OPERATIONAL GUIDELINE

Guidelines Title:	Applies to:		Reference #
Confidentiality	All employees and contractors		**2017-OCC-G0001**
Approved by:	**Dates:**		**Total # of Pages**
City Clerk	**Effective:**	01-Dec-2017	6
	Last Review:	01-May-2020	
	Next Review:	01-May-2022	
Authority:			
The Local Authority Freedom of Information and Protection of Privacy Act Privacy Policy # 2015-OCCOP-P0001 Access to Information Policy 2015-OCCOP-P0002			
Responsibility:			
Corporate Information Governance, Office of the City Clerk; Human Resources			

1.0 Purpose

The purpose of this guideline is to provide employees, including contractors, with an understanding of their individual responsibilities, as well as the City's collective responsibility, to protect confidential corporate information.

2.0 Scope

This guideline applies to all City employees, who handle (collect, create, use, modify, retain, store, access, transmit, discuss, share, disclose or destroy) confidential information in the possession or under the control of the City of Regina.

3.0 Definitions

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

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.

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

Disclosure – when personal information is made available or released.

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

Employer – City of Regina and employees responsible for managing the employee-employer relationships at the City of Regina.

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 – 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.

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.

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 Guideline

The City of Regina and all information in its possession or under its control is subject to *The Local Authority Freedom of Information and Protection of Privacy Act.*

Information created while an individual is employed by the City is the property of the City and not the employee.

- Employees should only have access to confidential information if there is an approved business purpose and the duties of their employment require access.
- Supervisory approval/authorization is required before access to confidential City information is granted.
- Confidential information must be protected.

4.1 Employee Responsibility

Every City employee who handles confidential corporate information, during the course of their employment or contract, is responsible to protect that information.

- Since June 1, 2015, as a condition of employment, all new hires, in scope and out of scope, are required to review and sign the Confidentiality Declaration Form as a condition of employment.
- For existing staff employed by the City prior to introduction of the Confidentiality Declaration Form, signature of the form is voluntary.

- In the absence of a signed Confidentiality Declaration Form, employees may be required to sign multiple and varied confidentiality/security forms relevant to their position to authorize them to access the City's network, software applications, databases, or various levels of confidential information.

- Penalties may be imposed for the inappropriate handling of confidential information in the possession or under the control of the City. Penalties imposed by the City may range from disciplinary action, up to and including dismissal. Penalties imposed by *The Local Authority Freedom of Information and Protection of Privacy Act* may include monetary fines and/or imprisonment.

4.2 Confidentiality Protection Tips

The following tips provide guidance for employees to ensure the protection of confidential information.

1. Review, become familiar with, and abide by the terms outlined in corporate bylaws, policies, procedures, guidelines and directives.

2. Do not collect, access, use or disclose any **confidential** City information unless for an approved City business purpose or with the consent of the City.

    - Do not collect, access, use or disclose any **personal** information unless for an approved City business purpose or with the consent of the person to whom the information relates.

    - Ensure contracts with privacy/confidentiality clauses are in place with information management service providers, vendors and/or third parties.

3. Only disclose confidential information to other employees when required for a legitimate business purpose authorized by the City.

4. Store and share confidential information in a secure manner with appropriate access restrictions and controls for both paper and electronic records.

    - Lock cabinets and limit physical access.

    - Apply screen savers, computer passwords, password protection.

    - Use encryption where warranted.

    - Use confidential shredding (not recycling or strip-shred) when disposing of confidential paper records.

5. Apply appropriate measures to protect confidential information when in transit electronically and physically.

    - Use caution when using email. Apply security controls including encryption and password protection.

- Text messaging is not a secure medium for sharing confidential information and should not be used.

- USB drives or other portable devices can easily be misplaced, lost or stolen and can contain viruses.

    - USB drives should not be used to store or transport confidential information, including personal information. If it is critical to use a USB, consider purchasing an encrypted device. At a minimum, ensure all confidential files are password protected.

    - Ensure USBs are formatted prior to use.

    - Avoid re-using USB drives.

    - Contact records@regina.ca to dispose of USBs and other portable devices in a secure manner.

- Ensure confidential paper records or unsecured electronic devices are never left unattended in personal or City vehicles.

    - In the event an electronic device is lost or stolen contact Technology & Digital Innovation immediately to lock or wipe the device.

6. Confidential records should remain in the City's office environment. If there is a legitimate need to remove them from the office environment, ensure there are adequate security provisions in place to prevent the information from getting into unauthorized hands.

7. Personal electronic devices should not be used for corporate purposes including capturing corporate audio or images, or storing confidential corporate records (e.g. photos, files, documents, texts, voicemail or email).

8. All confidential corporate paper or electronic records must remain with the corporation when an employee leaves employment with the City.

    - Copies should not be retained in paper or electronic form for personal use.

9. Employee user ID and/or passwords should not be disclosed or shared with any other employee or individual.

10. Confidential information must not be used for any personal benefit or profit.

11. Confidential information must not be shared in any public forum, at work, or outside the corporation.

    - Avoid discussing confidential corporate matters on coffee break or in hallways.

    - Do not share confidential work-related information in bars, restaurants, on social media, or at home, or with anyone inside or outside the corporation who

does not have a "need to know" (e.g. friends, family, acquaintances or colleagues).

12. Do not snoop.

    - When an employee with no "need to know" purposely chooses to seek out confidential information, that is snooping.

    - Even if an employee has legitimate, authorized access to a file or database, that access is meant to be used only for business purposes.

        - If an employee had authorized access to a file or database for a legitimate business purpose and the work duties no longer require that access, the employee should notify the supervisor to have access terminated.

    - If caught snooping, penalties may range from disciplinary action, up to and including dismissal, monetary fines and/or imprisonment, as described in 4.1.

13. Report any unauthorized handling of confidential information or potential for same, immediately to the Access and Privacy Team, Office of the City Clerk.

    - Follow the privacy breach protocol as outlined in the City's Privacy Breach Guideline.

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 guideline and ensuring this guideline is maintained.

Employees are responsible for:

- Compliance with this guideline and related policies and procedures.

6.0 Related Forms

Confidentiality Declaration form HR (0515)

7.0 Reference Material

The Local Authority Freedom of Information and Protection of Privacy Act
Privacy Policy # 2015-OCCOP-P0001
Access to Information Policy 2015-OCCOP-P0002
Privacy Breach Guideline 2016-OCC-G0001

8.0 Revision History

Date	Description of Revision	Authorized By	(Re)-Approval Required (y/n)
01-Dec-2017	Initial Release	CC	Yes
01-July-2018	Review – LA FOIP Amendments	CC	Yes
01-May-2020	Scheduled Review	CC	Yes