which merely disclosing the existence of an investigation or intelligence file will communicate information to the requester which may impede ongoing investigation or intelligence-

gathering.

EXCEPTIONS TO EXEMPTION FOR LAW ENFORCEMENT

ROUTINE INSPECTIONS [SUBSECTION 8(4)]

This subsection requires the City to disclose a record that is a report prepared in the course of routine inspections by an agency that is authorized to enforce and regulate compliance with a particular statute of Ontario.

For further discussion on routine inspections, see Law Enforcement Report [subsection 8(2)(a)].

DEGREE OF SUCCESS IN A LAW ENFORCEMENT PROGRAM [SUBSECTION 8(5)]

Subsection 8(5) provides that the exemptions in subsections 8(1) and (2) do not apply to a record regarding the degree of success achieved in a law enforcement program, unless the disclosure of such record would prejudice or interfere with, or adversely affect any of the matters referred to in 8(1) or (2).

The compelling public interest override in section 16 does not apply to this exemption.

RELATIONS WITH GOVERNMENTS [SECTION 9]

Section 9 provides a *mandatory* exemption where disclosure of a record could reasonably be expected to reveal information received in confidence from:

- the Government of Canada
- the Government of Ontario
- the government of another province or territory
- the government of a foreign country of state; or
- an international organization of states (e.g. the United Nations)

Records received in confidence from agencies or boards of these governments would be included in this exemption.

If the government which supplied the confidential information consents to its release, the exemption does not apply. The Act does not require the City to seek this consent, although in every case where this exemption is to be applied, the City should consider

whether it is appropriate to seek consent.

This exemption applies only to records received in confidence from the governments specified in section 9. This exemption does not apply to records received in confidence from another municipality or local board. The Act provides that the request can be transferred to the originating municipality or local board if that institution has the greater interest. See Part 3 for a discussion on this transfer provision.

The compelling public interest override provision in section 16 applies to this exemption.

THIRD PARTY INFORMATION [SECTION 10]

The City often acquires information about the activities of businesses in the private sector. Some of this information may constitute a valuable asset to the company, and disclosure would impair its ability to compete effectively. Subsection 10(1) provides a *mandatory* exemption from disclosure for certain third party information where disclosure could reasonably be expected to cause certain harms. This exemption is not limited to commercial third parties, but may also apply to any supplier of information which meets the tests specified below, including another institution.

Section 21 provides that before access is granted to a record that might contain information referred to in subsection 10(1) affecting the interests of a third party, that party must be notified and given the opportunity to make representations before a final access decision is made. If a third party claims in its representations that the record is exempt, the burden of establishing that the record falls within this section rests with that third party. Similarly, where the City asserts that section 10 applies, the burden of proof is on the City. Notification procedures are discussed in Part 3.

Before this exemption can be applied, *all* of the following three tests must be met:

- the information must fit within one of the specified categories of third party information;
- the information must have been *supplied* by the third party *in confidence,*

  implicitly or explicitly; and
- the disclosure of the information could reasonably be expected to cause certain harms specified in section 10.

The three tests are discussed in more detail immediately below:

TEST #1: CATEGORIES OF THIRD PARTY INFORMATION

Before subsection 10(1) applies, the record in question must contain one or more of the following types of information:

Trade Secret: A trade secret must consist of information and may be used for an industrial trade or business use. The trade secret is not generally known in that industry, trade or business and has economic value from not being generally known. It has also been treated in a manner to ensure its continued confidentiality.

Scientific Information: This term refers to information relating to or exhibiting the principles of science.

For Example:

> Scientific information would be contained in a proposal describing innovative energy technologies in a grant application.

Technical Information: This term refers to information particular to an art or profession, for instance, architectural design or system design specifications.

Commercial Information: This term refers to information concerning the sale, purchase, or exchange of goods, products or property.

For Example:

> Customer and price lists, lists of suppliers, marketing and advertising plans, and similar information related to the commercial operation of a business would be commercial information.

Financial Information: This term refers to information relating to money and its use or distribution.

For Example:

> Cost accounting methods, pricing practices, profit and loss data, overhead and operating costs are all examples of financial information.

Labour relations information: This term refers to information concerning the relationship between employers and their employees, both union and non-union, particularly information relating to collective bargaining.

For Example:

> Records relating to the bargaining positions of an employer and a union engaged in mediation proceedings would be labour relations information.

TEST #2: SUPPLIED IN CONFIDENCE

Subsection 10(1) provides that *the* information must be *supplied* in confidence. Information that is created or is gathered by the institution is not supplied by a third party and would not qualify for this exemption.

For Example:

> A fee paid by the City to a consultant is not supplied by the consultant; it is created by the institution.

The intention to maintain confidentiality may be expressed or may be implied by the circumstances (or the conduct of the parties). Confidentiality may be implied where there is evidence that the information was consistently treated in a confidential manner.

For Example:

> Generally, material provided as a result of a sealed tender meets the confidentiality test where the written policy of the institution stipulates that confidentiality would be maintained.

Information that was available to interested parties and the general public before the Act was in force cannot be supplied in confidence.

TEST #3: HARMS TEST

If the information falls within one of the categories described, and was supplied in confidence, it is then necessary to demonstrate that its disclosure could reasonably be expected to yield one of the results listed in subsections 10(1)(a), (b), (c), or (d).

COMPETITIVE POSITION OR NEGOTIATIONS [SUBSECTION 10(1)(A)]

This subsection applies where the disclosure could reasonably be expected to prejudice significantly the competitive position or interfere with the contractual or other negotiations of a person or organization (whether or not the person or organization is

the third party submitting the information).

The City or third party must present evidence that is detailed and convincing and must describe a set of facts and circumstances that would lead to a reasonable expectation that harm would occur if the information were released. Generalized statements of fact without sufficient evidence do not meet the test.

INFORMATION NO LONGER SUPPLIED [SUBSECTION 10(1)(B)]

This subsection applies where the disclosure could reasonably be expected to result in similar information no longer being supplied to the City where it is in the public interest that similar information continue to be supplied.

This provision would not apply where the information is submitted voluntarily in an application for a benefit or a grant, or where a statute requires the provision of this information.

The test is whether the third party or another source would entrust similar information to the City in the future if the information were disclosed. If not, this subsection applies.

UNDUE LOSS OR GAIN [SUBSECTION 10(1)(C)]

This subsection applies where the disclosure could reasonably be expected to result in undue loss or gain to any person or organization. Undue means more than necessary, excessive or unjustified.

LABOUR RELATIONS INFORMATION [SUBSECTION 10(1)(D)]

This subsection applies where the disclosure could reasonably be expected to reveal information supplied to or the report of a conciliation officer, mediator, labour relations officer or other person appointed to resolve a labour relations dispute.

EXCEPTION TO EXEMPTION FOR THIRD PARTY INFORMATION [SUBSECTION 10(2)]

Subsection 10(2) provides an exception to the exemption in subsection 10(1) where the affected third party consents to disclosure. While the City need not seek the consent of the third party in each case, he or she is required to *consider* whether the consent ought to be sought.

The compelling public interest provision in section 16 applies to this provision.

ECONOMIC AND OTHER INTERESTS [SECTION 11]

Section 11 provides a *discretionary* exemption for certain proprietary information of the City and the premature disclosure of certain plans or negotiating strategies. Information affecting the interests of third parties is covered by section 10.

Subsections 11(a) through (g) set out the types of information and circumstances covered by this exemption.

COMMERCIAL INFORMATION [SUBSECTION 11(A)]

This subsection allows the City to refuse access to trade secrets, or financial, commercial, scientific or technical information belonging to an institution and has monetary value or potential monetary value. These terms have the same meaning as in subsection 10(1), described above. The information may belong to the City or to another institution.

Having monetary value or potential monetary value means that the trade secret or information is or is potentially marketable.

EMPLOYEE RESEARCH [SUBSECTION 11(B)]

This subsection exempts information obtained through research by an employee of the City where the disclosure could reasonably be expected to deprive the employee of priority of publication. The employee must intend to publish the information.

ECONOMIC INTERESTS [SUBSECTION 11(C)]

This subsection exempts information where the disclosure could reasonably be expected to prejudice the economic interests or competitive position of the City.

Economic interests concern the production, distribution and consumption of goods and services. If it can be reasonably expected, for instance, that disclosure of certain information would cause an institution to pay a higher price for goods and services, that information may be exempt under subsection 11(c).

Competitive position applies only to those institutions engaged in the supply of goods and services on a competitive basis.

FINANCIAL INTERESTS [SUBSECTION 11(D)]

This subsection exempts information where the disclosure could reasonably be

expected to be injurious to the City's financial position.

Financial interests refers to the City's financial position, its ability to collect taxes and generate revenues, and its ability to protect its own interests in financial transactions with third parties.

NEGOTIATING STRATEGY [SUBSECTION 11(E)]

The City may refuse to disclose positions, plans, procedures, negotiations carried on by or on behalf of an institution.

Negotiations in this subsection mean discussions and communications where the intent is to arrive at a settlement or agreement. This exemption applies to on-going and future negotiations.

PERSONNEL OR ADMINISTRATION [SUBSECTION 11(F)]

The City may refuse to disclose plans relating to the management of personnel or the administration of an institution. This subsection is intended to cover the internal management plans of the City, such as a reorganization or relocation prior to implementation. See subsection 7(2)(h) which concerns proposals to change or establish a public program.

Once the plan has been put into operation or made public, subsection 11(f) does not apply.

POLICY DECISIONS/UNFAIR ADVANTAGE [SUBSECTION 11(G)]

This subsection exempts information such as proposed plans, policies or projects where the disclosure could reasonably be expected to result in:

- premature release of a pending policy decision; or
- undue financial benefit or loss to a person

There must be evidence to support the assertion that one of the two specified results would occur.

EXAMINATION OR TEST QUESTIONS [SUBSECTION 11(H)]

The City may refuse to disclose questions that are to be used in an examination or test for an educational purpose. Once the question is no longer to be used in an exam or

test, the exemption does not apply.

Questions for a job competition are not included in this exemption.

SUBMISSIONS UNDER THE MUNICIPAL BOUNDARY NEGOTIATIONS ACT [SUBSECTION 11(I)]

This subsection exempts records containing submissions made under the *Municipal Boundary Negotiations Act,* by a party municipality or other body. This exemption may only be invoked before the matter is resolved under the Act.

The compelling public interest provision in section 16 applies to this exemption.

SOLICITOR-CLIENT PRIVILEGE [SECTION 12]

Section 12 is a *discretionary* exemption relating to records which are subject to the solicitor-client privilege. All communications of a confidential nature between the City and its legal advisor directly related to legal advice are covered. This includes working papers and statements of the legal advisor's account with the client. For solicitor-client privilege to apply, four criteria must be met:

- there must be a written or oral communication;
- the communication must be of a confidential nature;
- the communication must be between the City and a legal advisor; and
- the communication must be directly related to seeking, formulating or giving legal advice.

Papers and materials created or obtained especially for the lawyer's brief for existing or contemplated litigation are privileged, whether or not the information has been communicated to or from the client.

Also included are records prepared by or for counsel employed or retained by an institution for use in giving legal advice or in contemplation of or for use in litigation.

While only the client may waive the privilege, all circumstances regarding the disclosure of a legal opinion must be considered to determine whether there has been a waiver.

For example:

> If a client disclosed an opinion to a specific party, intentionally and without any restrictions on its use, the release could constitute a waiver of the solicitor-client

privilege.

The City must take care to ensure that legal opinions are not released to a specific party as the solicitor-client privilege may be jeopardized. If the City wishes to release privileged information to a specific party, it should place restrictions on its use to retain the solicitor-client privilege.

Section 12 contains two branches:

Branch 1: common law privileges

This branch applies to a record that is subject to "solicitor-client privilege" at common law. The term "solicitor-client" encompasses two types of privilege:

- solicitor-client communication privilege
- litigation privilege

Common law solicitor-client communication privilege protects direct communications of a confidential nature between a solicitor and client, or their agents or employees, made for the purpose of obtaining or giving professional legal advice. The rationale for this privilege is to ensure that a client may confide in his or her lawyer on a legal matter without reservation [Order P-1551].

Branch 2: statutory privileges

Branch 2 is a statutory solicitor-client privilege that is available in the context of Crown counsel giving legal advice or conducting litigation. Similar to Branch 1, this branch encompasses the same two types of privilege as derived from the common law.

The statutory and common law privileges, although not necessarily identical, exist for similar reasons. One must consider the purpose of the common law privilege when considering whether the statutory privilege applies.

The compelling public interest provision in section 16 does not apply to this exemption.

DANGER TO SAFETY OR HEALTH [SECTION 13]

Section 13 provides a *discretionary* exemption relating to records, the disclosure of which could reasonably be expected to seriously threaten the safety or health of any individual.

This exemption is not intended to restrict an individual's right of access to his or her own

personal information, except where disclosure could threaten the safety or health of another individual.

The compelling public interest provision in section 16 applies to this exemption.

PERSONAL PRIVACY [SECTION 14]

Subsection 14(1) provides a *mandatory* exemption relating to the disclosure of personal information to an individual other than the individual to whom the information relates.

Section 14 is one of the keystone provisions of the Act. It balances the public's right of access to records and the individual's right of privacy respecting personal information.

Subsection 14(1) requires the City to refuse to disclose personal information, unless one of the circumstances listed in 14(1)(a) through (f) apply.

Subsections 14(2)(a) through (i) lists circumstances which should be considered in determining whether a disclosure of personal information constitutes an unjustified invasion of personal privacy.

Subsection 14(3) sets out circumstances where disclosure is presumed to be an unjustified invasion of personal privacy.

Subsection 14(4) lists when disclosure does not constitute an unjustified invasion of personal privacy.

Subsection 14(5) permits the City to refuse to confirm or deny the existence of a record if its disclosure would constitute an unjustified invasion of privacy.

Where the City has reason to believe that a disclosure might constitute an unjustified invasion of personal privacy, section 21 provides that the City must give notice to the person to whom the personal information relates before granting access to a record. This person must be given the opportunity to make representations about the disclosure. See **Notices to Affected Third Parties** in Part 3.

