

The rights of Toronto City Councillors to access information and their obligations to protect the confidentiality of information are set out in:

- Ontario's *Municipal Freedom of Information and Protection of Privacy Act*;
- Toronto's *Code of Conduct for Members of Council*.

The provincial Information and Privacy Commissioner and City's Integrity Commissioner oversee the application of these rights and obligations.

This guide helps Members of Council understand their rights and obligations and suggests ways to exercise those rights and meet those obligations. In doing so, it also outlines some of the requirements for making information accessible with which the City administration must comply.

### 1. Access to City information

1.1 Individual Councillors are provided access to City information as directly as possible, subject only to specific legislative restrictions.

Individual Councillors have the same rights of access to City records as a member of the public. A Councillor does not have greater rights of access to confidential information by virtue of office. Councillors may request City information from the appropriate Division Head or through the committee's Secretariat contact.

The City of Toronto is building a culture of openness as part of its commitment to delivering accountable government. This means that City information is made available and accessible to the public unless prohibited by law. Opening up government information leads to collaboration and information sharing, promotes citizen engagement, delivers more efficient public services, demonstrates accountability and provides economic development opportunities. Openness is a key driver for initiatives including:

- OPEN DATA (<http://www.toronto.ca/open>)

The Open Data initiative started in 2009 with the release of a limited number of data sets to the public. Data sets continue to be added to this site and it has been recognized by the Information and Privacy Commissioner in her *2009 Annual Report* (p. 7). Application developers have used City data to create web applications.

- PROACTIVE DISCLOSURE (PUBLISHED OR AVAILABLE ON REQUEST)

Closely related to Open Data, City divisions proactively publish documents and data by putting it on their website, making it available on request or in other ways. For example, Councillors proactively disclose expense information through the City Clerk's Office ([http://www.toronto.ca/city\\_council/salaries.htm#exps](http://www.toronto.ca/city_council/salaries.htm#exps)).

Other examples of proactively disclosed information include:

- Municipal Licensing & Standards Investigation Activity Search - information related to by-law enforcement activity by property address (<http://www.toronto.ca/investigationactivity/index.htm>)

- Toronto Public Health Dine Safe -inspection results of restaurants by Public Health (<http://www.toronto.ca/health/dinesafe/index.htm>)
- Children's Services Child Care Finder – maps and listings of licensed child care centres (<http://www.toronto.ca/children/index.htm>)
- Transportation Services Road restrictions (<http://map.toronto.ca/roadrestrictions/index.jsp>)

Not all information warrants publication. For example, it may be difficult to format the information for posting on the web. Divisional disclosure plans (or catalogs) summarize information that can be requested by Councillors and the public directly from the City division. This means that these do not need to be formal requests made under *MFIPPA*.

See the following for examples of disclosure plans:

- Toronto Building - [http://www.toronto.ca/cap/pdf/toronto\\_building.pdf](http://www.toronto.ca/cap/pdf/toronto_building.pdf)
- City Planning - [http://www.toronto.ca/cap/pdf/transportation\\_services.pdf](http://www.toronto.ca/cap/pdf/transportation_services.pdf)

Links to all current disclosure plans can be found at the City Clerk's Office website ([http://www.toronto.ca/cap/routine\\_disclosure\\_plan.htm](http://www.toronto.ca/cap/routine_disclosure_plan.htm)).

- FORMAL REQUESTS FOR INFORMATION

A formal request for City information under *MFIPPA* legislation. This is the appropriate process where the information may not exist in the form requested or where the requested information may relate to private individuals or other third party interests, etc. Access request forms are available at any Elections and Registry Services counter in City Hall and the civic centres, and on the City Clerk's Office website ([www.toronto.ca/cap](http://www.toronto.ca/cap)) and there is a legislated \$5 fee. (See "Access Request Process, Appendix A, for additional information.)

### 1.2 ACCESS BY COUNCILLORS TO PERSONAL INFORMATION

Councillors may obtain personal information about individuals only under the following conditions:

- with the written consent of the individual to disclosure of the particular information;
- under compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill, or deceased; or
- without consent of the individual in a closed meeting of Council/committee, for the purpose of conducting Council/committee business.

