OPERATIONAL POLICY

Policy Title:	Applies to:		Reference #
Privacy	All employees and contractors		**2015-OCCOP-P0001**
Approved by:	**Dates:**		**Total # of Pages**
Executive Leadership Team	**Effective:**	01-May-2015	6
	Last Review:	01-June-2018	
	Next Review:	01-June-2020	
Authority:			
The Local Authority Freedom of Information and Protection of Privacy Act			
Responsibility:			
Corporate Information Governance, Office of the City Clerk			

1.0 Purpose

The City of Regina (the "City") is committed to protecting personal information in its possession or under its control. Personal information is handled in accordance with *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).

The purpose of this policy is to establish appropriate controls around the collection, use and disclosure of personal information as required to carry out the City's legitimate business and public interest mandates, in accordance with LA FOIP.

2.0 Scope

This policy applies to all City employees and contractors who collect, access, use, process, store, modify, share, disclose and/or destroy personal information in the possession, or under the control, of the City of Regina.

3.0 Definitions

Access and Privacy Team – includes Privacy & Freedom of Information Officers located in Corporate Information Governance, Office of the City Clerk.

Authority – the legal authority to collect, use or disclose personal information derived from *The Local Authority Freedom of Information and Protection of Privacy Act*, a bylaw, other legislation or policy.

Collection – the gathering of personal information for an existing or proposed City program.

Confidentiality – indicates that certain information will be kept private or shared with only certain parties for certain purposes.

Confidential Information – information that is meant to be kept private or shared with only certain parties for certain purposes. Confidential information may include personal information and information of a sensitive nature which may be, but is not limited to, third party/proprietary/commercial information.

Consent – the agreement of an individual for the collection, use or disclosure of their personal information.

Contractor – an individual or company retained under contract to perform services for the City.

Disclosure – when personal, confidential or third party information is made available or released.

Duty to Protect – means the City's obligation to protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control.

Employee – an individual employed by the City, including an individual retained under a contract to perform services for the City.

Information – what a record contains. It is also a term used to refer to the content of an electronic database or application. Regardless of the form, all recorded information in the possession or under the control of the City is a record.

Information Management Service Provider – means a person or body that processes, stores, retains or destroys records of a local authority containing personal or confidential information or provides information management or information technology services to a local authority.

Initiative – is a standard term used to represent, but which is not limited to, a program, project, service, application or software upgrade.

LA FOIP – *The Local Authority Freedom of Information and Protection of Privacy Act*.

Personal Information – means recorded information about an identifiable individual which may include but is not limited to: information about an individual's race; religion; family status; age; birthdate; place of origin; employment or criminal history; financial information; health services number; driver's license number; social insurance number; home address, email address or telephone number; physical or mental condition of an individual; an individual's personal views or opinions except where they are about another individual.

Privacy – is the right to keep certain information private; freedom from unauthorized access to, use, or disclosure of one's personal/confidential information.

Privacy Breach – occurs when there is, unauthorized access to, use or disclosure of personal/confidential information. Such activity is unauthorized if it occurs in contravention of *The Local Authority Freedom of Information and Protection of Privacy Act.*

Privacy Assessment – is a tool used to review privacy risks, associated with collecting, accessing, using, processing, storing, modifying, sharing, disclosing and/or destroying personal/confidential information, typically undertaken during the initial or conceptual stage of an initiative. It consists of two parts: Part 1: Privacy Quick Assessment, Part 2: Privacy Impact Assessment.

Privacy Impact Assessment – is a detailed diagnostic tool used to identify and resolve privacy risks inherent to initiatives undertaken by the City.

Privacy Quick Assessment – is a preliminary diagnostic tool used to determine whether or not a particular initiative has or will have privacy concerns that need to be reviewed in more detail through a Privacy Impact Assessment.

Record – means a record of information in any form and includes information that is written, photographed, recorded, digitized or stored in any manner, but does not include computer programs or other mechanisms that produce records.

Third Party – means a person or company other than the City.

Use – when personal information collected by the City is used for any purpose.

4.0 Policy

LA FOIP is the primary legislation governing the City of Regina with respect to the protection of personal information in the City's possession or under its control. Other legislation may also authorize the collection, use or disclosure of information.

4.1 Privacy Protection

The City has a duty to protect the integrity, accuracy and confidentiality of personal information in its possession or under its control, as outlined in Section 23.1 of LA FOIP.

The City is authorized to, and may, enter into third party agreements that involve the sharing of personal information.

Every employee or contractor who collects, accesses, uses, processes, stores, modifies, shares, discloses and/or destroys personal information as a result of employment or contract with the City is:

- Required to sign and abide by any relevant City of Regina confidentiality agreements.
- Responsible for managing personal/confidential information in accordance with those agreements, this policy and related procedures and guidelines.
- Responsible for proactively incorporating privacy protection into all corporate initiatives.

Every City employee is responsible for safeguarding the privacy, confidentiality and security of information in the workplace and when working remotely.