EXCEPTIONS TO EXEMPTION FOR PERSONAL PRIVACY

Subsection 14(1)(a) through (f) outlines circumstances when personal information may be disclosed to someone other than the individual to whom the information relates.

CONSENT [SUBSECTION 14(1)(A)]

Personal information can be disclosed to someone other than the individual to whom the information relates with the prior request or consent of the individual. The record

must be one to which the individual is entitled to have access.

The request or consent should be in writing and be received before the personal information is disclosed.

COMPELLING CIRCUMSTANCES [SUBSECTION 14(1)(B)]

Personal information may be disclosed to a person other than the individual to whom the personal information relates in compelling circumstances affecting the health or safety of an individual.

Circumstances are *compelling* when either there is no other way to obtain personal information affecting health or safety, or there is an emergency situation where the delay in obtaining the information would be injurious to someone's health or safety. The determination of when compelling circumstances exist is left to the discretion of the head.

Where personal information is released under this subsection, upon disclosure, notification must be mailed to the last known address of the individual to whom the information relates. If the institution does not have the address, it must attempt to find out the address of the individual from the person who made the request.

PUBLIC RECORDS [SUBSECTION 14(1)(C)]

Personal information may be disclosed to another person in response to a request made under the Act if the personal information is collected and maintained specifically for the purpose of creating a record available to the general public.

A public record refers to a collection of personal information to which all members of the public have equal access.

DISCLOSURE EXPRESSLY AUTHORIZED BY STATUTE [SUBSECTION 14(1)(D)]

Personal information may be disclosed to a person other than the individual to whom the personal information relates where an Act of Ontario or Canada expressly authorizes disclosure.

For example:

> Personal information may be released to an individual other than the individual to whom the personal information relates pursuant to the Employment Insurance Act which contains a subsection that expressly authorizes disclosure of personal

information to the Employment Insurance Commission.

RESEARCH AGREEMENTS [SUBSECTION 14(1)(E)]

The City may disclose personal information in response to a request under the Act, if the disclosure is for a research purpose, when certain conditions are met. *Research purposes* are distinct from administrative, operational or regulatory uses of personal information in that research uses do not directly affect the individual to whom the information relates and do not relate to the usual administration of a program.

This provision covers disclosures to researchers receiving grants, consultants conducting contractual research and independent researchers. Access to personal information by researchers who are employees of the City is covered by Section 31 and subsection 32(d) and not subsection 14(1)(e).

The City must determine that conditions are appropriate for the disclosure of personal information for a research purpose. The following conditions must be met:

- the disclosure must be consistent with the conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained. If the information was provided with a reasonable expectation of confidentiality, access should not be granted without the consent of the individual;
- the research purpose for which disclosure is to be made cannot be reasonably achieved unless the information is provided in a form which allows individuals to be identified;
- the research must comply with conditions relating to security and confidentiality prescribed by the regulations. See Regulation 823 for a list of these conditions; and,
- the disclosure is not an unjustified invasion of privacy [subsection 14(1)(f)].

UNJUSTIFIED INVASION OF PERSONAL PRIVACY [SUBSECTION 14(1)(F)]

Access to another individual's personal information may be granted where the disclosure does not constitute an unjustified invasion of personal privacy. This is determined by balancing the factors set out in subsections 14(2) and 14(3).

FACTORS TO BE CONSIDERED

In determining whether disclosure of personal information to someone other than the

person to whom it relates constitutes an unjustified invasion of privacy, the City must consider all the relevant circumstances.

The circumstances listed in subsections 14(2)(a) through (i) should be considered in deciding whether or not to disclose personal information. Some may rebut the presumption in subsection 14(3) that release of the personal information would invade an individual's privacy; that is, the record could be disclosed. However, some of the enumerated circumstances in subsection 14(2) reinforce the presumptions in subsection 14(3) and favour a denial of access.

The list in subsection 14(2) is not exhaustive; any other relevant circumstances should be considered by the institution before a decision on disclosure is made.

PUBLIC SCRUTINY [SUBSECTION 14(2)(A)]

In determining whether disclosure constitutes an unjustified invasion of personal privacy, the City must consider whether disclosure is desirable for subjecting the activities of the institution to public scrutiny.

The City should consider the broader interests of public accountability. Invoking this provision should not be limited to instances where it is alleged that the City's normal practices or procedures were not followed.

PUBLIC HEALTH AND SAFETY [SUBSECTION 14(2)(B)]

One of the relevant circumstances the institution must consider in determining whether disclosure constitutes an unjustified invasion of personal privacy is if access to the personal information may promote public health and safety.

INFORMED CHOICE [SUBSECTION 14(2)(C)]

In determining whether disclosure constitutes an unjustified invasion of personal privacy, the City must consider whether disclosure will promote informed choice in the purchase of goods and services.

For example:

> Disclosure of an evaluation of a supplier's or consultant's performance could disclose personal information.

FAIR DETERMINATION OF RIGHTS [SUBSECTION 14(2)(D)]

In determining whether disclosure constitutes an unjustified invasion of personal

privacy, the City must consider whether the personal information is relevant to a fair determination of the requester's rights. There may be instances where the requester requires access to personal information about someone else in order to assist the requester in obtaining a determination of his or her rights.

Example:

> Records in respect of an investigation of alleged sexual harassment may be released to the person against whom the allegation is made, in the absence of other factors. One factor leading to non-disclosure might be evidence of potential harm to witnesses if their identities were disclosed.

UNFAIR EXPOSURE TO HARM [SUBSECTION 14(2)(D)]

The City must consider whether the individual will be exposed unfairly to pecuniary or other harm.

This consideration is relevant only where there is evidence that unfair pecuniary or other harm will result from the disclosure.

HIGHLY SENSITIVE INFORMATION [SUBSECTION 14(2)(F)]

One of the relevant circumstances the institution must consider in determining whether disclosure constitutes and unjustified invasion of personal privacy is if the information is highly sensitive.

INFORMATION INACCURATE OR UNRELIABLE [SUBSECTION 14(2)(G)]

The City must consider whether the personal information is unlikely to be accurate or reliable.

Subsection 30(2) requires the City to take reasonable steps to ensure that personal information is not used unless it is accurate and up to date.

INFORMATION SUPPLIED IN CONFIDENCE [SUBSECTION 14(2)(H)]

In determining whether disclosure constitutes an unjustified invasion of personal privacy, the City must consider whether the personal information was supplied by the individual to whom it relates in confidence.

This subsection does not apply to information supplied in confidence by one individual to another.

PRESUMED INVASION OF PRIVACY

Subsection 14(3) provides that disclosure of certain types of personal information is presumed to be an unjustified invasion of personal privacy. These factors must be considered in conjunction with those listed in subsection 14(2) above to determine if the disclosure of personal information may be considered an unjustified invasion of privacy.

MEDICAL RECORD [SUBSECTION 14(3)(A)]

Disclosure of information that relates to a medical psychiatric or psychological history, diagnosis, treatment or evaluation is presumed to constitute an unjustified invasion of personal privacy.

VIOLATION OF LAW [SUBSECTION 14(3)(B)]

Disclosure of personal information compiled as part of an investigation into a possible violation of law is presumed to constitute an unjustified invasion of personal privacy.

For example:

> Personal information relating to sexual harassment investigations compiled by, or on behalf of, the Ontario Human Rights Commission are records compiled as part of an investigation into a possible violation of law. However, where internal investigations are conducted by an institution's human resources staff, this provision does not apply. The fact that a complainant *might* take their concerns to the Ontario Human Rights Commission does not alter the fact that this type of internal investigation does not have a possible violation of law.

This exemption does not apply where disclosure is necessary to prosecute the violation or to continue the investigation.

ELIGIBILITY FOR SOCIAL PROGRAMS [SUBSECTION 14(3)(C)]

Disclosure of information that relates to eligibility for social service or welfare benefits is presumed to constitute an unjustified invasion of personal privacy.

EMPLOYMENT OR EDUCATIONAL HISTORY [SUBSECTION 14(3)(D)]

Disclosure of information that relates to an individual's employment or educational history is presumed to constitute an unjustified invasion of personal privacy. This presumption does not apply to employment-related duties or to employees expense claims.

FINANCIAL HISTORY [SUBSECTION 14(3)(F)]

Disclosure of personal information describing an individual's finances, income, assets, liabilities, net worth, bank balances, financial history or creditworthiness is presumed to constitute an unjustified invasion of personal privacy.

Specific salaries of individuals are personal information that must be protected, however, disclosure of a salary range is not considered an unjustified invasion of personal privacy.

PERSONAL RECOMMENDATIONS AND EVALUATIONS [SUBSECTION 14(3)(G)]

Disclosure of personal information consisting of personal recommendations or evaluations, character references, personnel evaluations is presumed to constitute an unjustified invasion of personal privacy.

RACE, ETHNIC ORIGIN, RELIGION OR SEXUAL ORIENTATION [SUBSECTION 14(3)(H)]

Disclosure of personal information which reveals an individual's racial or ethnic origin, religious or political beliefs or sexual orientation is presumed to constitute an unjustified invasion of personal privacy.

EXCEPTIONS TO THE EXEMPTION

Despite the other provisions of section 14, subsection 14(4) lists two types of personal information where disclosure does not constitute an unjustified invasion of privacy.

SALARY RANGE AND BENEFITS OF EMPLOYEES [SUBSECTION 14(4)(A)]

Disclosure of the classification, salary range and benefits, or employment responsibilities of an officer or employee of an institution is not an unjustified invasion of personal privacy. Note that the provision refers to *salary range*, not specific salary.

Officer or employee includes appointed officials and those persons who work for the City, or who perform their duties under a contract of employment.

PERSONAL SERVICE CONTRACTS [SUBSECTION 14(4)(B)]

Disclosure of the financial or other details of a contract for personal services between an individual and an institution is not an unjustified invasion of privacy. A contract in which an individual, not a company, is hired to perform professional services in respect of a particular problem or project would be included.

REFUSAL TO CONFIRM OR DENY

Where the head refused to give access to a record on the grounds of an unjustified invasion of privacy, the head may also refuse to confirm or deny the existence of the record. Where the head refused to confirm or deny the existence of a record in response to a request, notification to the requester under subsection 22(2) is required.

COMPELLING PUBLIC INTEREST

Members of the public often wish to know some information about elected officials and appointees to public positions on boards and committees. It is suggested that the City prepare brief biographies, making them available to the public upon request, however, the elected official or appointees should be made aware of this practice prior to such biographies being published.

The compelling public interest provision in section 16 applies to this exemption.

PUBLISHED INFORMATION [SECTION 15]

Section 15 is a *discretionary* exemption that allows the City to refuse disclosure of a record where:

- the record or the information contained in the record has been published or is currently available to the public; or
- there are reasonable grounds to believe that the record or information will be published by the City within 90 days of the request, or within a further period of time need for printing the material or for translating it before printing.

This exemption is not limited to information published only by the City. The City has a duty to inform a requester where the record or information in question is available.

Where the City invokes this exemption, it must consider the convenience of the requester compared to the convenience of the City.

Where the City is faced with an important issue, generating numerous requests over a long period of time, and the City will grant access to these records, it may be advantageous for the City to put together a package of information and have it published. A reasonable fee can be set for the package.

The compelling public interest exemption in section 16 does not apply to this exemption.

LIMITATIONS ON ACCESS TO ONE'S OWN PERSONAL INFORMATION [SECTION 38]

While all of the exemptions discussed above are in Part I of the Act (Access to Information), section 38 falls in part II (Protection of Individual Privacy).

In Part II, section 36 establishes a right of access to one's own personal information. Section 38 is a *discretionary* exemption to that right of access and sets out grounds for refusing to disclose personal information to the individual to whom the information relates.

GENERAL EXEMPTIONS [SUBSECTION 38(A)]

This subsection provides that an individual's right of access to his or her own personal information is subject to the exemptions applying to general information. This includes the exemptions in sections 6 through 14, and section 15 but not section 14 which applies to the disclosure of an individual's personal information to a third party.

UNJUSTIFIED INVASION OF ANOTHER'S PERSONAL PRIVACY [SUBSECTION 38(B)]

The City may refuse to disclose to an individual his or her own personal information where the disclosure would constitute an unjustified invasion of another individual's personal privacy. Subsections 14(2) and (3) provide the test for determining an unjustified invasion of personal privacy and guidance in interpreting this subsection.

There may be personal information about more than one individual in the same record. Severing may not be feasible because close family or business ties would allow individuals other than the requester to be identified despite severing. Therefore, if disclosure would invade the personal privacy of an individual other than the requester, disclosure may be refused.

There is a requirement for notification to the individual whose personal privacy may be invaded where release is contemplated. See **Notices to Affected Third Parties** in Part 3.

REVEALING A CONFIDENTIAL SOURCE [SUBSECTION 38(C)]

The City may refuse to disclose to an individual his or her own personal information when it is evaluative or opinion material where disclosure would reveal the identity of a source who furnished information to the City. The information must have been provided in circumstances where it may reasonably have been assumed that the identity of the source would be held in confidence. The evaluative or opinion material must be compiled solely for the purpose of determining suitability, eligibility or qualifications for

employment or for the awarding of contracts and other benefits.

The information to which the exemption applies is only that information which would reveal the identity of the source. The phrase *information furnished to the institution* indicates that the source is someone outside the City.

MEDICAL INFORMATION [SUBSECTION 38(D)]

The City may refuse to disclose to an individual his or her own personal information where the disclosure could reasonably be expected to prejudice the individual's mental or physical health. This provision is intended where disclosure would be injurious to the individual. It is not intended as a general provision for withholding access to medical information. Wherever possible, an individual should be granted access to his or her medical information.

The City may wish to consult with a medical practitioner to determine whether there is a reasonable expectation of prejudice to the individual's mental or physical health. When the information is disclosed to the requester, the medical practitioner or other appropriate professional may be present to provide explanations and to answer questions.