### 1.3 MORE INFORMATION ON COUNCILLORS' ACCESS TO CITY INFORMATION

The *Code of Conduct for Members of Council*

([http://www.toronto.ca/city\\_council/pdf/members\\_code\\_conduct.pdf](http://www.toronto.ca/city_council/pdf/members_code_conduct.pdf)) prohibits Members from using their authority to coerce or influence staff with the intent of interfering with that person's duties. The prohibition includes an obligation upon Members not to secure or attempt to secure information from City officials to which they are not entitled to have access.

Information regarding specific legislation and legislative restrictions governing access to City records is available from the Executive Director, Corporate Information Management Services, or Director, Council and Support Services.

## **2. Protecting confidential information**

2.1 Members of Council are prohibited by the *Code of Conduct* from disclosing confidential information unless required by law or authorized by Council. Confidential information may be shared with a Councillor through his or her role by City staff as a result of their work on Council or its committees or by a constituent or member of the public.

Councillors who have access to City records containing personal or other confidential information have a responsibility to protect this information while it is in their possession. Councillors must ensure that the privacy of the individual's personal information is protected at all times and kept physically secure to avoid unauthorized access or destruction.

Councillors are accountable for how their staff handle confidential information. It is recommended that Councillors emphasize to their staff the need to handle confidential information responsibly.

### **2.2 CONFIDENTIAL COUNCIL REPORTS**

Councillors are provided with confidential information when decisions need to be made at closed meetings of Council or one of its committees (for example, decisions relating to employment matters, legal advice, or details of ongoing negotiations or transactions). There are normally only a small percentage of confidential agenda items that are discussed in closed sessions. As noted above, Councillors must be authorized by law or the express authorization of Council to release confidential information in any form.

### **2.3 PERSONAL INFORMATION**

Personal information supplied by a constituent to deal with a specific matter should not be used for other unrelated purposes. For example, if an individual asks to be included on a distribution list about a particular issue, that individual should not be identified with the issue in a newsletter without their permission. Councillors should not disclose the constituent's personal information to others without the constituent's consent either.

Access and privacy training for Councillors and their staff is available on request by contacting the Executive Director, Corporate Information Management Services.

### **2.4 THE INTEGRITY COMMISSIONER**

Complaints citing failure to observe the *Code of Conduct* or a breach of privacy are periodically filed by members of the public against Councillors. The Integrity Commissioner investigates these complaints. If the Commissioner concludes that a violation did occur, the Integrity Commissioner may recommend to Council that a reprimand be administered.

The compliance section of the *Code of Conduct* provides additionally for penalties that include:

- Suspension for a period of up to 90 days;
- Removal from membership of a Committee or local board (restricted definition);
- Removal as Chair of a Committee or local board (restricted definition);
- Repayment or reimbursement of moneys received;
- Return of property or reimbursement of its value;
- A request for an apology to Council, the complainant, or both.

### 2.5 THE INFORMATION AND PRIVACY COMMISSIONER/ONTARIO

The Information and Privacy Commissioner (IPC) may investigate a privacy complaint made against a Member of Council when the complaint relates to City records.

Examples of privacy breaches include the following:

- disclosing personal information to a third party or in a public meeting without the individual's consent;
- misdirected mailings or release of e-mails involving personal information;
- insecure disposal of documents containing personal information, e.g. in a blue bin instead of shredding;
- stolen/lost laptops or other devices that contain unencrypted personal information.

This Guide was created on the basis of recommendations of the IPC following the investigation of a privacy complaint against the City of Toronto in 2006. (See "Privacy Complaint Report, Privacy Complaint No. MC-050018-1,"

<http://www.ipc.on.ca/English/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=7053>)

## 3. Managing information in a Councillor's Office

3.1 Risks of mishandling information are reduced if steps are taken to manage that information appropriately. Information in Councillors' offices normally includes records pertaining both to constituency, e.g., email from constituents, and the City, e.g., committee minutes. It makes sense to administer both kinds of records in ways that help Councillors and their staff protect confidential and personal information.

Keeping the two categories of records – constituency and City – separate will help ensure that the information in each is handled appropriately. Asking the question: "For what purpose was this information given to me?" can help clarify whether information relates to City or constituency business.

### 3.2 MANAGING CITY INFORMATION

Documents and records created in connection with City business, e.g., a schedule of meetings or meeting agendas, are considered City records. Records related to the Councillor's responsibilities as a Member of Council or to some aspect of City Council's mandate, e.g. as a member of a standing committee or special task force, are subject to

the provisions of MFIPPA. It is recommended that Councillors ensure that copies of these records are held by the relevant business division(s). City business divisions are responsible for the records of decisions and plans to ensure the effective, ongoing operation of the City.