4.1.1 Information Management Service Provider

Before disclosing personal information to an information management service provider, the City is required under Section 23.2 of LA FOIP to enter into a written agreement that meets the requirements of the Act and Regulations.

4.2 Purpose

Any personal information collected by or for the City must be collected for an identified business purpose. This purpose must be identified at or before the time of collection.

4.3 Consent

Appropriate consent or authority from LA FOIP is required to collect, use or disclose personal information.

Consent must be obtained directly from the individual to whom the information relates, where reasonably practicable to do so. In cases where gaining consent from the individual may not be feasible, appropriate or the only lawful means, the authority for collection must be derived from LA FOIP, a bylaw, other legislation or policy.

Obtaining informed consent is best practice, meaning that the individual is aware of and understands the purpose for the collection and how the information will be used or disclosed.

4.4 Collection

When collecting personal information, only collect the information necessary to perform the identified task or function.

4.5 Use and Disclosure

Personal information must only be used or disclosed for the purposes for which it was collected, or for a use that is consistent with that purpose; with the consent of the individual; or when collection, use or disclosure is authorized by legislation.

4.6 Retention

Personal information must be retained only as long as necessary for the fulfillment of its stated collection purpose, or as specified by law. When the retention requirements have been met appropriate steps must be taken to safely and securely dispose of the records.

4.7 Accuracy

Reasonable efforts must be made to ensure that the personal information used by the City for an administrative purpose is accurate, complete, and as up-to-date as reasonably possible.

4.8 Correction

An individual has the right to request correction of personal information as outlined in Section 31 of LA FOIP; to have a notation made if correction was requested but not made; and to be advised of the reason a request was disregarded.

4.9 Security

The City will ensure that appropriate security safeguards are in place to protect personal information. These safeguards are intended to address such concerns as appropriate access to information, breach prevention, recovery, information integrity and other potential security issues. Safeguards include physical, technical, procedural and organizational measures.

4.10 Access

With some exceptions, individuals have a right to be informed of the existence, use and disclosure of personal information pertaining to them and have the right to access their personal information upon request.

4.11 Privacy Breach

A privacy breach occurs when there is unauthorized access to, use, disclosure, or loss of personal/confidential information. Any employee or contractor who knows of, or suspects, a privacy breach must report it immediately to the Access and Privacy Team in the Office of the City Clerk and follow the privacy breach protocol:

- The breach must be contained and the unauthorized practice stopped to lessen any consequences for the individual(s) whose information was involved, as well as consequences to the City.
- Privacy breaches must be investigated and documented.
- Risk to individuals must be reviewed and notification to affected individuals should occur (when determined to be necessary) to avoid, mitigate or address harm which may come to the individual as a result of the breach.
- Safeguards must be developed and improvements made to prevent further breaches.

4.12 Ability to Challenge

An individual has the right to file a complaint regarding the handling of their information by contacting the APT or by submitting a Privacy Complaint form.

If the individual remains dissatisfied with the City's response, the individual has the right to raise their concerns with the Office of the Saskatchewan Information and Privacy Commissioner.

4.13 Privacy Assessment

A privacy assessment (PA) is a process designed to ensure compliance with the City's privacy protection responsibilities. A PA helps determine whether initiatives involving the use of personal/confidential information raise privacy risks. It measures, describes and quantifies those risks; and proposes solutions to eliminate or mitigate privacy risks to an acceptable level.

All initiatives must undergo, at a minimum, a Privacy Quick Assessment, which is an initial assessment that helps to determine whether a more detailed Privacy Impact Assessment is required.

5.0 Roles & Responsibilities

City Clerk is responsible for:

- Corporate information, including personal information at the City of Regina.

Manager of Corporate Information Governance is responsible for:

- Providing guidance with respect to this policy and ensuring this policy is maintained.

Access and Privacy Team is responsible for:

- Receiving and investigating all privacy complaints or breaches in relation to the application of this policy.
- Leading the privacy assessment process on initiatives where personal/confidential information is collected, used or disclosed.

Employees are responsible for:

- Compliance with this policy and related procedures and guidelines.

6.0 Related Forms

Privacy Complaint form

7.0 Reference Material

The Local Authority Freedom of Information and Protection of Privacy Act
Bylaw No. 2012-18 *The Records Retention and Disposal Schedules Bylaw, 2012*
Employee Privacy Guidelines #2015-OCCOP-G0001
Privacy Breach Guideline #2016-OCC-G0001
Privacy Assessment Policy #2015-OCC-P0005
Confidentiality Guideline #2017-OCC-G0001

8.0 Revision History

Date	Description of Revision	Authorized By	(Re)-Approval Required (y/n)
01-05-2015	Initial Release	ELT	No
01-05-2016	Scheduled Review	CLO & CC	Yes
01-05-2017	Review	CC	No
01-11-2017	Revision	CC	No
01-01-2018	Revision – update LA FOIP acronym	CC	No
01-06-2018	Schedule Review – LA FOIP Amendments	CC	Yes