RESEARCH OR STATISTICAL RECORD [SUBSECTION 38(D)]

The City may refuse to disclose to an individual his or her own personal information if the personal information is collected for a research or statistical purpose not directly affecting the individual. If the information is used for any other purpose, this exemption does not apply.

EXEMPTIONS

SECTION		MANDATORY	COMPELLING PUBLIC INTEREST PROVISION
s.6	Draft by-laws, records of closed meetings	Discretionary	No
s.7	Advice or Recommendations	Discretionary	Yes
s.8	Law Enforcement	Discretionary	No
s.9	Relations with governments	Mandatory	Yes
s.10	Third party information	Mandatory	Yes
s.11	Economic & other interests	Discretionary	Yes
s.12	Solicitor-client privilege	Discretionary	No
s.13	Danger to safety or health	Discretionary	Yes
s.14	Personal Information	Mandatory	Yes
s.15	Published Information	Discretionary	No
s.38	Limitations on access to own personal information	Discretionary	No

Guide to Decision Under Section 14

Request for another Individual's Personal Information

s.14(1)
Does an exception apply, i.e., s.14(1)(a) – (e) or s. 14(4)?

If so, release record
If not, consider s.14(3)

s.14(3)
Presumed unjustified invasion of privacy if record released?

"YES"	**"NO"**
If presumed invasion of privacy under s. 14(3), are there any grounds in s. 14(2) which rebut or modify this presumption? If yes, commence third party notice process. If no, record not disclosed.	If not presumed invasion of privacy under s.14(3), are there any grounds (inc. s.14(2) to indicate disclosure would be unjustified invasion? If yes, record not disclosed. If no, commence third party notice proceedings.

PART 5: PRIVACY PROTECTION

INTRODUCTION

One of the key principles of the *Municipal Freedom of Information and Protection of Privacy Act* is the protection of personal privacy. The requirements of the Act concerning personal privacy are set out in Part II and include:

- establishing standards for the collection, use and disclosure of personal information by institutions;
- requiring that personal information records are retained and disposed of in such a way that the confidentiality of the records is maintained at all times.

The requirements of Part II restrict the collection, use and disclosure of personal information to the circumstances outlined in this Part.

PUBLIC RECORDS [SECTION 27]

Section 27 states that the provisions of Part II of the Act (sections 28 to 38) do not apply to personal information maintained for the purpose of creating a record that is available to the general public.

Public records of personal information are usually established under a statute, and are records to which all members of the public have equal access. Personal information to which some members of the public have access, while others do not, is not a public record for the purposes of the *Municipal Freedom of Information and Protection of Privacy Act.*

For Example:

A public record is a list of electors required by Section 28 of the *Municipal Elections Act.*

NOTE: The list of electors is only available as a public record for a limited period of time during the Municipal Election.

Assessment rolls, as required by Section 39 of the *Assessment Act,* are public records.

COLLECTION OF PERSONAL INFORMATION [SECTIONS 28 AND 29]

This section expands the definition of personal information for the purpose of collection and sets out the authority for the collection of personal information.

EXPANDED DEFINITIONS OF PERSONAL INFORMATION [SUBSECTION 28(1)]

For the purposes of section 28 and 29, the definition of personal information found in section 2 of the Act is expanded to include non-record personal information.

Example:

> Personal information may be collected orally in a job interview. Although such information may not be recorded, the same rules regarding the collection of personal information apply.

When personal information is collected orally, it is very often a good business practice to make some written record that the information was received. There is no requirement in the Act, however, that such record be created.

AUTHORITY TO COLLECT [SECTION 29]

This subsection sets out the conditions under which personal information may be collected. Personal information is collected by the City when the the City actively acquires the information or invites an individual or others to send personal information to the City. An in individual may submit personal information on his or her own initiative without the information being requested by the City. Receipt of this information is not considered a collection unless the City keeps or uses the information.

Example:

> Unsolicited resumes which are sent to the City and are not in response to a job advertisement or competition are not collected. Resumes submitted in response to a job call are collected by the City and authorization for collection is subject to subsection 29(1).

One of three conditions must exist in order for personal information to be collected:

- the collection of personal information is expressly authorized by statute;
- the information collected is used for the purposes of law enforcement;
- the collection is necessary for the proper administration of a lawfully authorized activity.

For Example:

Personal information collected to develop a list of electors under section 21 of the *Municipal Elections Act* is a collection authorized specifically by a statute.

Information collected by social services investigators in the course of an investigation into social assistance fraud, is a collection for the purpose of law enforcement.

An activity is lawfully authorized when it is established by statute, regulation or by-law. A collection of personal information on an application for a municipal business license is necessary to the property administration of the licensing of businesses.

By implication, the authority to collect personal information is limited to the collection of necessary information.

MANNER OF COLLECTION [SUBSECTION 29(1)]

This subsection requires that personal information be collected directly from the individual to whom it relates, unless certain circumstances described in subsection 29(1)(a) through (h) permit an indirect collection.

INDIVIDUAL AUTHORIZATION [SUBSECTION 29(1)(A)]

An individual may authorize an indirect collection of personal information. Such authorization should generally include:

- the identification of the personal information to be collected;
- the source from which the personal information may be collected; and
- the name of the institution that is to collect the personal information.

A record should be kept with the date and the details of the authorization.

Notice of the collection should be given to the individual concerned at the same time as the authorization is obtained. Notice of collection of personal information is discussed later in this Part.

DISCLOSURE UNDER SECTION 32 [SECTION 29(1)(B)]

Personal information may be collected by the City from another institution where the disclosing institution has authority to disclose under Section 32 of the *Municipal Freedom of Information and Protection of Privacy Act*.

For Example:

> Under section 4(2) of the *General Welfare Assistance Act*, a municipality may collect personal information for the purpose of determining eligibility for social assistance benefits.

When a social assistance recipient moves to another municipality, the municipality originally providing benefits may disclose certain personal information about the recipient to the second municipality, so that the client's eligibility for social assistance may be determined.

The disclosure is *authorized* by subsection 32(c) of the MFIPPA as the disclosure to the second municipality is for the same or similar purpose for which the information was originally collected, namely, determining eligibility for social assistance benefits. The second municipality, therefore, may collect the information since it has been properly disclosed to it under subsection 32(c) of the Act.

AUTHORITY OF THE COMMISSIONER [SUBSECTION 29(1)(C)]

The Commissioner may authorize a collection from a source other than the individual. The Commissioner's authorization may be sought because the indirect collection is not specifically allowed under subsection 29(1), or where the City believes it is not possible or practical to collect the personal information directly or to obtain authorization directly from the individual concerned under subsection 29(1)(a). Subsection 46(c) provides this power to the Commissioner.

CONSUMER REPORTING ACT [SUBSECTION 29(1)(D)]

This subsection authorizes the City to collect personal information from a consumer report that is prepared in accordance with the *Consumer Reporting Act*. A complete list of information which may be included in such a report is contained in subsection 8(1)(d) of the *Consumer Reporting Act.*

HONOUR OR AWARD [SUBSECTION 29(1)(E)]

This subsection authorizes the City to collect personal information indirectly for the purpose of determining suitability for an honour or award to recognize outstanding achievement or distinguished service.

For Example:

> Personal information can be collected to determine which of a number of candidates should receive a Citizen of the Year award.

COURTS AND TRIBUNALS [SUBSECTION 29(1)(F)]

This subsection authorizes the City to collect personal information indirectly for the conduct of a proceeding or a possible proceeding before a court or judicial or quasi-judicial tribunal.

A judicial or quasi-judicial tribunal is a body constituted under a statute with power to decide the legal rights of a person or the eligibility of a person for a benefit or licence. Such tribunals are required to adhere to standards of procedural fairness similar to the procedures of courts.

Some examples of this type of tribunal include the Ontario Municipal Board, Appeal Tribunal, Assessment Review Court, Courts of Revision and Committees of Adjustment.

In some cases, after personal information has been collected, no proceeding takes place because, for example, there is insufficient evidence. Even though the tribunal may never hear the matter, this subsection applies as long as the purpose of the collection is to determine whether a proceeding can be commenced before a court or tribunal.

LAW ENFORCEMENT [SUBSECTION 29(1)(G)]

Personal information which is collected for the purpose of law enforcement may be collected from a source other than the individual about whom the information relates. Law enforcement is defined in section 2(1) of the Act.

STATUTORY AUTHORITY [SUBSECTION 29(1)(H)]

A statute, regulation or by-law may authorize a collection of personal information from a source other than the individual.

For example:

> Under section 6(4) of the *Municipal Health Services Act,* a municipal assessment commissioner may require any employer to furnish a list of employees residing in the municipality, and the dates upon which the employees are paid their salary or wages.

A licensing by-law for lodging houses authorizes a municipality to conduct reference checks as part of its approval of an application for a lodging licence.

NOTIFICATION REQUIREMENTS [SUBSECTION 29 (2)]

When personal information is collected by the City, either directly from the person about whom the information relates or indirectly from another source, the City must inform the individual that the collection has occurred. The notice to the individual must state:

- the legal authority for the collection;
- the principal purpose(s) for which the personal information will be used;
- the title, business address and telephone number of an official of the City who can answer the individual's questions about the collection.

The notice of legal authority should include a reference to the specific act and section, or by-law which authorizes the collection. Where an act or by-law does not specifically refer to the collection, then the notice should refer to the specific section of the act or by-law which establishes the activity or program under which the information is collection.

For example:

> Subsection 58(2) of the *Education Act* provides for the establishment of Boards of Education. Even though the *Education Act* may not specifically authorize each collection of personal information undertaken by a Board of Education, nonetheless subsection 58(2) of the act would provide sufficient statutory authority to undertake collections of personal information that are *necessary to the functioning of a board.*

The statement regarding the principal purpose(s) for which the information will be used should be consistent with the allowable uses of personal information in section 31 of the Act. The principal purpose(s) for which the information will be used should also be consistent with the statement in the index of personal information banks which describes the use and disclosure of personal information in each bank (see section 34 of the Act and Part 2 of this Manual).

Where the personal information is collected directly from the individual, notice should be given to the individual at the time of the collection. Where the personal information is collected on a form, the notice should be provided on the form itself.

A notification should be included on a form where the principal purpose of the form is to collect personal information and the information is used for the purpose of making a decision affecting the individual.

A notification on an application for employment form might read as follows:

> Personal information contained on this form is collected under the authority of the *Municipal Act*, SO 2001, and will be used to determine eligibility for employment. Questions about this collection should be directed to the Manager of Human Resources (or other official), address and telephone number and/or e-mail address.

Forms which are prescribed by a provincial regulation are not controlled by a municipality or local board. In cases where personal information is collected on a prescribed form, it is the responsibility of the provincial ministry controlling the form to include a notice on the form.

Alternative ways of providing notice of collection could include:

- providing notice through public advertisement in the press (eg. Where a public advertisement solicits the collection);
- orally informing the individual in the course of an in-person or telephone interview (and noting this in the individual's file);or
- including the notice in correspondence or as an insert with other mailed material.

Where personal information is collected and will be used or disclosed to another institution, the individual should be given notice of:

- the legal authority that the first institution has for collecting the information;
- the principal purposes for which the personal information will be used by that institution;
- the address and telephone number of an official in that institution who can answer questions; and
- the fact that the information will be used by a second institution and the name of that institution.

If the individual is not informed at the time of collection that the information will be used by another institution, then the second institution must provide notice to the individual.

Where indirect collection is permitted under subsection 29(1), notice to the individual is still required.

Subsection 29(3) provides that notice of collection of personal information is not required if:

- the type of information being collected would be exempt from access under subsection 8(1) or 8(2) (law enforcement);
- the Minister (Chairman of the Management Board of Cabinet) waives the notice. Each request for a waiver is considered on its own merits. Waivers will normally be requested for a class or group of individuals rather than one individual; or
- the regulations provide that the notice is not required.

The regulations provide that notification is not required where:

- Notice Frustrates Purpose of the Collection:

  In some cases, providing notice to the individual when personal information is collected may undermine the purpose for which the personal information is collected. The City might collect personal information to determine the whereabouts of someone who is indebted to the City and who has absconded to avoid paying the debt. In such circumstances, providing notice would frustrate the purpose of collecting the personal information, since notifying the debtor could result in the debtor taking further steps to avoid payment.

- Unjustified Invasion of Another Individual's Personal Privacy:

  Under the Act a notice of collection of personal information must describe how the information will be used. When the use touches upon sensitive personal matters involving another person, the notice may reveal personal information about another individual. An individual who applies for social assistance benefits from a municipality may be required to furnish the names and routine biographical details of the applicant's dependents or co-habitors. Providing notice to the dependents or co-habitor that personal information about them has been collected for the purpose of assessing the applicant's application would reveal sensitive personal information, namely that the individual has applied for assistance.

- Suitability or Eligibility for Award or Honour:

The City may collect the names and biographical details of persons to be considered for an award or honour. Where personal information about a candidate is collected for this purpose, a notice of collection of personal information is not required.

The head must make available to the public, a statement describing the purpose of the collection of personal information and the reason that the notice has not been given.

The statement should:

- Identify the program or activity for which the personal information is collected;
- Describe in general terms the type of personal information collected, and how the information will be used;
- State the time period during which the notice would not be given, for example, whether the notice is being dispensed with for a one-time only collection or for collections occurring regularly over an indefinite time period;
- Explain under which of the circumstances provided for by the regulations the notice has been dispensed with; and
- Advise that any concerns regarding the dispensing of notice may be brought to the attention of the Information and Privacy Commissioner.

The public statement should not disclose any personal information about an identifiable individual.

RETENTION OF RECORDS

The Act includes the power to make regulations relating to the retention period for personal information.

The regulations prescribe a minimum one year retention period for personal information following the last date of use of the information. The purpose of the minimum retention period is to ensure that the individual to whom the information relates has a reasonable opportunity to obtain access to the personal information [subsection 30(1)].

The one year minimum retention period can be shortened in two circumstances. First, where the individual to whom the information relates consents to an earlier disposal (the records need not be kept for one year). Individuals, however, cannot compel the

destruction of records. Second, where the City by by-law or resolution stipulates a shorter retention period for the personal information, then the shorter period becomes the minimum retention period.

