Best Practices for Mayors, Reeves, Councillors and School Board Members

In Handling Records that Contain Personal Information

This resource discusses the type of personal information that Mayors, Reeves, Councillors and School Board Members might collect that is not in the possession or control of the organizations they serve. It also discusses measures these elected officials should take to protect this information.

October 2023

Office of the
Saskatchewan Information
and Privacy Commissioner

Best Practices for Mayors, Reeves, Councillors and School Board Members

Mayors, Reeves, Councilors and School Board members (Elected Officials) who handle personal information may not realize that this information is required to be protected under *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). The Saskatchewan Information and Privacy Commissioner has developed this document to assist Elected Officials in protecting the personal information that they collect.

Before proceeding, it is important to understand in what limited circumstances LA FOIP may apply to certain information or records.

What is a Record

LA FOIP applies to information recorded in any form in the possession or under the control of a local authority. Subsection 2(1)(j) of LA FOIP describes a record as:

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

Municipalities and school boards are local authorities pursuant to LA FOIP. If the Elected Official of the local authority is engaged in carrying out the mandate or functions of the local authority, then LA FOIP most likely will apply to any information/records collected or generated while performing these duties. However, LA FOIP would not apply to records of Elected Officials if those are collected or generated in the course of conducting constituency business or political activities.

The second consideration is to determine if the records contain personal information.

What is Personal Information

For a full definition of what is considered personal information, see subsection 23(1) of LA FOIP.

To qualify as personal information, two components must exist:

1. The information must be about an identifiable individual.

2. The information must be personal in nature.

Some examples of what could constitute personal information:

- The individual's race, national or ethnic origin, colour or religious or political beliefs or associations.
- The individual's age, sex, marital status or family status.
- Information about the individual's educational, financial, employment or criminal history, including criminal records, whether or not a pardon has been given.
- An identifying number, symbol or other particular assigned to the individual.
- Anyone else's opinions about the individual.
- The individual's name, home or business address or home or business telephone number.
- The individual's personal views or opinions, except if they are about someone else.

Personal health information is treated as personal information under LA FOIP, which includes information that relates to health care or the health history of the individual.

Duty to Protect

In 2017, an amendment to LA FOIP added an explicit duty of local authorities to protect personal information in its possession or control (subsection 23.1 of LA FOIP). This includes having measures in place to ensure personal information is protected.

Section 23.1 of LA FOIP requires that a local authority have administrative, technical and physical safeguards to protect personal information. This duty extends to Elected Officials when undertaking local authority business. If collected, used or disclosed for other purposes, then best practices should be utilized to prevent privacy breaches.

Administrative safeguards are controls that focus on the internal organization's policies, procedures and maintenance of security measures that protect personal information. Examples include written policies and procedures, annual training for employees, confidentiality agreements, agreements with information management service providers (IMSPs), auditing programs, records retention and destruction schedules and access controls.

Technical Safeguards are the technological measures, which protect personal information in digital form and control access to it. Examples include separate user identifications,

role-based access, passwords, firewalls, identification and authentication controls, virus scanners and audit capabilities in digital systems.

Physical Safeguards are physical measures utilized to protect personal information contained in buildings and equipment from unauthorized intrusion and natural and environmental hazards. Examples include locked filing cabinets, offices and storage rooms, alarm systems and clean desk policies.

A privacy impact assessment (PIA) is an effective tool for assisting a local authority to identify any potential privacy risks and mitigation strategies related to these safeguards in existing or new systems, processes and projects. For further information on PIA's see our resource *Privacy Impact Assessment, A Guidance Document* and the blog, *Privacy Impact Assessments*.

Consent

Consent of the individual is required for the collection, use or disclosure of personal information. When an Elected Official talks to a citizen, have the citizen consent to you collecting, using or disclosing information and keep that consent on your file (either hardcopy or electronic). A written consent is the best, email consent is next best and consent over the telephone is least best. Telephone consent, and other important details such as date and time, should be recorded in your notes.

Purpose and Collection

Citizens and organizations consult Elected Officials on problems and issues they have with local government and/or the health system. In that process of asking for help, they may provide documents or give verbal information to Elected Officials which contains considerable sensitive personal information.

The collection of personal information should be limited to only what is necessary for the purposes for which it was collected. Before collecting any personal information, the Elected Official should pause and assess the purpose for collecting this information and whether this information is necessary for such a purpose.

Elected Officials should refrain from collecting more personal information than is necessary to fulfill the identified purpose. In particular, consider documents that you may not need to collect such as tax returns, doctor's reports, financial statements, laboratory tests and non-relevant correspondence.

Use and Disclosure

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

Local authorities and Elected Officials must abide by the need-to-know principle which stipulates that personal information should only be available to those individuals in an organization that have a legitimate need to know that information for the purpose of delivering their authorized services.

Individual Access

When personal information is collected or generated with an organization, individuals should be able to request access to view their information or obtain a copy upon request. They should be informed whether personal information about them exists how it is used and disclosed. If the individual believes there is inaccuracies in their personal information, they should be able to request it be corrected.

Retention Periods

Once the purpose for which the information was being collected has been fulfilled, the personal information should be disposed of, unless otherwise required to be retained by law.

With respect to records retention and disposal schedules, Elected Officials may want to consult with the Provincial Archives of Saskatchewan. Contact information for the Board is available on its website, The Provincial Archives of Saskatchewan (saskarchives.com).

A record retention and disposal schedule prescribe requirements for the length of time private record(s) of an Elected Official must be retained and the appropriate means of disposal at the end of its lifecycle. It is a best practice to develop a record retention and disposal schedule for your office to ensure that you have a list of all personal information that you have collected as well as knowing when you can delete such information. If again the records you have are related to the local authorities' business, then its record retention practices apply instead.

