Protection of Privacy Policy

Policy No. CIMS-006
Version No. 1.0
Approval Date: July 21, 2014

City Clerk's Office

TORONTO

An Information Management Policy

Subject:	**Protection of Privacy Policy**	**Policy No: CIMS-006** **Version No: 1.0**
Keywords:	Information management, privacy, breach, personal, information, data, accessibility, open government, principles, accountability, transparency, records, documents, framework, audit, divisional operations, MFIPPA, PHIPA, privacy, security, responsibility, collection notice.	**Effective:**
Issued by:	City Clerk's Office	**Issued on:** July 21, 2014

Supersedes:

Contact Information:

Deputy City Clerk, Corporate Information Management Services, City Clerk's Office

Tel: (416) 392-9673

13WT City Hall
100 Queen St. W,
Toronto, Ontario M5H 2N2

Revision History:

Version #	Version Date	Issued by	Changes in Document
1.0	2014-07-21	City Clerk's Office	Publication of version 1
1.0	2019-08-22	City Clerk's Office	Application Statement updated

TORONTO

Table of Contents

Foreword

City of Toronto Information Management Policies and Standards are the official publications on the policies, standards, directives, guidelines, technical reports and preferred practices endorsed by the Open Government Committee under delegated authority of the City Manager's Office. These publications support the City's responsibilities for coordinating standardization of Information Management in the City of Toronto. Publications that set new or revised policies or standards provide guidance and administrative information for their implementation. In particular, they describe where the application of a policy or standard is mandatory and specify any qualifications governing its implementation.

1. Introduction

Privacy plays a key role in a free, democratic society and is an essential element in maintaining public trust in government. The City of Toronto is committed to protecting the privacy of individuals, and will ensure that privacy protection continues to play a key role in an open, accessible and transparent government.

This Policy supports the City's effort with Open Government. Open Government is about improving the delivery of services and supporting initiatives that build trust and confidence in government. It is guided by four overarching principles of **transparency, participation, accountability and accessibility**.

The City maintains an Information Management Framework (IMF) that identifies its core information management principles and objectives. The IMF acts as a driver for, and supports the development of Information Management (IM) policies, standards, and directives, and is structured to align with Council priorities for a more accountable and accessible City. The Protection of Privacy Policy is an output of the Framework's Accountability Principle that sets the requirements for privacy protection and the public service responsibility for safeguarding personal information.

Personal information means recorded information about an identifiable individual.

Examples of personal information are:

- home address, personal email address, home phone number, identification numbers e.g. Social Insurance Number
- personal emails, forms or correspondence between the individual and the City
- ethnic origin, religion, age, gender, sexual orientation, marital status
- educational, medical, criminal or employment history, or personal financial transactions
- the individual's name when connected to any of the above

To qualify as personal information:

- it must be about an individual in a personal capacity;

- it is reasonable to expect an individual may be identified if the information is disclosed.

As a general rule, information associated with an individual in a professional, business or official capacity is not personal information.

The Protection of Privacy Policy is also an output of the City's Information Management Accountability Policy that highlights requirements to properly manage information and safeguard the protection of personal information.

This Policy includes a Protection of Privacy Framework. Refer to Appendix I. The Framework supports the Policy by establishing five easily communicated strategic objectives in accordance with established privacy law and best practices. The Framework should be used as a tool to help users understand and be aware of the protection of privacy requirements in the City of Toronto.

The City is legislatively obligated to protect personal information under the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), and the Personal Health Information Protection Act (PHIPA). Other legislation may also create obligations with respect to the protection of information or records held by the City.

2. Purpose

The purpose of this policy is to foster greater public trust by establishing clear accountability statements, including roles and responsibilities, for the protection of personal information collected, used, disclosed and disposed by the City of Toronto.

3. Application

This Policy applies to all City of Toronto Divisions, City employees, volunteers and contract employees hired by the City of Toronto.

This Policy applies to all personal information including personal health information managed by the City and is not limited by the scope of any individual statute or regulation with the exception of personal health information administered by Toronto Public Health.

The use of personal and confidential information by elected officials is governed by the Code of Conduct for Members of Council. Complaints regarding the misuse by elected officials of such information are investigated by the Integrity Commissioner. Guidance for elected officials on privacy protection is available in the Councillor's Guide to Access and Privacy Legislation.