This is a minimum retention period, and other operational and legal considerations may be required a longer retention period.

ACCURACY OF RECORDS

Subsection 30(2) requires the head to take reasonable steps to ensure that personal information is not used unless it is accurate and up to date.

Reasonable steps include checking for accuracy, including errors and omissions, at the time the personal information is collected. Any verification of information should be documented.

Although personal information may be accurate and up to date when collected, it may become outdated and, therefore, inaccurate. Before personal information is used, the following questions may be useful in assessing its accuracy:

- When was the information collected;
- Was the information collected directly from the individual to whom it relate?
- Was the accuracy of the information verified at the time it was collected? (eg. Was a birth certificate, passport, driver's licence, viewed to verify age?);
- Is the proposed use of the information consistent with the purpose for which it was collected? Information collected for one purpose may be misleading when used for a different purpose.
- How relevant is the personal information to the current use? (eg, if the information is used to determine eligibility for benefits based on age, the date of birth may be the most relevant piece of information.)
- What is the likelihood that the information is outdated?

EXCEPTION TO ACCURACY REQUIREMENT [SUBSECTION 30(3)]

Subsection 30(2) does not apply to information collected for law enforcement purposes.

USE OF PERSONAL INFORMATION [SECTION 31]

This section establishes general rules governing the use of personal information in the custody and control of the City. It recognizes that the individual's right to privacy includes the right to know how his or her personal information is being used. Personal information may be used within the institution where any one of the following circumstances exists.

INDIVIDUAL CONSENT [SUBSECTION 31(A)]

The City may use personal information where the individual to whom the information relates has consented to the use proposed by the institution.

This consent should be in writing and indicate:

- The particular personal information to be used;
- The use for which consent is given
- The date of the consent; and
- The institution to which consent is given.

Consent of the individual is required where none of the other circumstances described below exists.

PURPOSE FOR WHICH INFORMATION COLLECTED [SUBSECTION 31(B)]

The City may use personal information for the purpose for which the information was originally collected, or for a consistent purpose.

When collecting personal information, the City must notify the subject individual of the principal purpose(s) for which the personal information is to be used. In addition, the City is required to prepare descriptions of its personal information banks. These descriptions will list the principal uses of the personal Information. The City, therefore, may use personal information under its custody or control for the purposes indicated in the collection notice and in the personal information bank descriptions.

The City may also use personal information for a purpose which is consistent with the purpose(s) listed in the collection notice. For an explanation of a consistent purpose, see the discussion of section 33 later in this Part.

FOR THE PURPOSE DISCLOSED [SUBSECTION 31(C)]

An City may be in receipt of personal information disclosed to it by another institution under section 32 of this Act. The receiving institution may use this personal information only for the purpose for which it was disclosed by the first institution.

For example:

> If personal information is disclosed to the City from another institution in compassionate circumstances to assist in locating a family member [subsection 32(i)], that information is to be used by the receiving institution only to locate the family member and for no other purpose.

DISCLOSURE OF PERSONAL INFORMATION [SECTION 32]

Section 32 sets out the rules for disclosure of personal information other than to the individual to whom the information relates. The City shall not disclose personal information except in the specific circumstances enumerated in subsections 32(a) through 32(l).

Disclosure of personal information under section 32 is not dependent upon a request under the Act. Section 32 governs the disclosure of personal information in the day to day activities of the institution. Section 14, on the other hand, provides an exemption protecting personal privacy where a request for access has been made.

DISCLOSURE IN ACCORDANCE WITH PART I [SUBSECTION 32(A)]

Subsection 32(a) permits the City to disclose personal information in circumstances where such a disclosure would have been permitted under Part 1 of the Act even though the City had not received an access request. This subsection should be read in conjunction with subsection 50(1) which permits a head to disclose information even though an access request has not been received.

For example:

> Obligation to disclose (section 5) or compelling public interest (section 16) are instances where the head may disclose information in the absence of a request.

CONSENT TO DISCLOSURE [SUBSECTION 32(B)]

The City may disclose personal information where the individual has consented to the disclosure. Where this consent is not obtained in writing it should be documented and should indicate:

- The particular personal information to be disclosed;
- To whom the information may be disclosed and for what purpose it is to be used;
- The date of the consent and the institution to which the consent is given.

CONSISTENT PURPOSE [SUBSECTION 32(C)]

The City may disclose personal information for the purpose(s) for which it was originally collected, or for a consistent purpose. A purpose is a consistent purpose only if the individual from whom the information was directly collected might reasonably have expected such a use of the information.

For example:

> A public utility commission may disclose personal information to a debt collection agency to recover monies owed to the commission for utility bills in arrears. Such disclosures would reasonably be expected by persons who have not discharged their debts to the commission.

The City may also disclose personal information for a purpose which is consistent with the purpose(s) listed in the collection notice.

IN PERFORMANCE OF DUTIES [SUBSECTION 32(D)]

Personal information may be disclosed to an employee or officer of the City who needs the record in the performance of his or her duties, and where disclosure is necessary and proper in the discharge of the institution's functions. Municipal councilors are not necessarily considered officers of the corporation, however the Mayor is considered to be an officer.

Before an officer or employee of the City is granted access to personal information under this provision, both of the following conditions must be satisfied:

- The employee or officer must need the record of personal information in the performance of his or her duties;
- Disclosure of the personal information must be necessary and proper in discharging the institution's functions.

Disclosures that are merely convenient or desirable would not be allowed under subsection 32(d).

The City's functions include the administration of by-laws, statutory programs, and activities necessary to the overall operation of the City.

ACT OF LEGISLATURE OR PARLIAMENT [SUBSECTION 32(E)]

This subsection permits the City to disclose personal information for the purpose of complying with an act of the Legislature or of Parliament, or an agreement (ie, collective agreement) or arrangement thereunder, or a treaty. The agreement or arrangement must result from or be sanctioned by a federal or Ontario statute. Disclosure of personal information for the purposes of complying with a regulation or a by-law would be included.

For example:

Section 14 of the *Immunization of School Pupils Act* requires a medical officer of health to transfer a child's immunization records to another medical officer of health when that child moves to a school under the jurisdiction of the latter health unit.

Subsection 72(3) of the *Child and Family Services Act* requires a person (school teacher, principal, social worker, family counselor) to report suspicions of child abuse and to report the information on which the suspicion is based.

Subsection 199(3) of the *Highway Traffic Act* requires a police officer to forward accident reports to the Ministry of Transportation.

DISCLOSURE TO LAW ENFORCEMENT AGENCY [SUBSECTION 32(F)]

A law enforcement institution may disclose personal information to a law enforcement agency in Canada, or to a law enforcement agency in a foreign country under an

arrangement, a written agreement or treaty, or under legislative authority.

Only institutions under MFIPPA which are engaged in law enforcement (national, state or local police agency, a municipal or provincial police agency in Canada, the RCMP, or an agency empowered by statute to enforce a law or by-law) may disclose personal information under this subsection. Law enforcement is discussed in Part 4.

In exchange of personal information with foreign countries, written agreements or treaties should be established. Where this is not possible or practical, an arrangement may be made. An *arrangement* is an unwritten agreement for the exchange of personal information.

When a law enforcement institution discloses personal information to a police agency or other law enforcement agencies in Canada, an agreement or arrangement is not required.

AID IN LAW ENFORCEMENT [SUBSECTION 32(G)]

The City may disclose personal information to another institution covered by MFIPPA, or to a law enforcement agency in Canada to aid an investigation leading or likely to lead to a law enforcement proceeding.

Although this subsection permits the City to release personal information, the City may choose to require a search warrant before access to personal information is granted by an institution.

For example:

> The *Education Act* states that the Ontario Student Record is privileged for the information and use of supervisory officers and principal and teachers of the school. A school may require a police agency to provide a search warrant before disclosing such a record.

COMPELLING CIRCUMSTANCES [SUBSECTION 32(H)]

The City may disclose personal information in compelling circumstances affecting the health or safety of an individual. In compelling circumstances, there may be no other way to obtain the personal information, or there is an emergency where the delay in obtaining the information would be injurious to someone's health or safety. Before personal information is released under this subsection, both of the following conditions must be satisfied:

- The circumstances in which the release of personal information is contemplated

must be compelling, and

- The compelling circumstances must affect the health or safety of an individual.

This section is similar to subsection 14(1)(b).

Where personal information is disclosed under this subsection, notification of the disclosure must be provided in writing and must be mailed to the to the last known address of the individual to whom the information relates. This means the most recent address known to the institution which disclosed the personal information. If no address is known, the City should attempt to obtain it from the person who made the request for information.

COMPASSIONATE CIRCUMSTANCES [SUBSECTION 32(I)]

The City may disclose personal information in compassionate circumstances to facilitate contact with the next-of-kin, ill or deceased.

Compassionate circumstances are those where there is a need to make contact with a friend or next-of-kin to inform them of an individual's injury, illness, or death. The personal information to be disclosed may relate either to the injured or deceased person, or to the relative or friend who is to be contacted.

Only the personal information necessary to facilitate contact should be disclosed.

DISCLOSURE TO MINISTER [SUBSECTION 32(J)]

Personal information may be disclosed to the Minister of Government Services who is responsible for the Act.

For example:

> A request for waiver of notification of personal information under subsection 29(3)(b) may require the disclosure of personal information to the Minister.

DISCLOSURE TO INFORMATION AND PRIVACY COMMISSIONER [SUBSECTION 32(K)]

Personal information may be disclosed to the Information and Privacy Commissioner. Under subsection 41(4), the Commissioner has the authority to examine any record in the custody or control of an institution during the course of an inquiry.

GOVERNMENT OF CANADA OR GOVERNMENT OF ONTARIO [SUBSECTION 32(L)]

Disclosure of personal information is permitted to the Government of Canada or to the Government of Ontario in order to facilitate the auditing of shared-cost programs.

For example:

> Personal information contained in general social assistance case files established under the *Ontario Works Act and Ontario Disability Support Program Act* may be audited by the Province of Ontario.

CONSISTENT PURPOSE [SECTION 33]

Section 33 provides that when personal information is collected directly from the individual to whom it relates, the purpose of its use/disclosure is a consistent purpose only if the individual might reasonably have expected such a use/disclosure.

Subsection 31(b) permits the use of personal information for the purpose for which it was obtained or for a consistent purpose.

Section 32(c) permits disclosure of personal information for the purpose for which it was collected or for a consistent purpose.

A consistent purpose must be compatible with the purpose stated to the individual at the time the information was collected. The individual could therefore reasonably expect this use/disclosure of his or her personal information.

For example:

> An employee of the City could reasonably expect that personal information collected at the time of hiring might be used to assess eligibility for another position.

NEW USE/DISCLOSURE OF PERSONAL INFORMATION [SUBSECTIONS 35(1)(A) AND (B)]

The personal information banks maintained by the City should include a statement of the regular uses of the personal information and the regular users to whom the information is disclosed.

There may be instances where the City uses or discloses personal information for a purpose allowed by the Act, but where that use/purpose has not been listed in the

personal information bank descriptions. Where such a new use or disclosure has occurred, the City is required to:

- Make a record of that new use or disclosure; and
- Attach or link the record of use/disclosure to the personal information bank, so that when the personal information is accessed, the record of use/disclosure is accessed as well. In other words, the record of the new use/disclosure of the personal information becomes part of the personal information itself [subsection 35(2)].

If the new use or disclosure becomes a *regular* occurrence, the City should update its personal information bank description to include the new regular use/disclosure. Once the description has been updated, section 35 ceases to apply.

The requirement to create and attach a record of use/disclosure only applies to personal information which is part of a personal information bank. It does not apply to personal information contained within a general record.

The number of these use/disclosures is included in the annual report to the Commissioner as required by section 26 of the Act.

ROLE OF INFORMATION AND PRIVACY COMMISSIONER [SECTION 46]

Section 46 establishes the powers of the Commissioner relating to the protection of personal privacy.

Subsection 46(a) permits the Commissioner to offer comment on the privacy protection implications of proposed programs of institutions.

Subsection 46(b) enables the Commissioner to, after hearing representations from a head, order an institution to cease a collection practice and to destroy collections of personal information that contravene this Act.

Subsection 46(c) empowers the Commissioner to authorize the collection of personal information otherwise than directly from the individual to whom the information relates. [See the discussion under subsection 29(1)(c)].

Subsections 46(d), (e) and (f) respectively permit the Commissioner to engage in research into matters affecting the carrying out of the purposes of the Act, conduct public education programs about the Act and the Commissioner's role and activities and to receive representations from the public concerning the operation of this Act.

COMPLAINT PROCESS

If there is reason to believe that the City has breached an individual's privacy, a letter of complaint should be mailed or emailed including details about the incident to the following:

City of Brampton
Records and Information Management Office
2 Wellington St. W., 3rd Floor, West Tower
Brampton, Ontario
L6Y 4R2

Or e-mail:

Privacy@brampton.ca

We will investigate your confidential complaint and respond to you directly.

You also have the right to complain formally about a privacy breach to the Information and Privacy Commissioner (IPC).

The IPC will assign a compliance investigator to review the facts of the complaint and will determine if the City has complied with the privacy legislation requirements.

PRIVACY BREACH PROTOCOL

WHAT IS A PRIVACY BREACH

A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with the provision of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). Among the most common breaches of personal privacy is the unauthorized disclosure of personal information, contrary to section 32 of the Act.

Some examples of privacy breaches are:

- Employee Records – employee files containing social insurance numbers left in an unlocked area; Budget reports containing employee numbers and names, found in their entirety in recycle bins and garbage bins; theft from a car of a briefcase containing a list of home addresses of City staff;
- Business Records – a list of names, including credit card numbers, left on the photocopier; personal information disclosed to a Councillor who did not need it

to effectively decide on a matter;

Technology/computer error:

- Employee Records – sending very sensitive personal information to an unattended, open-area printer; password written on a sticky note stuck to a monitor; resumes faxed or emailed to a wrong destination or person.
- Business Records – stolen laptop containing names and addresses of permit holders; disposal of equipment with memory capabilities (e.g., memory keys, disks, laptops, cell phones) without secure destruction of the personal information.