The Mayor, as Head of Council and Chief Executive Officer, is an officer of the City. The Mayor's records that relate to mayoral duties, as opposed to a councillor's constituency or personal papers, are considered to be in the City's custody or control and therefore subject to *MFIPPA*.

### 3.3 MANAGING CONSTITUENCY INFORMATION

Documents and records received or created interacting with constituents are considered personal. Constituency records generally relate to issues the Councillor is dealing with involving one or more members of the public who either live or own a business within the Councillor's ward. Constituency records may include letters, emails, faxes, telephone messages, and mailing lists.

Constituency information is not subject to *MFIPPA*. The IPC has confirmed that, except in unusual circumstances, a Councillor is not an officer or employee of the City. Councillors' constituency liaison records are considered "personal" and are not subject to *MFIPPA*. Accordingly, under *MFIPPA*, a person generally does not have a right to access a Councillor's constituency records.

### 3.4 PROTECTING PERSONAL AND CONFIDENTIAL INFORMATION

Documents containing confidential or personal information should be stored in locked cabinets except when in active use. Data stored on laptop computers, USB drives or similar devices should be encrypted or otherwise password protected. Documents and devices should not be left unattended in vehicles or in other offices.

Care should be taken to ensure that personal information is not disclosed during public meetings without prior, written consent of the affected individual(s).

### 3.5 THE CITY CLERK'S OFFICE

Council has delegated responsibility for overseeing the administration of *MFIPPA* to the City Clerk. The City Clerk's Office also has overall responsibility for setting standards, policies, implementing effective procedures and tools for the management of City information, and providing training to City staff for the efficient and effective management of City information.

## 4. Glossary of Terms

**ACCESS TO INFORMATION (principle):** information should be available to the public. Necessary exemptions from the right of access should be limited and specific.

**CITY RECORDS:** Documents and information received or created by City officials and employees in the operation of the City and delivery of services to the public.

**CONSTITUENCY RECORDS:** Documents and information received or created by Councillors, including their staff, that relate to matters dealing with their constituents.

**CONFIDENTIAL INFORMATION:** includes information in the possession of or received in confidence by the City.

MFIPPA restricts or prohibits disclosure of information based on defined exemptions, for example, trade secrets, law enforcement investigations, financial or commercial information received from third parties in confidence, personal information, and legal matters. The *City of Toronto Act, 2006* allows information that concerns personnel, labour relations, litigation, property acquisitions, or security to be discussed in closed meetings of Council or Committee.

**INFORMATION AND PRIVACY COMMISSIONER (IPC):** The IPC is a provincial officer independent of the Ontario (and municipal) government charged with upholding and promoting open government and the protection of personal privacy in Ontario.

**INTEGRITY COMMISSIONER:** The Integrity Commissioner is a municipal officer independent of the City administration charged with

- providing advice and education to Members of Council and members of City Boards to assist in maintaining a high standard of ethical behaviour in City government;
- investigating complaints (formal or informal) about the conduct of Members of Council and members of City Boards to determine whether the City's Code of Conduct has been violated.

**MFIPPA:** The *Municipal Freedom of Information and Protection of Privacy Act* (Ontario).

**OPEN DATA:** City information provided for free and online that can be downloaded and used by anyone. This data is vetted prior to being opened to ensure that confidential information is removed.

**PERSONAL INFORMATION:** is information about an identifiable individual, such as (but not limited to) address, race, religion, gender, family status, employment history, medical history, any identifying number assigned to the individual, personal opinions or views of an individual about another individual, and correspondence of a private or confidential nature from an individual.

Information about a person in an official, business or employment capacity is not considered personal.

**PRIVACY BREACH:** A privacy breach occurs when personal information is collected, used, disclosed or destroyed in ways that are not in accordance with privacy legislation.

