REGINA Infinite Horizons | City of Regina

OPERATIONAL GUIDELINE

Guideline Title:	Applies to:		Reference #
Employee Privacy	City of Regina employees and contractors		2015-OCCOP-G0001
Approved by:	**Dates:**		**Total # of Pages**
City Clerk	**Effective:**	01-May-2015	8
	Last Review:	01-Aug-2021	
	Next Review:	01-Aug-2023	
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			

1.0 Purpose

The City of Regina (the "Employer") is committed to ensuring that the personal information of its employees is protected in accordance with *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).

The employer collects personal information about its employees for hiring purposes and for providing services such as payroll, pension, benefits, and health-related services as well as to maintain records on training and education, performance, disciplinary actions and union grievances. All personal information that is collected by the City is done so in accordance with LA FOIP or other legal authority.

The purpose of this guideline is to establish appropriate controls around the handling of employee information, consistent with the fundamental principles of privacy protection, as well as to ensure that employees are aware of any limitation the employer may encounter in restricting access or sharing employee personal information.

Any questions regarding these guidelines should be directed to the Access and Privacy Team (APT) in the Office of the City Clerk.

2.0 Scope

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

3.0 Definitions

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

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.

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

Disclosure – when personal information is made available or released.

***Duty to Protect* –** 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.

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.

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

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

Private Information – information relating to an individual's private matters/non-corporate life (e.g. email, text or voice recorded correspondence to family and friends, photos of family activities, non-work calendar appointments). Note: private information may contain personal information.

Record – 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 – a person or company other than the City.
Use – when personal information collected by the City is used for any purpose.

4.0 Guideline

Employee personal information may include but is not limited to the following: 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 employee; an employee's personal views or opinions except where they are about another individual.

Employee personal information does not include business card information such as name, business title and business contact information when used or disclosed for the purpose of business communications; classification, salary, discretionary benefits or employment responsibilities; business travel expenses; professional opinions; other information as identified by legislation.

The employer is responsible to develop employee privacy awareness programs and provide training opportunities.

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

Every City employee and contractor who handles employee personal information, as a result of their employment or contract with the City, is required to sign and abide by any relevant City of Regina confidentiality agreements; is responsible for managing personal and confidential information in accordance with those agreements, the City of Regina Privacy Policy and Confidentiality Guideline, as well as this guideline; and is responsible for proactively incorporating privacy protection into all initiatives.

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

4.1 Duty to Protect

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

4.2 Collection

Any employee personal information collected by or for the employer must be relevant to an authorized program or activity and must only be collected for a legitimate business purpose. The employer must only collect personal information that is necessary for its stated purpose or as required by law.

An employee must be informed on why the personal information is being collected and its intended uses, except when doing so would result in the collection of inaccurate or misleading information.

The employer collects personal information about its employees for purposes such as:

- Recruitment
- Administering pay and payroll deductions
- Complying with tax requirements and legal obligations
- Administering pension and benefits
- Employment verification
- Documenting training, educational, certification and licensing requirements
- Monitoring, documenting, assessing and addressing employee performance
- Processing work-related claims
- Documenting absences from work
- Responding to medical emergencies
- Administering employee services (e.g. parking, employee facility passes)
- Monitoring (e.g. surveillance for the protection of employees and third parties, protection against theft, vandalism, and damage to City property)
- Medical information for purpose of accommodation/leave

4.3 Consent

Consent should be informed, meaning that the employee is aware of and understands the purpose for the collection and how the information will be used or disclosed.

An employee is deemed to have consented to the collection, use and disclosure of their personal information if they have given the information voluntarily, if they have signed an acknowledgement or if it is reasonable that a person would voluntarily provide that information. Written consent is preferred in situations that allow it.

Generally, consent must be obtained from the employee prior to collecting, using or disclosing their personal information; however, in some cases gaining consent from the employee may not be feasible, appropriate or the only lawful means for collecting, using or disclosing employee personal information. In these cases, the employer must still have legitimate authority from LA FOIP, a bylaw, other legislation or policy. If the collection, use or disclosure is authorized by corporate policy, that policy must be compliant with LA FOIP and the employer must undertake reasonable efforts to make sure that employees are aware of the policy and have access to the policy.

4.4 Confidentiality

Records containing personal information about current or former employees are private and confidential, should be identified as such, and must be stored in a secure manner with appropriate access restrictions and controls for both paper and electronic records.

Generally, only authorized individuals have a right to access an employee's personal information, unless that employee has given informed, written consent.

4.5 Employee Access

An employee has the right to be informed of the existence, use and disclosure of information pertaining to them. Employees also have the right to access their personal information upon request, to challenge the accuracy and completeness of their personal information and to request their personal information be amended when appropriate.

- To view their own personnel file, an employee would make a written request to People & Organizational Culture (POC) or the business area. Access will be provided during normal business hours, and at a mutually convenient time. Proof of identification is required.