If an individual believes that the City has failed to comply with one or more of the privacy protection provisions of the Act, and that his or her privacy has been compromised as a result, the individual can file a complaint with the Information and Privacy Commissioner of Ontario (IPC). As well, upon learning of a possible privacy breach, the IPC may itself initiate a complaint in the absence of an individual complainant.

If the IPC establishes that there was a privacy breach, it will make recommendations that assist the City in taking whatever remedial steps are necessary to prevent future similar occurrences.

ROLES AND RESPONSIBILITIES IN RESPONDING TO PRIVACY BREACHES - EMPLOYEES

All City employees need to be alert to the potential for personal information to be compromised, and therefore potentially play a role in identifying, notifying and containing a breach. Employees have the responsibility to:

- Notify their supervisor immediately, or in his/her absence, the Freedom of Information Coordinator upon becoming aware of a breach or suspected breach;
- Contain, if possible, the suspected breach by suspending the process or activity that caused the breach.

SENIOR ADMINISTRATION, DIRECTORS, MANAGERS

These individuals are responsible for alerting the Freedom of Information Coordinator of a breach or suspected breach and will work with the Coordinator to implement the 5 steps of the response protocol.

Senior administration, directors and managers have the responsibility to:

- Obtain all available information about the nature of the breach or suspected breach, and determine what happened;
- Alert the Freedom of Information Coordinator and provide as much information about the breach as is currently available;
- Work with the Freedom of Information Coordinator to undertake all appropriate actions to contain the breach;
- Ensure details of the breach and corrective actions are documented.

FREEDOM OF INFORMATION COORDINATOR

The Freedom of Information Coordinator plays a central role in the response to a breach by ensuring that all 5 steps of the response protocol are implemented (see next page).

The Freedom of Information Coordinator will follow the following 5 steps (see next page for response protocol).

Step 1	Respond
Step 2	Contain
Step 3	Investigate
Step 4	Notify
Step 5	Implement Change

THIRD PARTY SERVICE PROVIDERS

The City uses contracted third party service providers to carry out or manage certain services on its behalf. Typical third party service providers are external consultants, records storage and shredding, external researchers and data storage. In such circumstances, the City retains responsibility for protecting personal information in accordance with MFIPPA.

All third party service providers must take reasonable steps to monitor and enforce their compliance with the privacy and security requirements defined in the contracts or service agreements and are required to inform the City of all actual and suspected privacy breaches.

The third party service providers have the responsibility to:

- Inform the City's Freedom of Information Coordinator as soon as a

privacy breach or suspected privacy breach is discovered;

- Take all necessary action to contain the breach as directed by the Freedom of Information Coordinator;
- Document how the breach was discovered; what corrective actions were taken and report back;
- Undertake a full assessment of the privacy breach in accordance with the third party service provider's contractual obligations;
- Take all remedial action to decrease the risk of future breaches;
- Fulfill contractual obligations to comply with privacy legislation.

RESPONSE PROTOCOL: FIVE STEPS IMPLEMENTED CONCURRENTLY BY THE FOI COORDINATOR.

Initiate these steps as soon as a privacy breach has been reported:

STEP 1 – RESPOND

- Assess the situation to determine if a breach has indeed occurred and what needs to be done;
- When a privacy breach is identified by an internal or external source, contact the appropriate area to respond to the breach;
- Provide advice on appropriate steps to take to respond to the breach;
- Report the privacy breach to key persons within the City and, if necessary, to law enforcement;
- Evaluate effectiveness of response to the breach and implement improvement as necessary.

STEP 2 – CONTAIN

- Identify the scope of the breach and contain it (e.g., retrieve the hard copies of any personal information that has been disclosed, determine if the breach would allow unauthorized access to any other personal information such as electronic information system, change passwords and identification numbers and/or temporarily shut down the system if necessary to contain the breach).
- Document the breach and containment activities;
- Develop briefing materials;
- Brief the accountable decision maker, and key persons on the privacy

breach and how it is being managed.

STEP 3 – INVESTIGATE

Once the privacy breach is contained:

- Conduct an investigation with the involvement of other parties as necessary:
  - Identify and analyze the events that led to the privacy breach;
  - Evaluate what was done to contain it;
  - Recommend remedial action so future breaches do not occur.
- Document the results of internal investigation and use the privacy breach checklist for record keeping, including:
  - Background and scope of the investigation;
  - Legislative implications;
  - How the assessment was conducted;
  - Source and cause of the breach;
  - Inventory of the systems and programs affected by the breach;
  - Determination of the effectiveness of existing security and privacy procedures and practices;
  - Evaluation of the effectiveness of the City's response to the breach;
  - Findings, including a chronology of events and recommendations of remedial actions;
  - The reported impact of the privacy breach on those individuals whose privacy was compromised.

STEP 4 – NOTIFY

- Notify, as required, the individuals whose personal information was disclosed;

The purpose of providing notice of a privacy breach to the individuals whose personal information was involved in the incident is to provide them with information about:

- What happened;

- The nature of potential or actual risks or harms;
- What mitigating actions the City is taking; and,
- Appropriate action for individuals to take to protect themselves against harm.

If personal information that could lead to identity theft has been disclosed, affected individuals should be provided with information on steps they can take to protect themselves. If the office of the Information and Privacy Commissioner (IPC) is investigating the privacy breach, indicate that to the affected individuals. Give an explanation of the individual's right to complain to the IPC about the City's handling of their personal information, along with contact information for the IPC.

- Notify appropriate managers and employees within the City of the breach;
- Report the privacy breach to the Information and Privacy Commissioner as appropriate.

Contact information:
Information & Privacy Commissioner
1-800-387-0073
info@ipc.on.ca
www.ipc.on.ca

STEP 5 – IMPLEMENT CHANGE

When determining what changes and remedial actions need to be implemented, consider whether it is necessary to:

- Review the relevant information management systems to enhance compliance with privacy legislation;
- Amend or reinforce the existing procedures and practices for managing and safeguarding personal information;
- Develop and implement new security or privacy measures, if required;
- Review employee training on legislative requirements, security and privacy procedures and practices to reduce potential or future breaches, and strengthen as required;
- Test and evaluate remedial actions to determine if they have been implemented correctly and if policies, procedures and practices need to be modified;

- Recommend remedial action to the accountable decision maker.

HOW DO YOU DETERMINE IF NOTIFICATION IS REQUIRED:

The following factors should be considered when determining whether notification is required:

RISK OF IDENTITY THEFT

Is there a risk of identity theft or other fraud in the City? How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's licence numbers, personal health numbers, debit card numbers with password information, or any other information that can be used for fraud by third parties (e.g., financial).

RISK OF PHYSICAL HARM

Does the loss or theft of information place any individual at risk of physical harm, stalking, or harassment?

RISK OF HURT, HUMILIATION, OR DAMAGE TO REPUTATION

Could the loss or theft of information lead to hurt, humiliation, or damage to an individual's reputation? This type of harm can occur with the loss or theft of information such as mental health records, medical records, or disciplinary records.

RISK OF LOSS OF BUSINESS OR EMPLOYMENT OPPORTUNITIES

Could the loss or theft of information result in damage to an individual's reputation, affecting his/her business or employment opportunities?

IPC WEBSITE

The IPC has published a number of documents that can assist in avoiding a privacy breach. These documents can be found in the **Resources** section of the IPC's website.

The following publications offer guidelines and best practices for protecting privacy:

- *Guidelines on Facsimile Transmission Security;*
- *Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office;*
- *Moving Information: Privacy & Security Guidelines;*
- *E-mail Encryption Made Simple;*
- *Best Practices for Protecting Individual Privacy in Conducting Survey Research;*
- *Indirect Collection Guidelines;*
- *Model Data Sharing Agreement;*
- *Model Access and Privacy Agreement;*
- *Safeguarding Privacy in a Mobile Workplace.*

Guidance is also contained in a number of IPC Practices publications which contain suggestions on how government organizations can further protect privacy.

Privacy Complaint Reports that are publicly available are accessible through the IPC's website. Information about the IPC's privacy complaint process can also be found at www.ipc.on.ca

Authority to Collect [s.28(2)]
Direct notification? [s.29(1)]
Notification of Collection [s. 29(2)]

USE	DISCLOSURE
Accurate and up to date? [s.30(2)]	Accurate and up to date? [s.30(2)]
With consent? [s.31(a)]	With consent? [s.32(b)]
For consistent purpose? [s.31(b)]	For consistent purpose? [s.32(c)]
For the purpose disclosed? [s.31(c)]	Other specific circumstances? [s.32(d) – (l)]
New use? If so, document new use? [s.35]	New disclosure? If so, document new disclosure? [s.35]

Retention and Disposal

Personal information secure and Protected throughout retention and during disposal?

Minimum retention period as Established by regulation?

Personal Information Banks

All personal information banks Identified and described? [s.34(1)]

Descriptions available to public? [s.34(1)]

Descriptions accurate, including new regular uses and disclosures? [s.34(2)]

A. Security of Personal, Confidential or Sensitive Information

1. All hard copies of personal, confidential or sensitive information should be stored in lockable filing cabinets.
2. All electronic personal information records must be maintained in a password-protected database.
3. Do not store personal, confidential or sensitive information on a Shared Network Drive.
4. Immediately pick up any personal, confidential or sensitive records sent to printer, photocopier or received by fax.
5. Immediately retrieve personal, confidential or sensitive information left at the printer/photocopier/fax machine or return them to the owner.
6. Before sending personal, confidential or sensitive information via email, take precautions such as removing personal information.
7. If no alternative to faxing personal, confidential or sensitive information is available, the following precautions should be taken:
    - Ensure that a fax cover sheet is used that contains contact information of both the sender and recent with the mention “Confidential”.
    - Call the intended recipient immediately before and after sending the fax to ensure receipt and immediate pick-up.
    - Print and check a confirmation activity sheet to ensure that the fax reached its intended recipient.
    - Retrieve originals from the fax machine as soon as completed.
8. If it is necessary to take information out of the office, take all necessary precautions to ensure it is protected. Ensure you have managerial approval to take personal, confidential or sensitive information from the workplace.
9. Ensure that you do not access personal information you do not need to perform your duties and responsibilities.
10. Ensure procedures are followed for safeguarding personal information on laptops, memory sticks, personal digital assistants (Blackberry devices), etc.

B. Limitation of Collection, Use, Retention and Disclosure of Personal Information

1. Do not collect, use or disclose identifiable personal information if it is not needed in the performance of duties and responsibilities.
2. If identifiable personal information collection is necessary, it is necessary to obtain the consent of the individual to whom the information relates before collecting, using or disclosing their personal information.
3. The collection, use or disclosure of personal information collected must be limited to that which is required in the performance of your duties and responsibilities.
4. There must be a clear purpose for each type of personal information that is being collected, used or disclosed.
5. Forms, surveys, websites, etc. must provide a notice to individuals regarding the collection of personal information.
6. Ensure that all personal information collected, used or disclosed is utilized for the purpose for which it was collected or a consistent purpose.
7. All notices of collection must provide the specific purposes of the collection, the legal authority for collection and the contact information for an official who can answer questions about the purpose of the collection.
8. Personal, confidential or sensitive information must be disposed of in accordance with established records retention schedules.
9. All personal information stored in the memory of electronic devices (e.g., personal computers, printers, photocopiers, fax machines, etc.) must be deleted prior to these devices being removed from the office.

C. Workstation Security

1. Use a password-protected screen saver and set it to turn on after 5 minutes of inactivity.
2. Always log off or sign out of applications not being used and close the browser window.
3. Shut down the computer at the end of the day.
4. Position the monitor in such a way so that casual observers cannot view

personal, confidential or sensitive information.

5. Adopted a “clean desk” model so that no personal, confidential or sensitive information or material is left unsecured on the desk.

6. Check to ensure that all desk drawers, filing cabinets and/or doors before are locked before leaving for the day.

D. Accuracy

1. Update personal information on a regular basis to ensure that it is still accurate.

2. Ensure procedures are in place so that individuals can update their own personal information so that it is still accurate.

3. Ensure procedures are in place for informing third party service providers to whom personal information has been disclosed, that the information has been updated.

E. Third-Party Service Providers

1. Ensure that when personal information is shared with, or collected, used or disclosed by a third party service provider under an arrangement with the City, that the provider follows its own privacy policies, procedures and practices.

2. Ensure there is a written agreement in place with any third party service provider with which the City is sharing personal information. If the third party has permission to collect, use or disclose personal information on behalf of the City, compliance must be monitored.

F. Employee Records

1. All personnel records, regardless of where they are located, must be securely stored and must only be accessible by authorized personnel.

2. Staff must receive training and must be aware of the City’s Privacy and Access requirements.

G. Privacy Breaches

1. All staff have an obligation to immediately report a suspected or actual privacy breach to their supervisor and the Freedom of Information Coordinator.

2. Staff must all be aware of the City's "Responding to a Suspected Privacy Breach" protocol.

PART 6: FEES

INTRODUCTION

Under the *Municipal Act*, Council can pass a by-law to set fees for copies of records and documents requested by members of the public. The City has such a by-law (i.e. the User Fee By-Law). The fees set out in the by-law can be charged for access requests made outside of the MFIPPA processes (i.e. for proactive disclosure).

In cases where records are not normally made available to the public for a fee and where a request is made under the Act, the person making the request may be required to pay costs incurred by the institution in processing the request [section 45].

CHARGEABLE COSTS

The costs that can be charged under the Act include costs for searching for records and preparing them for disclosure; computer and other costs incurred, and shipping costs.

The costs are specified in R.R.O. 1990, Reg. 823, section 6 (see Appendix 5).

There are two instances where costs may not be charged. An individual is not required to pay a fee for access to his or her own personal information [subsection 45(2)]. Also, the time spent for internal decision-making on an access request cannot be charged to the requester.

The Harmonized Sales Tax (HST) is not applicable to fees charged under the Act. The following are the costs that can be charged to the requester:

COSTS FOR PHOTOCOPIES AND COMPUTER PRINTOUTS

The City can charge $0.20 per page for photocopies and computer printouts. This cost includes the cost of staff time to feed documents into a photocopier.