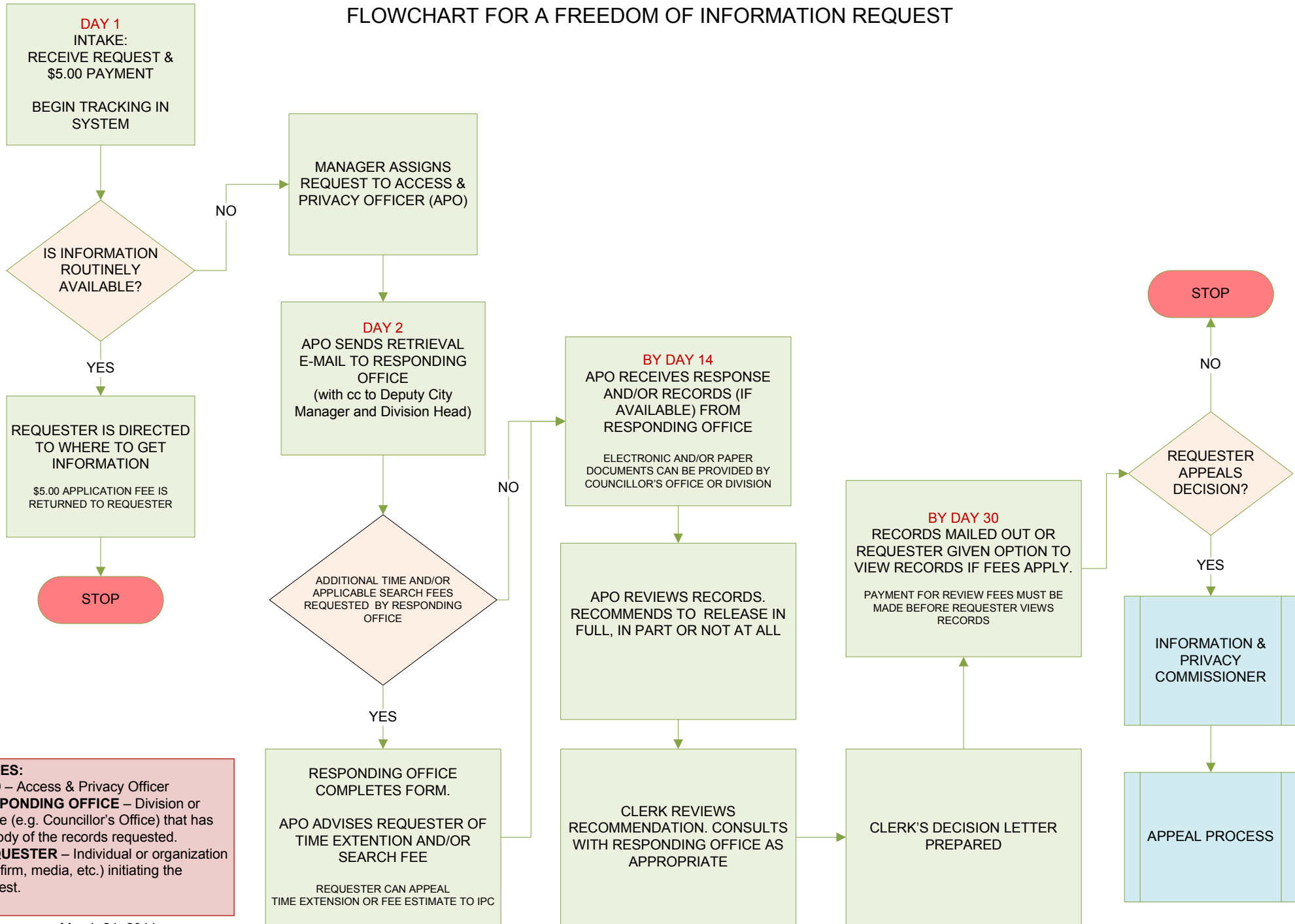
**PRIVACY PROTECTION (principle):** Governments have an obligation to protect the privacy of individuals with respect to personal information about themselves held by government. This includes controls over the collection, use, disclosure, and security of that information and a duty to provide individuals with a right of access to their own personal information.

**PROACTIVE DISCLOSURE:** This refers to City divisions actively making records and information available to the public, e.g., by posting on the City's website or making the information available on request, without requiring any sort of official review prior to release.

