What you need to know when
Collecting Personal Information Fact Sheet

All City of Toronto staff have legal obligations when collecting personal information from the public. This fact sheet defines personal information and outlines City staff's responsibilities when collecting personal information.

What is Personal Information?

Personal information is defined in the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) as recorded information about an identifiable individual.

Personal information is information about individuals in a personal capacity. Information about an individual's business, official, or professional capacity is not personal information. Personal information includes:

- The name and address of an individual who completed an application requesting a City service;
- A City employee's medical or banking information;
- Pedestrian traffic captured on video from City street cameras, or;
- The name and opinion of an individual who completed a survey about a City planning issue.

Personal information does not include:

- The name and contact information of a third party vendor working with the City;
- Information about City staff in their professional capacity, or;
- Contact information for a volunteer with a City division.

Municipal Freedom of Information & Protection of Privacy Act, R.S.O. 1990, c. M.56, s. 2 (2)

Can I Collect Personal Information?

City staff may collect personal information through a number of methods (e.g. paper or electronic forms, surveys, sign-up sheets, social media, web applications, registration systems).

Staff must ensure that there is a City by-law or legal statute that gives the division the authority to collect personal information for a specific stated purpose, e.g. to issue a swim pass, conduct a survey, or provide shelter services.

Municipal Freedom of Information & Protection of Privacy Act, R.S.O. 1990, c. M.56, s. 28

How Do I Share Data?

Divisions that collect or share personal information with a third party (e.g. a Provincial Ministry, hired consultants, or community partners) must enter into a data sharing agreement. It must ensure that:

- The collection and sharing of personal information is compliant with MFIPPA, and,
- The combination of two or more data sets does not re-identify an individual.

How Do I Collect Personal Information?

The City is obligated by law to inform individuals of the purpose for collecting personal information through a "Notice of Collection" statement. This notice must include three elements:

- A citation of the legal authority to collect the information;
- The specific purpose for collecting the personal information, and;
- Contact information of a staff member who can answer questions about the collection.

Municipal Freedom of Information & Protection of Privacy Act, R.S.O. 1990, c. M.56, s. 29 (2), and Reg. 823, s.4

What you need to know when
Collecting Personal Information Fact Sheet

Do I Have to Collect Personal Information Directly from the Individual?

Yes, not from third party sources, such as social media sources or websites. There are some exceptions, for example:

- The individual has delegated their authority to a legal representative, (e.g. a lawyer or through a power of attorney);
- The information is collected as part of a law enforcement investigation,(e.g. a property complaint filed with Municipal Licensing & Standards);
- The information is collected to determine if someone is eligible for an award, or;
- If a statute permits another method of collection. (e.g. The Municipal Elections Act permits the collection of property owners' information for the voters list from the Municipal Property Assessment Corporation)

Municipal Freedom of Information & Protection of Privacy Act, R.S.O. 1990, c. M.56, s. 29 (1)

Who Can Help Me?

The City Clerk's Office reviews personal information collection methods e.g. forms, surveys, telephone, or over-the-counter registration with divisions. This review ensures compliance with legislation, corporate identity standards, and the Accessibility for Ontarians with Disabilities Act (AODA).

What Are Some Best Practices?

Divisions are responsible for ensuring personal information is protected from unauthorized access, use, destruction, or disclosure including:

- Building Privacy by Design into new business processes and technology systems;
- Conducting a Privacy Impact Assessment on new technology to protect privacy and security, and;
- Implementing physical access and security measures to prevent the disclosure of sensitive information to unauthorized individuals.

Questions? Need more Information?

- Privacy and Confidentiality online resources and training
- Consult a privacy expert: privacy@toronto.ca.