The City can charge $10 for a CD.

SEARCH TIME

A charge of $7.50 for each 15 minutes can be made for manual search time that is

needed to locate a record. If more than one person is conducting the search, each person's time can be charged.

RECORD PREPARATION CHARGES

Staff time involved in physically preparing the record for disclosure can be charged also at the rate of $7.50 for each 15 minutes. This includes the time for severing exempt material prior to disclosure. Severing or redacting a record includes physically handling, for instance, putting removable tape over exempt portions of the record before it is photocopied, or electronically redacting exempt information from the record.

The City cannot charge staff time involved in reviewing the records to determine if any exemptions apply.

COMPUTER COSTS

The City can charge $15.00 for each 15 minutes spent by a staff person for developing a computer program or other method of producing a record from machine readable record.

In some instances producing a record from a machine readable record will require the manipulation of information stored in a data base. It may be necessary to develop a program to retrieve the particular information.

COSTS FOR SERVICES OUTSIDE THE INSTITUTION

Computer and other costs incurred in locating, retrieving, processing and copying a record can be charged to the requester if those costs are specified in an invoice received by the City. The City may require outside services to assist in locating, retrieving, processing or copying records. Where the City receives an invoice for the cost of outside services, these can be passed on to the requester. The City should ensure, however, that the cost for using outside services would not be greater than the cost of handling the matter internally.

SHIPPING COSTS

Shipping charges such as postage or courier costs can be charged to the requester.

FEE ESTIMATES AND DEPOSITS

Where a fee estimate is $100.00 or more, the City may require the requester to pay a

deposit equal to 50% of the estimate before completing the request.

The City is not required to release records to a requester until the fee has been paid, or the issue of fees has been resolved after an appeal to the Information and Privacy Commissioner.

See Part 3 for the procedure for calculating fee estimates.

WAIVING FEES

The City shall waive all or part of the fees if in the City's opinion it is fair and equitable to do so after considering:

- The extent to which the actual cost of processing, collecting and copying the record varies from the amount of payment required by the Act;
- Whether the payment will cause a financial hardship to the person requesting the record;
- Whether dissemination of the record will benefit public health or safety;
- Whether the person requesting access to the record is given access to it; and
- If the amount of a payment would be $5.00 or less, whether the amount of the payment is too small to justify requiring payment.

The City's decision not to waive a fee may be appealed to the Information and Privacy Commissioner [subsection 45(5)].

PART 7: COMMISSIONER AND APPEALS

INTRODUCTION

MFIPPA gives persons a right to appeal decisions about access to records that are made by the City. Appeals are filed with the Information and Privacy Commissioner (Commissioner) who is an officer of the Ontario Legislature and is independent of the government or any other institution.

This Part outlines the powers of the Commissioner and the appeal process. Many of the procedures have been developed by the Commissioner and are subject to change. Where clarification is needed during an appeal, the City should contact the Appeals Officer assigned to the appeal.

INFORMATION AND PRIVACY COMMISSIONER

THE APPOINTMENT OF THE COMMISSIONER

The Commissioner is appointed by the Lieutenant Governor in Council and is appointed for a term of 5 years and may be reappointed for a further term or terms. The Commissioner is removable at any time for cause by the Lieutenant Governor in Council on the address of the Assembly.

THE POWERS OF THE COMMISSIONER ON APPEAL

The Commissioner makes decisions in respect of appeals by issuing an order [sub section 43(1)]. The order may contain any conditions the Commissioner considers appropriate [subsection 43(3)]. Orders made by the Commissioner are binding on all parties to the appeal. It is an offence to willfully fail to comply with an order of the Commissioner [subsection 48(1)(f)].

Once the order is made, the Commissioner must give notice of the order to appellant, the City and any other affected person [subsection 43(4)].

Where the City has relied on a discretionary exemption to withhold a record, the Commissioner shall not order the disclosure of the record or part of it, however, the Commissioner may order the City to consider the exercise of discretion, where it has not been done.

An appeal is to be made within 30 calendar days after the notice of the decision is given [subsection 39(2)], however, where the City cannot show that it is prejudiced by the delay, appeals launched after the 30-day period may be allowed.

For Example:

> Prejudice may be established where the records referable to the appeal have been destroyed.

Generally, any decision the City makes under the Act may be appealed to the Commissioner. The decisions that can be appealed include:

- A decision to extend the time limit for responding to a request under section 20;
- Refusal to grant access to a record on the ground that the record does not exist;
- Refusal to grant access to a record on the ground that the record is exempt;
- Granting access to only part of the record;
- Granting a request for access to a record or part that may contain information referred to in section 10 (third party information) or that contains personal information where the disclosure may be an unjustified invasion of personal privacy under subsection 14(1)(f);
- Refusal to confirm or deny the existence of a record that deals with law enforcement [subsection 8(3)] or would, if disclosed, be an unjustified invasion of personal privacy [subsection 14(5)];
- A deemed refusal to grant access to records under subsection 22(4);
- A refusal to make a correction to personal information requested under subsection 36(2)(a);
- The amount of a fee charged under section 45;
- Refusal to waive a fee charged under section 45; and
- Refusal to allow a requester to examine the original record under sections 23 or 37.

WHO CAN APPEAL?

The following persons can appeal to the Commissioner:

- A person who has made a request for access to a record under subsection 17(1);
- A person who has made a request for access to his or her own personal information under subsection 37(1);
- A person who has requested correction of his or her own personal information under subsection 36(2); and
- An affected third party who has received a notice under subsection 21(1) that the City intends to disclose a record that may affect the interest of the third party.

THE APPEAL PROCESS

NOTICE OF APPEAL BY REQUESTER

An appeal is initiated by the requester by filing a written notice of appeal with the Commissioner. The appeal must be accompanied by a fee of $25.00 if the request involved general information and $10.00 if the request involved the requester's personal information.

The Commissioner recommends that decision letters sent by the City include a paragraph informing the requester that he or she can appeal the decision to the Commissioner's Office within 30 days. Let the requester know that an appeal should be accompanied by:

- The file number assigned to the request by the City;
- A copy of the decision letter; and
- A copy of the original request for information.

(See Appendix A)

Upon receiving a notice of appeal, the Commissioner must notify the City that an appeal has been filed. The Commissioner must also notify any other person who, in the Commissioner's opinion, is "affected" by the appeal [subsection 39(3)]. The City's Freedom of Information Coordinator should also be notified.

Where the City has any information about the affected persons who should be notified of the appeal, this information should be conveyed to the Appeals Officer assigned to

the case. The affected persons should contact the Freedom of Information Coordinator for further information about the appeal.

CONFIRMATION OF APPEAL

The Commissioner's Office notifies the City that an appeal has been filed by sending out a "Confirmation of Appeal" letter that generally informs the City of the name of the requester, the appeal number and the name of the Appeals Officer assigned to the case.

The "Confirmation of Appeal" letter also asks the City to provide the following information where applicable:

- A copy of the original request;
- The decision;
- Any correspondence related to the request or decision making process;
- An index of records and exemptions; and,
- The record both redacted and un-redacted.

Where the appeal relates to either a time extension or a fee matter, the request for the last two items above will be omitted. Additional information may also be forthcoming at this time that will assist the City to deal with the appeal promptly and efficiently.

DUTY TO PROVIDE RECORDS

The Commissioner may call for and examine any record that is in the custody and under the control of the City, despite Parts I and II of the Act or any other Act or privilege [subsection 41(4)]. Subsection 41(12) states that where records are provided no one is liable to prosecution for an offence against any other Act because of the provision of records. The Commissioner may not delegate his or her authority to any person other than an Assistant Commissioner, the power to require a record referred to in section 8 (law enforcement) to be produced and examined [section 44].

While the Commissioner may require records to be produced, and may enter and inspect any premises occupied by the City for the purpose of the investigation [subsection 41(4)], the City, in exceptional circumstances, may require that the examination of a record by the Commissioner be of the original at its site [subsection 41(6)]. This power may be invoked, for example, if the record is fragile, unique or involves a large volume of records.

Before entering any premises, the Commissioner must notify the City of his or her

purpose [subsection 41(7)].

MEDIATION AND INQUIRY

MEDIATION

According to section 40 of the Act, the Commissioner may authorize a mediator to investigate the circumstances of any appeal and to try to effect a settlement of the matter under appeal.

An Appeals Officer assigned to an appeal will review the circumstances of the case and verify the City's position. Acting as a go-between, he or she will also try to settle the appeal or simply the issues, based on discussions with the appellant and the City [section 40]. In a mediated settlement both parties reach an agreement about the matter under appeal.

The Commissioner's Office will attempt to settle the issues at appeal before resorting to an order. The general time period allotted for mediation is 3 months. It may be shortened if it is apparent that no agreement can be reached. The appeal will then proceed to an inquiry.

THE INQUIRY

Where mediation is unsuccessful, the Commissioner is required to conduct an inquiry to review the City's decision [subsection 41(1)]. At this stage, the appellant and the City receive a "Notice of Inquiry" letter. This notice advises the parties that they are entitled to make representations, usually in writing but can be verbal, to the Commissioner.

Generally, the Notice of Inquiry will supply the parties to the appeal with concise background information and will summarize the facts and issues in the appeal. The Notice of Inquiry will also focus on identifying the requirements of exemption claims as they arise in particular appeals.

The Notice of Inquiry will contain specific questions that relate directly to the issue at appeal. These questions are to be answered by the City and any other party to the appeal. The representations need not be limited to the questions posed in the Notice of Inquiry. Parties may submit additional facts that bear on the appeal.

BURDEN OF PROOF

According to Section 42, where the City denies access to a record or part of a record, the City must prove on appeal that the record, or part, falls within an exemption under the Act. If an affected third party does not want the record or part to be released, the

third party has to prove that the record or part should be exempt from disclosure.

The onus of proving the application of an exemption or an exception to an exemption is on the party claiming the exemption.

WRITTEN OR ORAL REPRESENTATIONS

Inquiries in respect of access to records must be conducted in a manner that protects the confidentiality of records. Therefore, the normal rules governing the rights of parties appearing before tribunals do not apply [subsection 41(2)]. These include the right to a public hearing and the right to cross-examine witnesses.

An inquiry may be conducted in private [subsection 41(3)]. The Commissioner's normal practice is to conduct inquiries through written representations, however, an appellant or the City may request an opportunity to make an oral submission.

The Commissioner may also ask that representations be shared between the parties to the appeal.

The Commissioner has the power to summon and examine on oath any person who may have information relating to the inquiry [subsection 41(8)]. Anything said or any document produced during an inquiry is privileged in the same manner as if the inquiry were proceeding in a court [subsection 41(9), (10) and (11)]. Testimony provided during an inquiry may not be used in other proceedings, except in respect of a prosecution for perjury [subsection 41(10)].

All parties to the appeal must be given the opportunity to make representations, however, no person is entitled to be present during, to have access to, or to comment on representations made to the Commissioner by any other person [subsection 41(13)].

The City, the appellant and any affected party may be represented by counsel or an agent [subsection 41(14)].

COMPLIANCE INVESTIGATIONS

MFIPPA recognizes that the City should have basic standards for protecting personal information in its possession. The privacy provisions of the Act require the City to use appropriate practices and procedures for collecting, storing, using, disclosing and ultimately disposing of personal information.

The Compliance Department of the Commissioner's Office initiates an investigation when a public complaint is received; when an appeal raises compliance or privacy issues; or when the Commissioner's Office determines that a particular issue warrants investigation. Compliance Investigators are directed to conduct a thorough review of

the City‘s practices and procedures and to report findings to the Assistant Commissioner (Privacy).

JUDICIAL REVIEW

The Commissioner has the power to issue a binding order which is not subject to an appeal. Appeals are distinct from judicial review proceedings. Judicial review proceedings are governed by the *Judicial Review Procedure Act*. Applications for Judicial Review may be brought before Divisional Court by a party to an appeal where it is alleged that the Commissioner has made a serious error or where substantial wrong or miscarriage of justice has occurred.

In the order issued by the Commissioner, the party against whom the order is made is advised of the right to apply for judicial review and given 30 days to make the application. Where no application for judicial review is made within that period, the party must comply with the order.

OFFENCES [SECTION 48]

Section 48 of the Act outlines offences under MFIPPA, the penalty for offences and when the consent of the Attorney General is required for prosecution.

Subsections 48(1)(a), (b) and (c) create offences relating to breaches of privacy protection provisions of the Act.

Subsections 48(1)(d), (e) and (f) create offences relating to the obstruction of the Information and Privacy Commissioner in the carrying out of his or her duties or exercising his or her powers.

It is an offence to willfully disclose personal information in contravention of the Act [subsection 48(1)(a)]. The offence consists of intentionally and knowingly disclosing personal information in a manner that is not authorized by the Act.

It is an offence to willfully maintain a personal information bank that contravenes the Act [subsection 48(10(b)]. The offence in this case is to intentionally maintain a secret personal information bank that is not described and made public as required by section 34. The IPC may order the destruction of a collection of personal information that contravenes the Act. The Commissioner may also order the City to cease collecting certain types of personal information.

It is an offence to make a request under this Act for access to or correction of personal information under false pretenses [subsection 48(1)(c)].

Subsections 48(1)(d), (e) and (f) create offences relating to the obstruction of the Information and Privacy Commissioner in the carrying out of his or her duties or exercising his or her powers.

It is an offence to willfully obstruct the Commissioner in the performance of his or her functions under the Act [subsection 48(1)(d)]. Subsection 48(1)(d) creates an offence of willfully making a false statement to mislead or attempt to mislead the Commissioner. It is an offence to willfully fail to comply with an order of the Commissioner [subsection 48(1)(f)].

A person who is found guilty of an offence is liable to a fine not exceeding $5,000 [subsection 48(3)].

A prosecution cannot be commenced under subsection 48(1)(d), (e) or (f) without the consent of the Attorney General.