The City's Accountability Officers include the Auditor General, Integrity Commissioner, the Lobbyist Registrar and the Ombudsman. The Officers report to and are directly accountable to City Council. The *City of Toronto Act, 2006* requires that the Officers perform their duties in an independent manner and establishes confidentiality requirements of their information. These confidentiality requirements are recognized in Toronto Municipal Code Chapter 3, Accountability Officers, and the City's *Protection of Accountability Officers' Information Directive* developed to safeguard the confidentiality of the Officers' records. In the event of a privacy

breach related to any of the Accountability Officers, the City would seek guidance of the Information and Privacy Commissioner of Ontario.

Most City agencies and corporations are separate institutions under MFIPPA and have their own designated Head for privacy matters. The City of Toronto encourages City Agencies and Corporations to review, adopt or update this Policy appropriate to their business circumstances.

4. Policy Statement

The City of Toronto will:

a. Ensure all employees share responsibility for the protection of personal information privacy and compliance with the roles and responsibilities identified in this Policy;

b. Plan for and ensure that privacy protection requirements are embedded in the design of all City programs, processes, projects and technology architecture.

c. Establish and communicate a set of privacy standards and guidelines to improve the protection of personal information by identifying, investigating, assessing, monitoring and mitigating personal information privacy risks in City programs and activities involving the collection, use, disclosure and disposal of personal information.

d. Apply this policy and related policies and practices in the collection, use, disclosure, and disposal of personal information;

e. Clearly communicate to the public how personal information is collected, used, disclosed and disposed.

f. Make privacy training mandatory, commensurate with their job responsibilities, for all City staff, volunteers and contract staff hired by the City of Toronto;

g. Establish a learning plan to improve employee privacy awareness commensurate with the complexity and sensitivity of the information to which they have access.

5. Organizational Outcomes

It is expected that by complying with this policy the City will:

a. Increase trust and confidence in Toronto's government;

b. Ensure statutory and regulatory compliance with and effective application of privacy legislation;

c. Establish rules and procedures for managing privacy investigations and other privacy matters;

d. Communicate and identify roles and responsibilities for City staff, volunteers and contracted staff related to the management of personal information; and

e. Integrate Privacy by Design principles into all new or modified programs, technologies and activities that involve the use of personal information.

6. Roles and Responsibilities

City Manager will:

a. Provide oversight of and compliance with this Policy and Framework by all City staff;

Deputy City Managers will:

b. Administer and communicate this Policy and Framework broadly to all staff within their Cluster;

c. Integrate protection of personal privacy requirements into the development, implementation, evaluation, and reporting activities of divisional programs and services within their cluster;

d. Promote a culture and business practices that ensure City information is shared and accessible to the greatest extent possible, while respecting security and privacy requirements of personal information and other confidentiality obligations;

City Clerk will:

e. Develop and implement policies, programs and services for management and protection of personal information based on Privacy by Design principles;

f. In partnership with City Divisions implement this policy;

g. Review divisional practices for the collection, use, disclosure and disposition of personal information;

h. Consult with business programs to meet privacy requirements as identified in this Policy, applicable legislation, privacy standards and procedures;

i. Establish privacy standards, guidelines and procedures to support this Policy and Framework;

j. Coordinate the response to complaints regarding the misuse of personal information;

k. Investigate reports of privacy breaches and communicate findings to complainant;

l. Authorize sign-off of the Privacy Impact Assessment report prior to implementation of any technology, system, program or service involving the collection or use of personal information or personal health information;

m. Execute recommendations identified in Privacy Impact Assessment reports;

n. Request from the CIO a certificate of assurance for all Threat Risk Assessments and Vulnerability Assessments on any technological system that collects or uses personal information or personal health information;

Executive Director, Human Resources will:

o. In partnership with the City Clerk establish a training and education plan, including the development of e-learning modules, to improve privacy awareness in the City of Toronto;

p. Build privacy awareness and training into all new staff orientation programs;

Chief Information Officer will:

q. Implement Privacy by Design principles in Enterprise Architecture, information technology policies, standards, procedures and technologies;

r. Create personal information privacy and security standards for technologies that will ensure adequate safeguards and compliance for those technologies or technological processes that collect, use, disclose or retain personal information;

s. Conduct Risk Assessments (Privacy Impact Assessments, Threat Risk Assessments, and Vulnerability Assessments) on all technological systems involving the collection or use of personal information prior to implementation or deployment;

t. Authorize sign-off of the Privacy Impact Assessment report prior to implementation of any technology, system, program or service involving the collection or use of personal information or personal health information; and;

u. Execute recommendations identified in Privacy Impact Assessment reports;

v. Provide to the City Clerk a certificate of assurance for all Threat Risk Assessments and Vulnerability Assessments on any technological system that collects or uses personal information or personal health information;