- If the file contains personal information about another individual, that individual's information **must be removed** before the file can be viewed by the employee.

- A review of the personnel file must be carried out in the presence of a designated POC employee to maintain the accuracy and integrity of the file.

- A review of personal information held in other business areas must be carried out in the presence of the manager or supervisor of that business area.

- The employee may not remove the file or any of its contents but may request copies of information contained in the file.

4.6 Third Party Access

An employee may give written consent for another individual to access information in their file. The employee may not be aware of the types of information contained in their file; there is an obligation to ensure the employee understands what they are consenting to before releasing information to the third party.

Access to employee files is restricted to authorized employees who have a legitimate business purpose to access (e.g. where it is necessary in the performance of their administrative duties or there is a legitimate need, such as for the safety of the individual; or to facilitate contact with next of kin in an emergency). Otherwise, consent must be obtained.

- In situations where employees apply for other jobs within the City, the hiring manager may not access performance, disciplinary or other actions of an employee as part of the selection process; this type of information should be gathered through the reference check process.

4.7 Home Contact Information

Employee home contact information will not be disclosed to others unless required to do so by agreement (e.g. collective agreement), by law, in an emergency situation or with the employee's consent.

4.8 Retention

Paper files are maintained until retention requirements have been met, in accordance with the City's *Records Retention and Disposal Schedules Bylaw* and are then securely destroyed. Electronic documents are subject to the same provisions.

4.9 Accuracy

Reasonable efforts must be made to ensure that the employee personal information collected is as accurate, complete and as up to date as required for the purposes it is being used.

4.10 Right of Correction

An individual has the right to request correction of personal information as outlined in Section 31 of LA FOIP.

If an employee has concerns with the accuracy of their personal information or would like their information amended, they should contact the area responsible for collecting the information or their supervisor.

Circumstances may exist where the employer may not agree with, or disregard changes requested by the employee. In that situation the employer will document:

- Date that a correction was requested
- Correction that was requested
- Reasons the correction was not made or was disregarded
- Signature of the employee who documented the request

The City has an obligation to advise the individual within 30 days, in writing, of the decision to make the correction or why it chose to disregard the request.

If the employee has a complaint regarding their information or the response received on the request for correction, they can contact the APT.

4.11 Privacy Breach

A privacy breach occurs when there is unauthorized access to, use or disclosure of personal information. Such activity is unauthorized if it occurs in contravention of LA FOIP.

If an employee believes a privacy breach has occurred with respect to their own, or to another employee's information, the employee must report the suspected privacy breach to the APT. The APT will investigate the breach to determine what actions are required according to privacy breach protocol.

4.12 Security

The employer endeavors to maintain physical, technical and organizational/administrative safeguards to protect employee personal information. These safeguards are designed to prevent loss and unauthorized access, copying, use, modification, disclosure or destruction of personal information.

4.13 Risk Assessments

For any new initiative where there is employee personal information collected, used or disclosed, risk assessments must be conducted to ensure all privacy and security risks have been identified, mitigated or accepted.

4.14 Private Information

Information relating to an employee's private life, including email of a private nature, should not be transmitted or stored on servers or systems owned by the City. Employees should have no expectation of privacy when using City servers or systems. Private information, stored on corporate servers or systems, may be subject to viewing by authorized personnel and use of City servers or systems could put private information into the purview of an access to information request. Any private information should be removed to a personally owned device or a personal email account.

4.15 Questions and Concerns

Questions or concerns about the appropriateness of collecting, using or disclosing employee personal information can be directed to the APT.

4.16 Ability to Challenge

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

If the employee remains dissatisfied after the APT has received, reviewed and responded to a concern, the employee has the right to raise their concerns with the Office of the Saskatchewan Information and Privacy Commissioner.

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.
- Administering privacy breach protocol.

Employees are responsible for:

- Compliance with this guideline and related policies and procedures.
- Protecting personal information.
- Notifying the APT in the event of a suspected or actual privacy breach and providing cooperation during the breach investigation.

6.0 Related Forms

Privacy Complaint Form

7.0 Reference Material

The Local Authority Freedom of Information and Protection of Privacy Act
The Records Retention and Disposal Schedules Bylaw, 2012 No. 2012-18
Privacy Policy # 2015-OCCOP-P0001
Access to Information Policy #2015-OCCOP-P0002
Privacy Breach Guideline #2016-OCC-G0001
Confidentiality Guideline #2017-OCC-G0001
Email Acceptable Use Policy EAU-001

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
15-12-2017	Revision – Update LA FOIP acronym	CC	No
01-07-2018	Scheduled Review – LA FOIP Amendments	CC	Yes
15-07-2019	Revision – Section 4	CC	Yes
01-08-2021	Scheduled Review	CC	Yes