LIABILITY [SUBSECTIONS 49(2) AND (3)]

Civil actions cannot be brought against an employee of the City for monetary damages resulting from the disclosure or non disclosure of a record under the Act, if the action was done in good faith. Subsection 49(2) also provides that no civil action can be brought against an employee for failure to give a required notice under the Act if reasonable care was taken to give notice.

The Act preserves the liability of the City, as opposed to the individual employee, to civil proceedings for damages, however, an employee's actions can make the City liable.

APPENDICES

A) SAMPLE NOTIFICATION LETTERS

1. Notice of receipt of request
2. Notice to Institution Receiving a Transferred/Forwarded Request
3. Notice of time extension
4. Fee estimate/interim notice decision regarding disclosure
5. Notice to affected third party (section 10: third party information)
6. Notice to affected third party (section 14: personal privacy)
7. Notice to requester where third party is affected
8. Notice to affected third party after representations where head intends to release t he record(s)
9. Notice to requester regarding an access decision
10. Notice to requester – correction of personal information
11. Additional Information where appeals are likely
12. Internal memo to program area regarding an FOI request

See Part 3 (Access Procedures) for a detailed discussion of when notifications are required during the processing of a request.

[Date]

[Requester's Name and Address]

Dear _____

Re: FOI Request #

This acknowledges your access request which we received on [**insert date**] under the *Municipal Freedom of Information and Protection of Privacy Act.* We received your $5.00 application fee and your request for access to the following: [**insert details of records requested**]

Option: Further information/Clarification required]

Unfortunately, the request does not provide sufficient detail to identify the record(s). Please supply the following information so that we may begin to process your request:

[**insert details of records requested**]

We would be happy to answer any questions or assist you in clarifying or reformulating your request.

If we do not hear from you within 30 days of this letter's date, we will close your file.

Option: Transfer/Forward

[**Name and address of other institution**] has (custody or control of) **OR** [a greater interest in] the records you seek. Under section 25 of the Act, we (forwarded) **OR** (transferred) your request to them. Since we are not processing your request, we are returning your $5.00 application fee with this letter. Please send a new application fee to the institution listed above.

You may appeal this decision to the Information and Privacy Commissioner. The Commissioner can be reached at:

[**insert details of IPC]**

[See also Additional Information #11]

Please contact [**name, title and phone number of person responsible**] if you have any questions. We would appreciate you using the Request number assigned to your request in any further correspondence.

NOTE: As quickly as possible, the other institution should be notified that a request is being forwarded/ transferred.

Sincerely,

[**Date**]

[**Name and Address transferee institution**]

Dear _____

Re: FOI Request #

The enclosed request for access was received by the City of Brampton on [**date**]. This request is [transferred/forwarded] to you under section 25 of the *Municipal Freedom of Information and Protection of Privacy Act* as we believe your institution has [custody or control of/greater interest in] the record.

We have returned the application fee to the requester and have instructed him/her to send an application fee to you.

Sincerely,

[**Date**]

[**Requester's name and address**]

Dear _____

Re: FOI Request #

This acknowledges receipt of your access request which we received on [**insert date**] under the *Municipal Freedom of Information and Protection of Privacy Act*. We received your $5.00 application fee and your request for access to the following:

[**insert details of records requested**]

A request under the Act usually must be answered within 30 calendar days, however, section 27 of the Act (enclosed) allows for time extensions under certain circumstances. The time limit for answering your request has been extended for an additional [**insert number**] days to [**insert date**].

The reason for the time extension is [**insert reason**]:

You may request that our decision to extend the time limit be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[**insert address]**

(See also Additional Information #11)

Please contact [**name, title and phone number of person responsible**] if you have any questions. We would appreciate you using the Request number assigned to your request in any further correspondence.

Sincerely,

[**Date**]

[**Requester's name and**

address] Dear _____

Re: FOI Request #

This acknowledges receipt of your access request on [**insert date**] under the *Municipal Freedom of Information and Protection of Privacy Act* for access to [**describe records requested**]. An initial review of the records indicates that it will cost an estimated [**enter amount**] to process your request. The fee estimate is based on [**explain fee estimate**].

As we have not yet reviewed the records in detail, no final decision has been made regarding access but the following exemptions will likely apply. [**Generally describe what exemptions might apply to the records**].

[AND: Where the fee estimate is over $100.00]

Regulation 823 says that where the fee estimate is over $100.00, the City may request a deposit equal to 50% of the estimated fee. We will wait until we receive the amount of [**enter amount**] from you before we resume processing the request.

The Act provides that all or part of the fee can be waived if in our opinion it is fair and equitable to do so, if the fee will cause you financial hardship or if dissemination of the record will benefit public health or safety. You may be required to provide proof to support any waiver claims. Please notify [**insert name, title and phone number**] as soon as possible of you wish to proceed with a request for a fee waiver.

If you disagree with any aspect of the fees, or wish to revise your request, please discuss the matter with us. Afterward, you may request that this fee estimate be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

(See also Additional Information #11)

Please note that you have 30 days from the receipt of this letter to request a review from the Commissioner. If we have not heard from you within 30 days, we will close your file.

Please contact [**name, title and phone number**] with any questions. We would appreciate you using the Request number assigned to your request in any further correspondence.

Sincerely,

NOTE: A Notice of Time Extension can be included in this letter if required.

[**Date**]

[**Affected third party's name and**

address] Dear ____

Re: FOI Request #

The City of Brampton has received a request for access to records under the *Municipal Freedom of Information and Protection of Privacy Act* to disclose [**describe in detail the records as they relate to s. 10 affected third party**].

According to Section 21 of the Act, a third party whose interests may be affected must be given the opportunity to make representation to the City concerning disclosure of the records.

To successfully qualify for a third party exemption, *all* of the following 3 tests must be met:

- The information must fit within one of the specified categories of third party information: trade secret or scientific, technical, commercial, financial or labor relations information;
- The information must have been *supplied* by the third party *in confidence*

  implicitly or explicitly; and
- The disclosure of the information could reasonably be expected to cause one of the harms outlined below:

  i. Prejudice your competitive position or interfere with any contractual rights you possess, or

  ii. Result in you no longer supplying this or similar information to the City of Brampton;

  iii. Result in undue loss or gain to any person, business or organization of which you are aware.

Under section 10 of the Act, we must release these records unless the above conditions are met. Please review the attached records.

If you have concerns about the release of the records, please contact us, in writing, no later than [insert date] outlining your concerns. In order to support your claims against the release of the records or portions of the records, you must show how those records meet the third party criteria set out in this letter.

We will notify you in writing by [insert date] **about our decision regarding the release of the records.**

Enclosed are copies of sections 10 and 21 of the Act for your convenience and information. Please contact [name, title and phone number of person responsible] **if you have any questions. We would appreciate you using the request number assigned to the request in any further correspondence.**

Sincerely

[**Date**]

[**Affected third party's name and**

address] Dear ____

Re: FOI Request #

The City of Brampton has received a request under the *Municipal Freedom of Information and Protection of Privacy Act* to disclose [**describe in detail the records as they relate to the affected individual**].

Section 14 of the Act says individuals have the opportunity to make representations about the release of their personal information to a third party.

Your views regarding disclosure of these records is appreciated. Please indicate in writing whether or not you consider that the disclosure of the enclosed records would be an invasion of your personal privacy. Section 14 of the Act outlines circumstances where the disclosure of personal information may be an unjustified invasion of personal privacy.

Your response must be received no later than [**insert date**]. You will be notified in writing by [**insert date**] about our decision regarding the release of the records.

Enclosed are copies of sections 14 and 21 of the Act for your convenience and information. Please contact [**name, title and phone number of person responsible**] if you have any further questions. We would appreciate you using the Reqeust number assigned to the request in any correspondence.

Sincerely

[**Date**]

[**Requester's name and**

address] Re: FOI Request

#

This acknowledges your access request which we received on [insert date] under the *Municipal Freedom of Information and protection of privacy Act* for access to [**describe records requested**].

The disclosure of the records may affect the interest of a third party.

The third party whose interests may be affected is being given the opportunity to make representations about the release of the record(s).

A decision on whether or not the record(s) will be disclosed will be made by [**insert date**], under section 21 of the Act.

Enclosed is a copy of section 21 of the Act for your convenience and information. Please contact [**name, title and phone number of person responsible**] if you have any further questions. We would appreciate you using the Request number assigned to the request in any correspondence.

Sincerely,

[**Date**]

[**Affected third party's name and**

address] Dear _____

Re: FOI Request #

We have received and considered your representations concerning disclosure if [details of the record(s)]. Our decision is to grant access [**or partial access]** to the record(s). [**Give reasons for the decision**].

Under Section 21 of the *Municipal Freedom of Information and Protection of Privacy Act* you may request that this decision be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

(See also Additional Information #11)

You have until [**insert date**] to request a review, otherwise the records will be released to the requester.

Please contact [**name, title and phone number of person responsible**] if you have any further questions. We would appreciate you using the request number assigned to the request in any further correspondence.

Sincerely

[**Date**]

[**Requester's name and**

address] Dear_____

Re: FOI Request #

In response to your request under the *Municipal Freedom of Information and protection of Privacy Act* for access to [**describe records requested]:**

Option: access granted

We are pleased to inform you access is granted to [**insert details**].

Option: subject to copyright

Please note that you are bound by any copyright that applies to the records you receive under this ct.

Option: no records exist

Access cannot be provided to [**insert details of nonexistent records**] as the records do not exist.

Option: denial of access

Access is denied to [**insert details of withheld records**] under section(s) [**insert section numbers]** of the Act. The provisions apply to the record(s) because [**insert reasons**].

Option: refusal to confirm existence

Under section [**14(5) or 8(3)]** we cannot confirm or deny the existence of the record.

Option: summary of records categories

Due to the complexity of your request, we have summarized the records in the attached Index of Records.

You may request that this decision be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

(See also Additional Information #11)

Please note that you have 30 days from the receipt of this letter to request a review.

Please contact [**name, title and phone number of person responsible**] if you have any questions. We would appreciate you using the request # assigned to your request in any further correspondence.

Sincerely

NOTE: In this notice (if partial access is granted) the following could be included:

- **Indicate the fees for access to the records, if any;**
- **Give the requester the option to view the record; or**
- **Indicate that identification will be required if access is given to an individual's own personal information**

[**Date**]

[**Requester's name and**

address] Dear__

Re: FOI Request #

Your request under the *Municipal Freedom of Information and Protection of Privacy Act* for a correction of personal information was received on **[insert date].**

The correction was made and a copy of the corrected record is attached. On request, you are entitled to have the correction sent to those persons to whom the information was disclosed over the past 12 months.

OR

The correction was not made to the personal information. In reaching this decision, we considered the following 3 elements: 1) whether the information is personal and private;

2) whether the information is inexact, incomplete or ambiguous and 3) whether the correction would be a substitution of opinion **AND/OR [insert reason why the request was refused] [optional].**

You are entitled to require that a statement of disagreement be attached to the record and that the statement of disagreement be sent to any person to whom the record was disclosed over the past 12 months.

You may appeal this decision to the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

(See also Additional Information #11)

Please note that you have 30 days from the receipt of this letter to request a review.

Sincerely

#11 ADDITIONAL INFORMATION WHERE APPEALS ARE LIKELY

If you decide to appeal a decision to the Information and Privacy Commissioner, please provide the Commissioner's office with:

1. The request number assigned to the request
2. A copy of this decision letter, and
3. A copy of the original request you sent to the City of Brampton

Appeals to the Commissioner must also be accompanied by the appropriate fee. Fees vary according to the nature of the request being appealed as follows:

a) $25 if the person appealing has made a request for access to a general record under subsection 17(1) MFIPPA;

b) $10 if the person appealing has made a request for access to personal information under subsection 37(1) MFIPPA; and

c) $10 if the person appealing has made a request for correction of personal information under subsection 36(20 of MFIPPA.

No fee is payable for appealing a decision of a head to the Commissioner if the person appealing is a third party given notice of a request under subsection 21(1) of MFIPPA.

MEMORANDUM TO: (Name of Contact and Program

Area) OUR REFERENCE: FOI Request #

The attached request was made under the *Municipal Freedom of Information and Protection of Privacy Act* and concerns records which we believe to be in the custody of your division.

Please review the request and conduct a search for the records.

Your response to this request should be forwarded to this office, to be received on or before (date), and should include:

1. Original of the records. If some or all of the responsive records are available only in electronic format, please contact the FOI Coordinator immediately to discuss format.
2. Name(s) of staff who searched for the records, as well as the time spent locating and searching for the records.

If the records are not in the custody of your area, please provide a "nil" response. You should be aware that "nil" responses may require an affidavit at a later date, therefore, please note the date, time and location of the searches conducted and by whom they were conducted.

If due to volume of records, or any other legitimate reason, you are unable to provide the records on or before (date), please let us know as soon as possible as it may be necessary to inform the requester that a time extension is required.

The response must be signed off by the Director of the program

area. If you have any questions, please call me at (telephone #)

Freedom of Information Coordinator

B) ROLES AND RESPONSIBILITIES

INTRODUCTION

The City, as a whole and the Head (City Clerk) are accountable for complying with MFIPPA. Complying with the access to information and privacy requirements of MFIPPA involves all employees of the City and is an integral part of the business of each division. Staff should not see complying with MFIPPA requirements as separate from the business of delivering a program or service. Under MFIPPA, the Information and Privacy Commissioner (IPC) has investigation and order-making powers to enforce compliance.

Accordingly, City staff must make the processing of requests for access to information a top priority so that the City does not exceed the statutory time limits under MFIPPA for issuing decisions on access to information requests.

ROLE OF THE HEAD

The Head is responsible for making sure that the "institution" (the City of Brampton) properly discharges its statutory obligations under MFIPPA.

In discharging this responsibility, the Head makes sure that the departments/divisions adhere to the procedures in this manual and to other City procedures and practices that promote compliance with MFIPPA.

RESPONSIBILITIES

The Head is responsible for:

- Intervening effectively when staff members are not meeting internal benchmarks for departmental action;
- Ensuring that staff members meet statutory timelines for responding to an access request.