Elected Officials that have collected personal information should destroy the sensitive information as soon as they no longer require it or once the file is closed.

If an Elected Official is no longer running for office, the Elected Official may wish to transfer or share certain open files related to unresolved issues or cases where the constituent or organization is now represented by another Elected Official. If there are records of a sensitive nature or containing personal information, the Elected Official should get written consent from the individual before transferring the records.

In assessing what is the appropriate retention period and whether it is time to dispose of personal information, an Elected Official should consider the following points:

- Reviewing the purpose for having collected the personal information in the first place is generally helpful in assessing how long certain personal information should be retained.
- If personal information was used to make a decision about an individual, it should be retained for the legally required period of time – or other reasonable amount of time in the absence of legislative requirements – to allow the individual to access that information in order to understand, and possibly challenge, the basis for the decision (i.e., employment records that hold personal information).

Elected Officials need to make informed choices about how long to keep personal information and when and how to safely dispose of it. The capacity and desirability to retain massive amounts of personal information indefinitely increases the risks and consequences of a potential privacy breach.

If retaining personal information would result in a prejudice for the concerned individual or increase the risk and exposure of potential privacy breaches, the Elected Official should consider safely disposing of it.

Secure disposal

If an Elected Official has personal information in his or her control, he or she cannot simply throw it away in the trash. The Elected Official must find a way to securely dispose of it.

In instances where an Elected Official is planning a move, or is closing his/her doors, personal information should be securely transferred or disposed of.

There are several commonly accepted ways for Elected Official's to properly dispose of personal information depending on the form in which it is being stored. The goal is to irreversibly destroy the media or delete the information which contains personal information so that this information cannot be reconstructed or recovered in any way.

When going through the process of destruction, an Elected Official should also destroy all associated copies and backup files.

Types of Data Storage

Information is mainly stored in two types of formats:

- Hard copy: physical representations of data, such as paper. This includes, among other things, notes, memos, messages, correspondence, transaction records and reports.
- Electronic copy: information stored on electronic media, such as computer servers, hard drives, copier and printer hard drives, removable solid drives including memory, and USB flash drives, mobile phones and magnetic tapes.

There are several ways in which personal information can be securely deleted or removed by completely destroying the media, whether hard or electronic copy. It is a way to ensure that the information stored on it can never be recovered. This can be accomplished using a variety of methods including disintegration, incineration, pulverizing, shredding using a cross-shed shredder, melting and overwriting.

If personal information is stored on a cloud server, deleting the record may not delete the personal information from the cloud. Depending on the cloud service provider used, there may be different processes or permissions to permanently, immediately (there may be a grace period) delete the information. Some cloud service providers may offer additional options to prevent the information from being recovered (such as overwriting the information).

Use of Third Parties

An Elected Official should assess the risks and benefits of destroying personal information on-site or off-site. If an Elected Official does not have appropriate tools to safely destroy sensitive information on-site, it may consider the services of a third-party contractor. In some cases, the sheer volume of the personal information to be disposed of can tip the balance towards using companies specialized in data destruction.

Third parties, in this context, are sometimes referred to as information management service providers.

When considering using a third party to dispose of personal information, an Elected Official should consider the sensitivity of the personal information and take steps to manage the risks accordingly.

An Elected Official should ensure that the third party contractor has verifiable credentials and can guarantee both a secure transfer of records from the Elected Official's office to their own destruction facility, and a secure destruction method that matches the media and the sensitivity of personal information.

If an Elected Official decides to contract out, he or she should keep in mind that he/she remains responsible for the information to be disposed of. Best practices when dealing with third parties include:

- Entering into a written contract with the contractor.
- Including privacy protection clauses in the contract to ensure the third party provides an appropriate level of protection.
- Including monitoring and auditing clauses in the contract to ensure tracking of the personal information and quality control.

Putting it All Together: Developing Internal Policies & Procedures

In setting up policies and procedures, an Elected Official should consider the following checklist:

- Is information in the Elected Official's office periodically being reviewed to determine whether the purpose of the collection has been fulfilled. How often.
- Is there an inventory of what personal information is being retained, for which purpose and for how long and is it related to the local authorities' business or its own.
- Are security measures (password protection, role-based access) in place to ensure only those with a 'need to know' have access to the personal information.
- Are audit functions built into electronic systems to ensure unauthorized access is traceable.
- Is personal information being segregated and stored in a secure area with restricted access.
- Have you developed a records retention and disposal schedule.
- Does personal information exist in multiple copies. Are there back-ups. If so, where and how are the copies and back-ups stored.

- Are additional copies of personal information being immediately and securely destroyed (i.e., scanned paper copes are shredded and not placed in trash).
- Is a process in place to immediately and securely control personal information that may be dropped off.
- When should the Elected Official dispose of the personal information.
- How should the Elected Official dispose of personal information, copies and backups.
- What measures should be taken to ensure the equipment or devices used for storing the personal information (servers, mobile phones, copiers, scanners, etc.) are properly disposed of, or sanitized.
- Is there a designated secure area for destroying documents.

For further guidance on handling personal information, please see *Guide to LA FOIP, Chapter 6, Protection of Privacy*.

Contact Information

If individuals have concerns with the manner in how their personal information is collected, used, disclosed, retained or destroyed, you can refer them to our office.

If you have any questions regarding the collection, use, disclosure, retention or disposal of personal information that is in your possession or control during your term, please feel free to contact us:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

intake@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC