OPERATIONAL GUIDELINE

Guideline Title:	Applies to:		Reference #
Privacy Incident/Complaint	All employees and contractors		2016-OCC-G0001
Approved by:	**Dates:**		**Total # of Pages**
City Clerk	**Effective:**	01-May-2015	12
	Last Review:	01-Sept-2021	
	Next Review:	01-Sept-2023	
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 purpose of this guideline is to assist City employees and contractors to identify and investigate a privacy incident or privacy complaint.

2.0 Scope

This guideline applies to all City of Regina employees and contractors.

3.0 Definitions

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

Contractor – an individual or company retained under 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.

IPC – the Saskatchewan Information and Privacy Commissioner.

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

Lead Investigator – the business area employee assigned to manage a privacy incident.

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 information.

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

Privacy Complaint – when a concern is expressed with the way the City handles personal information.

Privacy Incident – a reported situation where it is suspected that personal information has been improperly handled, but which may not be determined to be a breach.

Record – 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 – a person or company other than the City.

4.0 Guideline

4.1 Privacy Incident

A privacy incident is a reported situation where it is suspected that personal information in the possession or under the control of the City has been improperly handled. An incident may be reported by an employee or by an external party.

A privacy incident is typically identified when an employee or external party brings a privacy concern forward to a business area and/or the Access and Privacy Team (APT).

- It is critical that the APT be notified immediately when it is suspected that an incident may occur or perceived that an incident has occurred.
- The lead investigator (as determined by the business area) is responsible for completing the Business Area Privacy Incident Report and submitting it to the APT.
- The APT determines if an incident response team is required.
- The APT investigates the incident and completes the APT Privacy Incident Investigation Report retaining all documentation related to the incident in accordance with the City's *Records Retention Bylaw.*
- The APT is responsible to determine whether the privacy incident constitutes a privacy breach, to notify the business area of that determination and to make recommendations to the business area on containment, mitigation, notification and future preventative measures.

4.2 Privacy Complaint

A privacy complaint may be made by an employee or an external party who believes the City has mishandled personal information.

When a Privacy Complaint form or written communication regarding a privacy complaint is received at the City it should be forwarded immediately, in confidence, to the Access and Privacy Team.

- The APT communicates with the complainant as required to determine the nature of the complaint.

- The APT investigates the complaint and completes a Privacy Complaint Investigation Report retaining all documentation related to the complaint in accordance with the City's *Records Retention Bylaw.*

4.3 Privacy Breach

The incident or complaint is determined to be a privacy breach when unauthorized access to, use or disclosure of personal information occurs in contravention of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).

To be in contravention of LA FOIP, the incident must involve:

- Personal information of an identifiable individual, as defined under LA FOIP.

Examples of a privacy breach may include:

- Personal information emailed or faxed to the wrong person.

- Letters containing personal information mailed to the wrong person or address.

- Lost or stolen digital devices, computers or portable storage devices, which store personal information and are inadequately secured (i.e. encryption, password protection).

- Equipment containing personal information destroyed in an unsecure manner.

- Personal information accessed by an individual for a non-approved purpose (i.e. snooping).

Personal information stolen, lost, misdirected and/or mistakenly or intentionally accessed or disclosed constitutes a breach and must be investigated.

4.3.1 Containment

A reasonable effort must be made to contain a breach, as quickly as possible, through the following actions:

- Stop the unauthorized practice.

- Recover the information.

- Shut down or correct any weaknesses in security.

Examples of containment may include:

- If a fax is sent to a wrong number, ask the recipient to securely destroy any paper records including copies. Ask for written confirmation that the records have been destroyed.

- If an email is sent to the wrong individual, call the recipient and ask them NOT to forward or reply to the message and to delete the message from all folders (Inbox, Sent Items, Deleted Items, Recover Deleted Items from Server, other). Ask for written confirmation that the records have been deleted.

- If an unauthorized person has or may have access to a database or computer system, notify Innovation, Energy & Technology (IET) to have the account disabled or passwords changed.

- If a letter is sent to the wrong person, ask the individual to return the letter or have someone pick it up. It is incumbent on the City to provide assurances, to those affected, that the inappropriately disclosed information has been recovered.