### **Appendix A: Process diagrams**

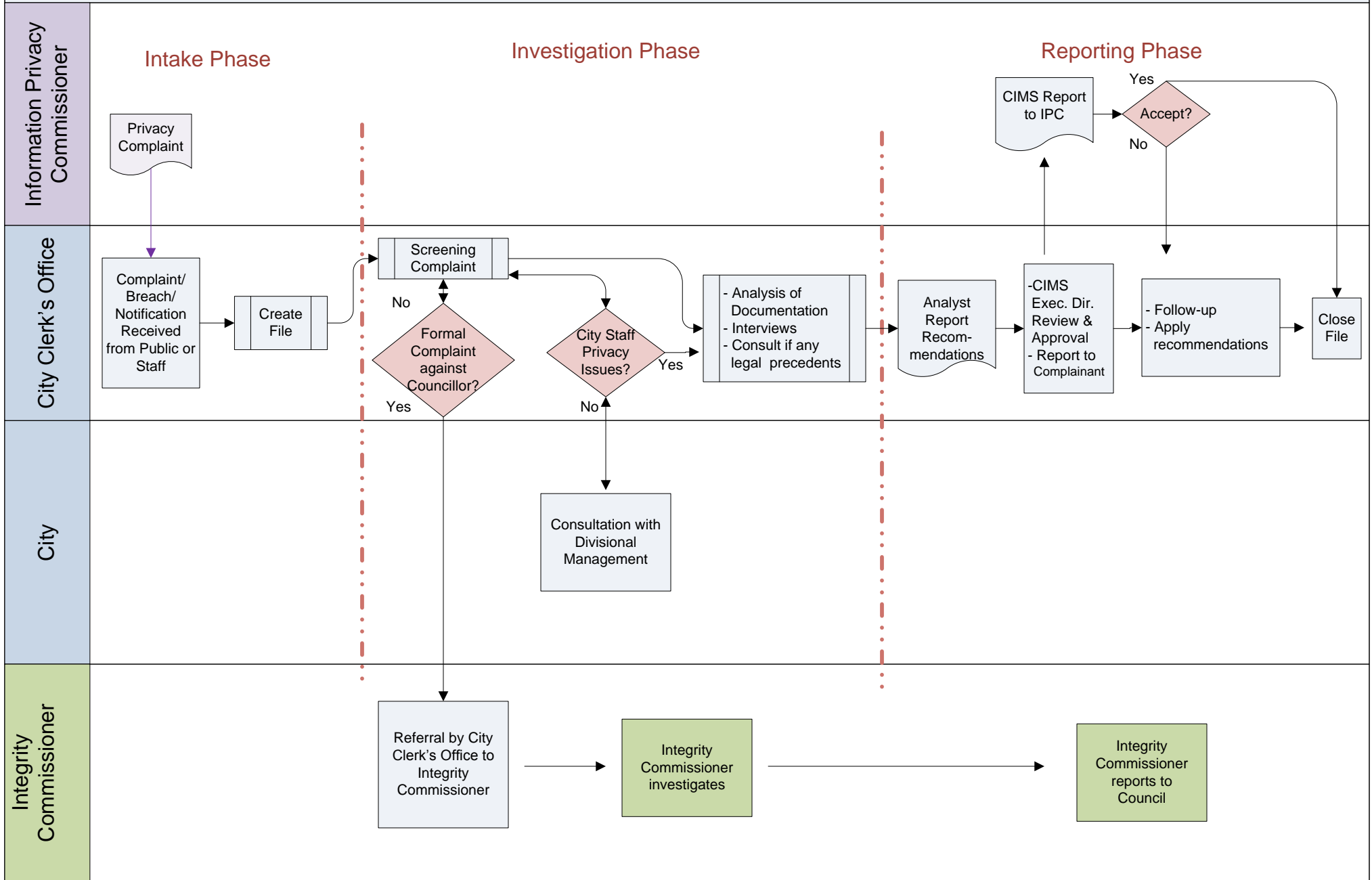
- Access requests
- Privacy investigations
- Appeals