DEPARTMENTAL/DIVISIONAL CONTACTS

The Director of each division shall be the primary contact for the purpose of responding to formal access requests that requesters submit under MFIPPA. The Director is responsible:

- to ensure an appropriate member of staff responds to all MFIPPA requests

pertaining to the division;

- to intervene, if necessary, to make sure that the retrieval and review of records is timely and complete;
- to be the primary contact for communications regarding release of records under MFIPPA.

RESPONSIBILITIES

It is the responsibility of each department/division to:

- ensure that staff receive MFIPPA training offered by the Freedom of Information Coordinator and records management training offered by Records Services;
- ensure that a properly trained staff member is tasked with fulfilling the functions set out in the Access and Privacy Manual;
- ensure that the Freedom of Information Coordinator is provided with tracking sheets and records responsive to access requests within the time limits communicated by the Coordinator;

Staff assigned to researching and retrieving records must have the skills and training required to perform their duties, including:

- a working knowledge of the access provisions of MFIPPA;
- familiarity with the division's record holdings;
- an understanding of the operational significance and context of division records;
- ability to work under tight timelines;
- sound judgment, analytical and organizational skills

FREEDOM OF INFORMATION COORDINATOR ROLE

On behalf of the City Clerk, the Freedom of Information Coordinator receives requests for access to records that are submitted by requesters in writing under MFIPPA. The Coordinator also coordinates the City's response to these requests and decides on behalf of the Clerk whether a requester is entitled to receive records, subject to any right of appeal to the Information and Privacy Commissioner/Ontario.

RESPONSIBILITIES

- Manages the overall process of responding to access requests;
- Receives access requests, clarifies requests, if necessary, and contacts the appropriate PL to begin searching for and retrieving appropriate records and/or requests time extensions;
- Informs departmental/divisional management staff on how the division is complying with timeframes and access request procedures;
- Determines by discussing with requesters and division staff whether a requester can access all or substantial portions of requested records outside of the statutory requirements of the Act;
- Makes sure that the City claims any required time extensions and charges fees and deposits; prepares time extension and fee estimate/deposit letters, based on documented input received from division staff;
- Reviews records provided by the divisions;
- Redacts exempt information and prepares records for release;
- Prepares decision letters;
- Provides training, advice and support for City staff as required;
- Liaises with the Clerk, Legal staff and division staff on appeals or complaints to the IPC;
- Manages all stages of the appeal process, including mediation and inquiry.

LEGAL SERVICES ROLE

Legal Services provides legal opinions on access requests, as requested by the Freedom of Information Coordinator. Legal Services may represent the City on appeals to the IPC and in proceedings before the IPC.

RESPONSIBILITIES

- Provide legal advice on jurisdictional issues with MFIPPA and other statutes to the City Clerk and divisions as required;
- Represent the City before the IPC in inquiries arising from decisions regarding access to records;

- Provide advice to the City Clerk on whether to seek judicial review of IPC decisions under MFIPPA;
- Communicate to the Freedom of Information Coordinator any legal issues about access requests as required;
- Refer any formal requests from program areas for advice regarding the interpretation of MFIPPA to the Freedom of Information Coordinator;
- Notify the Freedom of Information Coordinator prior to disclosure to a City division of advice or opinions on the interpretation of MFIPPA to ensure consistent treatment of open access files and direction to program areas;
- Prepare representations or reconsideration requests, where necessary, regarding inquiries conducted by the IPC for the Clerk's signature in accordance with the timelines set by the IPC for submission of representations;
- Provide legal opinions (formal or informal) as requested by the Freedom of Information Coordinator.

C) PRIVACY BREACH REPORT

Breach Report #_____

Take immediate action when you have been advised of a suspected privacy breach. Many of the steps outlined below have to be carried out simultaneously. Steps 1 and 2 are completed based on the information received either directly from an employee, or orally through his/her immediate supervisor (e.g., phone call) or in written form (e.g., e-mail).

Step 1 – Respond, and Step 2 – Contain

1. **Person Reporting Suspected Breach:**			
First Name:		Last Name:	
Job Title:			
Location (Department/ Division):			
Name of immediate supervisor:			
Phone:		E-mail:	
2. When Incident Occurred:			
Date (mm/dd/yyyy):		Time indicate (am/pm):	
3. Incident Details:			
Number of individuals whose information was accessed without consent or authorization i.e.) health/ medical information, biographical information such as home address, phone numbers, names and contact information of family members, behavior concerns, disciplinary information, etc.			
Whom the personal information belongs to and how many individuals were affected (i.e. employee, third party, volunteer):			
Who had unauthorized access to the personal information and how that access was made:			
Efforts made, if any, to contain the privacy breach (i.e. suspending the process/ activity that caused the breach)			

Date (mm/dd/yyyy):		Time indicate (am/pm):	

Step 3 – Investigate

Following a report of a suspected privacy breach, ensure that the activity/process has been contained if possible. Conduct an investigation of the information supplied in Steps 1 and 2 of this report in conjunction with current privacy legislation (MFIPPA) and with the City's practices and procedures to determine if the incident is, in fact, a breach. Note: You may wish to consult legal counsel to assist in your investigation.

If a breach HAS NOT occurred:

> Contact the person who reported the suspected breach and his/her immediate supervisor to advise him/her of your determination. No further action is required by the employee or supervisor

Step 4 – Notify

If a breach HAS occurred:

Notify the following individuals as appropriate:

- Individuals whose privacy was breached
- Senior administration/ supervisor/ manager
- Legal Counsel
- Other
- Information and Privacy Commissioner (IPC)*

***Note**: The type and extent of the breach will influence your decision to notify the IPC.

Step 5 – Implement Change

Steps taken to correct the problem:

- Develop, change or enhance policies and procedures
- Ensure strengthening of security and privacy controls
- Advise IPC of investigation findings and corrective action

Provide additional notices (as deemed appropriate):

- Relevant third parties
- Consider public announcement (i.e. statement and/or apology)

Prevent future breaches:

- Arrange employee training on privacy and security
- Recommend appropriate and necessary security safeguards
- Evaluate the effectiveness of remedial actions

The FOI Coordinator may wish to review City policies, procedures, practices and training materials to ascertain whether any revisions are required to ensure a clearer understanding of what constitutes a privacy breach.

Sign-off

The Head or designate (i.e. FOI Coordinator) is required to sign below to formally acknowledge that the breach was managed in accordance with privacy legislation.

_____	_____
Print Name/ Title	Signature

Sign-off Date:_____

(mm/dd/yyyy)

D) PROACTIVE DISCLOSURE

OVERVIEW

A major challenge for all levels of government is meeting the public's growing need for information in a cost effective way. To satisfy this demand and foster open government, the IPC encourages the proactive disclosure of information.

Proactive disclosure occurs when:

- A request for a general record can be granted outside of the formal access process prescribed by MFIPPA (informal disclosure); or
- Information or records are periodically released (without any request) pursuant to a specific strategy for release of information (routine disclosure).

There are many advantages to proactive disclosure. Not only will the public be better served and better informed, but proactive disclosure is cost effective for the City as well. Processing requests and appeals within the confines of MFIPPA is more expensive and time consuming than having predictable access to pre-identified categories of records.

Proactive disclosure can be labour saving. Classifying records as subject to proactive disclosure and ensuring that front line staff is aware of these classifications will make it easier for staff to provide information to the public in an efficient manner.

The establishment of proactive disclosure practices can be an important part of the City's commitment to an open exchange of information with the public that it serves. City divisions are encouraged to be proactive in establishing practices that foster proactive disclosure. In the process of determining these practices, the following principles should be incorporated:

1. In the spirit of MFIPPA, unless there is a statutory requirement or reason not to release the documentation, proactive disclosure of general records should become the norm.
2. Good customer service should always be of primary importance whether requests for information are made formally or informally. The actual needs of the customer should be addressed to the extent possible. Anticipating the needs of the customer and making the information available in advance of a request is the ultimate objective for which City divisions should aim.

Although proactive disclosure is not specifically mandated by statute in Ontario, MFIPPA makes provision for the disclosure of information outside the formal access process – for example, through oral requests or in the absence of requests.

RESPONSIBILITY FOR PROACTIVE DISCLOSURE

Each department is responsible for ensuring appropriate proactive disclosure practices are developed and implemented. The Freedom of Information Coordinator provides guidance and research to assist in developing such practices and for promoting proactive disclosure concepts to City departments.

GUIDELINES FOR CITY DEPARTMENTS/DIVISIONS

The following practices are intended as tools which can help determine which records could be classified as subject to proactive disclosure.

As required by MFIPPA, the City has developed a directory of records identifying the various types of records maintained by each department/division. The directory of records represents a good starting position to implement proactive disclosure.

The City's classification system contains access codes which can assist in determining whether the records can be proactively disclosed.

When reviewing records, look for trends in the requests you receive. For example, a matter continually subject to public debate that would result in a number of requests may constitute a trend. Use these trends to help identify other record categories that could be subject to proactive disclosure. As trends develop, you will find that the process of classifying records will become easier.

To determine which types of general records are good candidates for proactive disclosure, the following practices should be considered:

1. If disclosure is mandated by another piece of legislation, the record is to be released. For example, the *Assessment Act* requires that the assessment roll be made available for examination by the public.
2. Once records have been identified for proactive disclosure, the authority to disclose these documents should be delegated, to the extent possible, to front line staff within the division.

3. A list of division records subject to proactive disclosure should be created and distributed to front line staff. This list can then be used as a reference source.

4. When a list of records is prepared, front line staff can provide feedback on the list by evaluating how useful it is and provide suggestions on how to improve it. Divisions can then add records to the list and update the directory of records.

5. Any class of record which is released regularly, without exemption, should be reviewed to determine whether it should be subject to proactive disclosure.

6. All newly created records should be evaluated to determine if there might be public benefit/interest in proactive disclosure.

7. If a record contains both general information and personal information, but the main purpose of the record is to provide general information, review the record to determine if the personal information can be removed. If the information is removed and the record is then modified, parts of the record could then become subject to proactive disclosure.

8. Where a division decides that a record is not subject to proactive disclosure, the division should consider whether parts of the record could be subject to proactive disclosure (for example, complaints – a complaint can be released routinely once the personal information has been removed).

9. Records that are to be subject to proactive disclosure should be determined by the nature of the record and not by the identity of the requester or the use to which the record will be put.

10. The list of records which are subject to proactive disclosure should be reviewed on an annual basis to ensure the list is accurate and up to date.

11. Apply proactive disclosure principles to make the process of providing access to an individual's personal information a more routine and less time consuming process, always bearing in mind the need to protect the privacy of others. For example, ensuring to the extent possible that records compiled in a client file contain only that person's personal information. This would give access to the individual a routine matter.

The following provides examples of legislation that requires proactive disclosure of City records:

Legal Authority	Records Subject to Proactive disclosure
Municipal Act, s.158	Business Licensing List • The classes of business subject to licensing • The amount of each business licence fee • The cost of administering and enforcing the licensing by –law with respect to each class of business • How the amount of the licence fee is calculated The classes of business subject to business registration
Municipal Act, s.253	Records of the Clerk • By-laws and resolutions of the City and its local boards • Agendas and minutes and proceedings of regular, special or committee meetings of Council or a local board, whether the minutes and proceedings have been adopted or not • Records considered at a meeting (reports), except reports considered during a meeting closed to the public • The records of Council • Statements of remuneration and expenses of elected officials
Municipal Act, s. 268	Property Register Public register listing and describing the land owned or leased by the City or local board
Municipal Act, s.295	Financial Statements Audited financial statements, the notes to the financial statements, the auditor's report and the tax rate information for the current and previous year as contained in the financial review
Municipal Act, s.299	Efficiency and Effectiveness Information Information designated by the Province which relates to the efficiency and effectiveness of the City's operations

Municipal Act, s.300	Service Improvements Annual notice to the public of: • Improvements in the efficiency and effectiveness of the delivery of services by the City and its local boards • Barriers identified by the City and its local boards to achieving improvements in efficiency and effectiveness
Municipal Act, s.331	Property Tax Information List of the comparable properties and the determination made with respect to that eligible property (provided to property owner)
Municipal Act, s.352	Tax Statements Itemized statement of amounts owing for taxes on any separately assessed rateable property
Municipal Act, S.374	Tax Arrears Certificates • Notice of the registration of the tax arrears certificate (provided to owner and interested parties) • Statutory declaration stating the names and addresses of the persons to whom notice was sent
Municipal Act, s.378	Property Tax Extension Agreements • Extension agreements with the owner of the land, the spouse of the owner, a mortgagee or tenant in occupation of the land extending the period of time in which the cancellation price is to be paid
Municipal Act, s.379	Service Fees List • A list indicating which City services, activities and use of properties are subject to fees or charges and the amount of each fee or charge
Municipal Act, Reg.119/03 s.392	Local Improvement Roll Local improvement roll and statement of cost of the work

Assessment Act, s.39	Assessment Roll Description of land, names of persons liable to assessment, amount assessable against each person, names of tenant supporters of a school board, number of acres, current value, amount of taxable land, value of land exempt from taxation, classification, religion (if Roman Catholic), type of school board the person supports, corporations designated as ratepayers
Emergency Management Act, s.10	Emergency Plans Provision of necessary services during an emergency, procedures and manner of responding to the emergency
Municipal Elections Act, s.88	Election Records Documents filed with or prepared by the Clerk for an election. The List of Electors is only available during the period of the election.
Planning Act, s.20	Official Plan Goals, objectives and policies established primarily to manage and direct physical change and the effects on the social, economic and natural environment of the City or part of it
Planning Act, s.44	Committee of Adjustment Records Minutes and records of all applications and decisions and of all other official business of the committee
Ontario Heritage Act, s.27	Heritage Property Register Legal description, name and address of the owner, statement explaining the cultural heritage value or interest, description of the heritage attributes

In addition to legal requirements for proactive disclosure in other legislation as set out above, there are many other documents currently being disclosed by the City on a routine basis.

Some of these are:

- Employees' own personal information
- Fire Incident Reports
- Environmental records
- Budget information/financial statements