- If an electronic device has been lost or stolen, report it to IET immediately. This ensures appropriate safeguards are taken to protect the information on the device (i.e. remotely wipe, etc.).

Do not compromise the ability to investigate the breach.

- Be careful not to destroy evidence that may be valuable in determining the cause of the breach or that will allow the City to take appropriate corrective action.

If there is a risk of criminal harm, the business area should contact the Regina Police Service (RPS) immediately.

- If an emergency, call 911.

- If not an emergency, call 306-777-6500.

The main objective is to lessen any consequences for the individual(s) whose personal information is involved, as well as consequences to the City.

4.3.2 Risk Assessment

The APT considers the following when assessing risk and to determine necessary mitigations:

Nature of breach:

- What data elements have been breached?
    - Generally, the more sensitive the data, the higher the risk.
    - A combination of information is typically more sensitive than a single piece of information.
    - Personal information, considered more sensitive in nature, may include health information, government-issued identification such as social insurance number, driver's license, or health card number, or financial account number (such as credit or debit card) that could be used for identity theft.
- What use is there for the personal information?
- Could it be used for fraudulent or other harmful purposes?
- What is the context of the personal information involved?
    - A list of names and addresses which could be found in a telephone book or online is less sensitive than a list of names and addresses of employees who are away on sick leave.

Cause of breach:

- What was the cause of the breach?
- Is there risk of further exposure of the information?
- What was the extent of the unauthorized collection, use or disclosure of the information?
- How many individuals may have had access to the information?
- Was the information lost or was it stolen?
    - If stolen, was it likely the information was the target of the theft?
- Was the information encrypted or not readily accessible?
- Has the information been recovered?
- What steps have already been taken to minimize harm?
- Is this a systemic issue or an isolated incident?
- Was the breach accidental or was there malicious intent?

Individuals affected by breach:

- How many individuals are affected by the breach?
- Who is affected (public, employees, customers)?

Foreseeable Harm:

- Who is in receipt of the information?
    - Someone who accidentally receives the information and reports it is less likely to misuse the information than someone suspected of criminal activity.
- Is there a relationship between the person affected by the breach and the recipient of the information?
    - A close relationship between the victim and recipient may increase the likelihood of harm (e.g. if an estranged spouse has gained unauthorized access to a home address or phone number).
- What harm to the victim may result from the breach?
    - Physical safety and security.
    - Identity theft or fraud.
    - Loss of employment or business opportunities.
    - Damage to reputation or relationships.
    - Hurt or humiliation.
- What harm to the City may result from the breach?
    - Loss of trust.
    - Loss of assets.
    - Financial exposure.
    - Loss of contracts/business.
- What harm to the public may result from the breach?
    - Risk to public health and/or safety.
- Is the harm imminent?

4.3.3 Mitigation

The APT makes recommendations on immediate corrective action to reduce the harm of the privacy breach under investigation.

Process improvements may also be recommended over the long term to ensure future breaches do not occur.

4.3.4 Notification

It must be determined whether notification is necessary to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed. Some considerations may be:

- Is notification required by legislation?
- Is there a contractual obligation to notify?
- Is there a risk of identity theft or fraud?
- Is there a risk of physical harm?
- Is there a risk of hurt, humiliation or damage to reputation?
- Is there a risk of loss of business or employment opportunities?
- Is there a risk of loss of confidence in the City?
- Do good customer relations dictate that notification is appropriate?

Notification should occur as soon as possible after the breach.

- If the Regina Police Service (RPS) has been notified, notification to those affected may need to be delayed to not interfere with a criminal investigation.

Direct notification (by phone, letter, email or in person) is preferred.

Indirect notification (media reports, posted notices, via websites) should generally only occur where:

- Direct notification would cause further harm.
- Direct notification is cost prohibitive.
- Contact information is lacking.
- Large number of individuals are affected by the breach and direct notification would be impractical.

In some cases, using multiple methods of notification may be the most effective.