# ACCESS AND PRIVACY FLOWCHART FOR A FREEDOM OF INFORMATION REQUEST

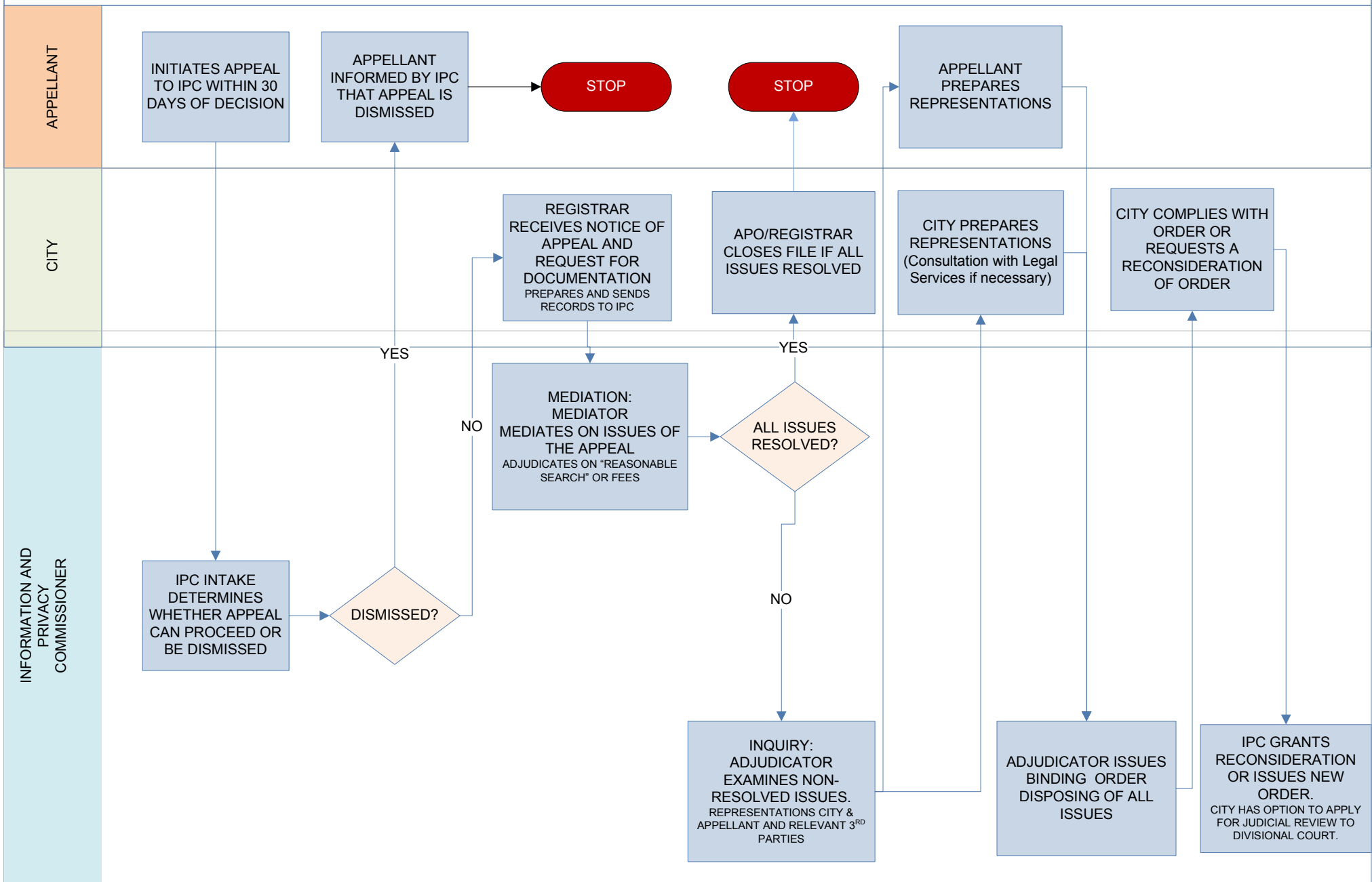


**NOTES:**  
**APO** – Access & Privacy Officer  
**RESPONDING OFFICE** – Division or Office (e.g. Councillor's Office) that has custody of the records requested.  
**REQUESTER** – Individual or organization (law firm, media, etc.) initiating the request.

# Privacy Complaint Management Process



# Appeals to the Information and Privacy Commissioner (IPC)



## NOTES:

1. IPC has three main stages of the Appeal Process – Intake, Mediation and Adjudication (Inquiry).
2. Depending on the nature of the appeal, an order disposing of the issues may be issued at any one of these stages – e.g. Special Appeals and Reasonable Search Appeals may be settled at the Mediation Stage. Similarly, the IPC Registrar or Intake Analyst may dismiss an appeal that is not within the IPC's jurisdiction.
3. The Inquiry Process involves the drafting and submission of representations, often in consultation with Legal Services and taking into consideration any relevant third-party representations.
4. Judicial Review is the process whereby "IPC decisions in access appeals can only be challenged on limited grounds using a special type of court proceeding called "judicial review."