Division Heads will:

w. Be accountable for ensuring personal information is collected, used, disclosed and disposed in accordance with legislation and associated regulations, standards and other City policies, and for compliance with this policy;

x. Implement this Policy and Framework and communicate to staff under their direction;

y. Report out on their privacy protection activities via their annual Division Information Management Plans;

z. Receive formal privacy investigation reports and make final decisions about the disposition of a complaint;

aa. Restrict access to personal information to those individuals who require access to personal information in order to perform their duties and where access is necessary for the administration of their business;

bb. Maintain personal information and develop, and implement processes whereby individuals can view information held about them and what the City uses it for. These processes will also facilitate individuals needing to correct or update their information;

cc. In collaboration with City Clerk, the CIO, Director, Purchasing and Materials Management, and the City Manager require vendors and contractors comply with this policy and that privacy rules and concerns are referenced in all procurement documents;

dd. Require staff, vendors and contractors maintain a level of privacy awareness appropriate with their responsibilities;

ee. Inform staff of the legal and administrative consequences of any inappropriate or unauthorized access to, or collection, use, disclosure, or disposition of, personal information related to a particular program or activity;

ff. Consult with the City Clerk and the CIO during the planning stages, before any procurement, and prior to implementation of any technology, system, program or service involving the collection, use, disclosure or disposition of personal information or personal health information, by:

i. Jointly with the City Clerk and CIO, authorizing sign-off of the Privacy Impact Assessment report;
ii. Executing recommendations identified in Privacy Impact Assessment reports;
iii. Completing Threat Risk Assessments and Vulnerability Assessments and implement recommendations on any technological system that

collects or uses personal information or personal health information.

All Employees and Volunteers will:

gg. Manage personal information that is part of a business record in accordance with the City's Responsible Record Keeping Directive and the requirements identified in this Policy;

hh. Take privacy awareness and training for the appropriate handling of personal information to understand their responsibilities to protect privacy in executing their operational duties;

ii. Be responsible for the privacy of City of Toronto business information regardless of whether the technology used to manage the information is personally owned or City owned;

jj. Be aware of their privacy responsibilities noted in the City's Acceptable Use Policy;

kk. Be aware of their privacy responsibilities noted in the City's Video Surveillance Policy;

ll. Follow specific procedures established for disclosing personal information to a law enforcement agency in Canada;

mm. Comply with applicable legislation that governs the collection, use, disclosure and disposition of the personal information under their control.

7. Definitions

Collection
The collection of personal information from or about the individual to whom the information relates including unintended or unprompted receipt.

Disclosure
The release of personal information by any method (e.g., sharing information by any means such as verbally, sending an email, posting online) to anybody or person.

Disposition
The action taken with regards to personal information including destruction, transfer to another entity, or permanent preservation.

Information Management
The means, by which the City of Toronto responsibly plans, creates, capture, organizes, protects, uses, controls, shares, disposes of, and evaluates its

information, and through which it ensures that the value of that information is identified, trusted and used to the fullest extent.

Personal information
Personal information is recorded information about an identifiable individual ". Refer to section 2 (1) of MFIPPA for additional information.
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm

Personal Health Information
Personal health information is identifying information about an individual that relates to their health or providing health care to the individual. Refer to section 4 PHIPA for additional information:
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm#BK5

Privacy by Design
To build privacy and data protection, into the design specifications and architecture of information and communication systems and technologies at the beginning, in order to facilitate compliance with privacy and data protection principles.
http://www.privacybydesign.ca/

Privacy breach
The improper or unauthorized creation, collection, use, disclosure, retention or disposition of personal information.

Privacy Impact Assessment (PIA)
The PIA is a process for identifying, assessing and mitigating privacy risks. The City of Toronto develops and maintains privacy impact assessments for all new or modified programs and activities that involve the use of personal information or personal health information for an administrative or operational purpose.
http://www1.toronto.ca/City%20Of%20Toronto/City%20Clerks/Corporate%20Information%20Management%20Services/Files/pdf/P/PIA-Policy.pdf

Threat Risk Assessment (TRA)
The TRA is the process for identifying the threats to confidentiality, integrity, or availability of Information Technology (IT) assets, assessing current vulnerabilities for each IT assets based on existing or proposed controls, analysing and quantifying the risk levels for the vulnerable IT assets, and providing recommendations to lower the risks to acceptable level.

Use
The purpose(s) for which the information was obtained or compiled.

Vulnerability Assessment (VA)
The VA is the process for identifying potential system level or technical weaknesses in the Information Technology (IT) system that could be exploited to compromise the

confidentiality, integrity and availability of IT assets, analysing and quantifying the risk levels for each vulnerability identified, and providing recommendations to mitigate the risks to acceptable level.