Notification should include the following:

- Date of the breach.
- Description of the breach (a general description of what happened).
- Description of the information breached (i.e. name, medical records, credit card numbers or banking information, social insurance numbers).
- Risk(s) to the individual caused by the breach.
- Steps taken to control or reduce harm.
- Steps planned to prevent future privacy breaches.
- Steps the individual can take to further mitigate the risk of harm:
    - Who to contact regarding social insurance numbers, personal health card numbers or driver's license numbers?
    - How to contact a credit reporting agency to set up a credit watch.
    - Who to contact at the City to answer questions or provide further information?
    - Advise that the individual has a right to complain to the IPC.
    - Contact information for the Saskatchewan IPC.
    - If the City has already notified the IPC, that detail should also be provided in the notification letter.
    - In anticipation of telephone calls, emails or other contact by the public or the media, a list of frequently asked questions may be prepared to assist staff in responding to further inquiries (i.e. Service Regina, Communications).
    - Consider whether the following authorities or organizations should be informed of the breach:
        - Police, if
            - Risk of criminal harm.
        - IPC, depending on
            - Sensitivity of the personal information.
            - The number of people affected by the breach.

- If the information could be used to commit identity theft.
- If there is a reasonable chance of financial, economic or non-monetary harm.
- If the information was fully recovered without further disclosure.
- If there were safeguards such as encryption in place to protect the information from unauthorized collection, use and disclosure.
- Whether the City needs advice or assistance from the IPC.

- If there are other internal or external parties requiring notification, such as:
  - Third party contractors.
  - Other business areas.
  - Unions.
  - Communications.
  - Insurers or others if required by contractual obligations.
  - Credit card companies and/or credit reporting agencies.
  - Other professional or regulatory bodies.

4.3.5 Prevention

Once immediate steps are taken to mitigate the risks associated with the breach, time should be taken to thoroughly investigate the cause of the breach and to develop or improve appropriate long-term safeguards against further breaches. Adopting security and privacy protection measures is critical.

The following points will assist to prevent privacy breaches:

- Only collect the information necessary to perform the business function. You must be able to identify the need.
- Only use or disclose information if it is consistent with why the information was originally collected.
- If in doubt, obtain consent.

Keep the information only as long as it is needed:

- Make sure information is accurate and current.
- Make sure information is secure. Some examples of this include:
    - Policies and procedures defining and limiting access to personal information.
    - Encryption.
    - Strong passwords.
    - No password sharing.
    - Appropriate access restrictions.
    - Locked filing cabinets.
    - Clean desk policy.
    - Use only authorized means to access City information.
    - Firewall protection.
    - City-approved applications or devices.
- Ensure access to databases, files and software is removed when employees leave their employment or change positions within the City if there is no business purpose for them to have access in their new position.
- Contact the APT when contemplating the implementation of new software or applications to reduce privacy risks and provide advice on privacy concerns.
- Initiate the privacy impact assessment process for new initiatives and when changes are anticipated to current initiatives.
- Attend privacy training sessions and review online training modules to be aware of employee obligations with respect to LA FOIP.
- Regularly audit programs and personal information being collected to ensure it is still required.
- Ensure employees sign confidentiality agreements prior to being given access to personal information.
    - File signed agreements and retain in accordance with *The Records Retention and Disposal Schedules Bylaw*.

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.

Access and Privacy Team is responsible for:

- Ensuring compliance with access and privacy provisions of LA FOIP as well as City policies, guidelines and procedures.
- Providing advice regarding relevant records and issues that should be considered when determining whether to disclose or withhold the information.
- Attending relevant training.

Employees are responsible for:

- Compliance with this guideline and related policies and procedures.

6.0 Related Forms

Privacy Complaint Form
Business Area Privacy Incident Report
APT Privacy Incident Investigation Report
Privacy Complaint Investigation Report
Privacy Breach Notification Template

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*
Privacy Policy # 2015-OCCOP-P0001
Employee Privacy Guideline # 2015-OCCOP-G0001
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: Privacy Breach/Complaint Protocol	ELT	No
01-05-2016	Replace Privacy Breach/Complaint Protocol with Privacy Breach Guideline	CLO & CC	Yes
01-05-2017	Scheduled Review	CC	No
01-01-2018	Revision	CC	No
01-07-2018	Revision - Rename	CC	Yes
01-07-2019	Review - Definitions	CC	Yes
01-09-2021	Scheduled Review	CC	Yes