8. Compliance

All City staff, volunteers, and contract staff hired by the City of Toronto are responsible for complying with this Policy.

9. Policy Approval

Joseph P. Pennachetti
City Manager

Signature _____ Date: July 21, 2014

10. Policy Review

This policy is reviewed regularly.
Approval follows the process in effect at the time of review.

11. Authority

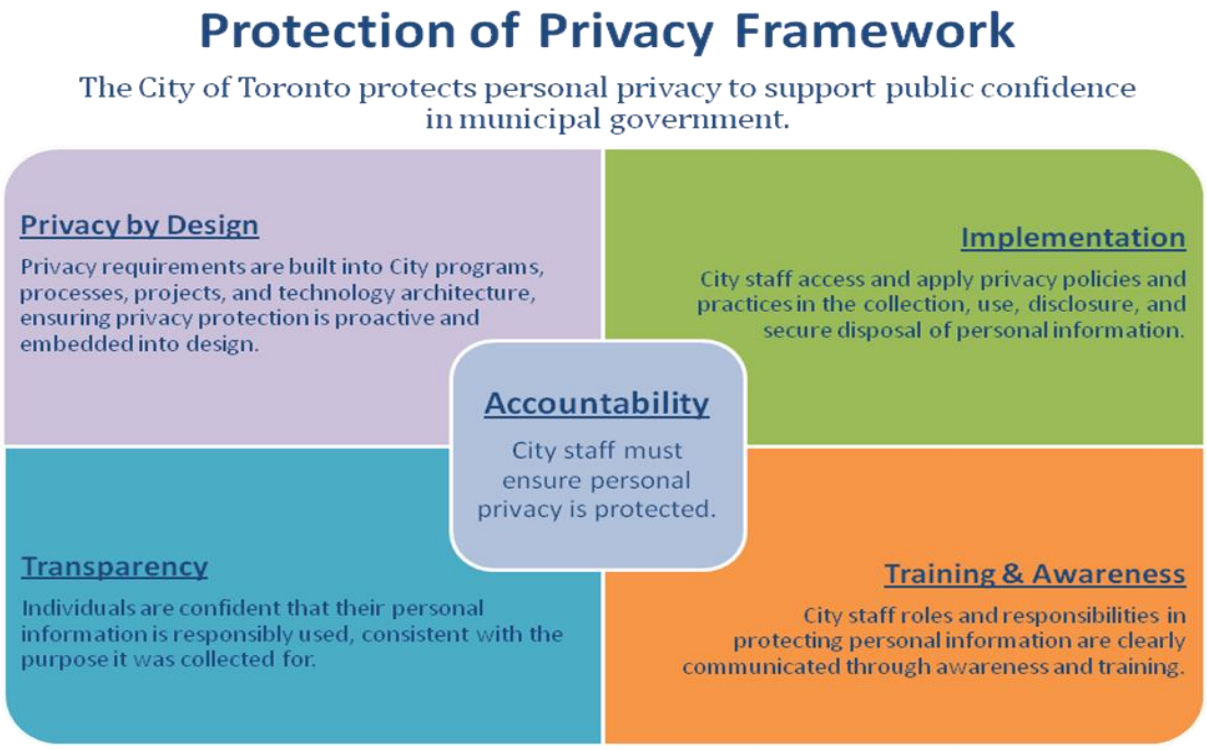
1. *City of Toronto Act, 2006*

12. References

1. Corporate Information Management Services Mandate, August 17, 2010
2. Municipal Code, Chapters 169 & 217
3. *Municipal Freedom of Information and Protection of Privacy Act, 1990*
4. *Personal Health Information Protection Act, 2004*
5. *Privacy Impact Assessment Policy, 2013*

13. Appendix I: Protection of Privacy Framework

This Policy includes a Protection of Privacy Framework that supports the Policy by establishing five easily communicated strategic objectives in accordance with established privacy law and best practices. The five strategic objectives are: Accountability, Privacy by Design, Implementation, Transparency; and, Training and Awareness.This framework should be used as a tool to help users understand privacy requirements in the City of Toronto.



Examples of how the Framework is used day-to-day:

Privacy by Design: Privacy impact assessments must be conducted on all new technology.

Transparency: Individuals are advised on all City forms how their personal information will be used, and receive a full response to any privacy concerns they may have.

Implementation: The daily application of formal privacy practices and processes as required by MFIPPA, PHIPA and other privacy legislation to foster a culture of accountability and trust.

Training & Awareness: Mandatory privacy training, commensurate with job responsibilities, for all City staff whose progress is monitored and reported annually by Division Heads.