How FOIP applies to you

A Guide for Members of the Legislative Assembly and Minister's Offices

In 2017, amendments were made to *The Freedom of Information and Protection of Privacy Act* (FOIP) which caused some of the protection of privacy portions of the Act to apply to members of the Legislative Assembly (MLAs), their employees and cabinet ministers' offices. This guide explains what MLAs and Ministers should know.

January 2018

Office of the
Saskatchewan Information
and Privacy Commissioner

How FOIP applies to you

A Guide for Members of the Legislative Assembly and Minister's Offices

Amendments made to *The Freedom of Information and Protection of Privacy Act* (FOIP) effective January 1, 2018 caused members of the Legislative Assembly (MLAs) and their employees and members of Executive Council (Ministers) and their offices subject to Part IV of FOIP. As a result the offices of MLAs and Ministers must take steps to protect personal information.

This guide will assist MLA's, Minister's and their employees to ensure they are compliant with FOIP.

WHAT PARTS OF FOIP APPLY?

Note: MLA's and Minister's offices are referred to as a government institution in FOIP. When referring to MLAs and/or Ministers and their employees, the term "office" will be used in this document.

The access to information portions of FOIP do not apply to offices.

Subsections 3(3) and (4) of FOIP provide as follows:

> (3) Subject to the regulations, the following sections apply, with any necessary modification, to offices of members of the Assembly and their employees as if the members and their offices were government institutions:
>
> (a) sections 24 to 30;
>
> (b) section 33.
>
> (4) Subject to the regulations, the following sections apply, with any necessary modification, to offices of members of the Executive Council and their employees as if the members and their offices were part of the government institution for which the member of the Executive Council serves as the head:
>
> (a) sections 24 and 24.1;
>
> (b) sections 25 to 30;
>
> (c) section 33.

The majority of Part IV of FOIP – Protection of Privacy – applies to offices. However, individuals do not have a right to access personal information or request corrections to personal information.

Minister's offices are not subject to section 24.2 of FOIP which deals with information management service providers (IMSPs) while this section does apply to MLA offices.

How Do I Protect Personal Information? (The Duty to Protect)

Sections 25 to 30 of FOIP and its Regulations provide the rules on when offices should collect, use and disclose personal information. Any collections, uses or disclosures unauthorized by FOIP would be a privacy breach. Additionally, section 24.1 of FOIP imposes a duty on offices to protect personal information. It requires that these offices have administrative, technical and physical safeguards in place to protect personal information.

Administrative safeguards are controls that focus on internal organizations, 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 IMSPs, auditing programs, records retention and destruction schedules and access restrictions.

Technical Safeguards are the technology and the policy and procedures for its use that protect personal information and control access to it. Examples include separate user identifications, passwords, firewalls, identification and authentication controls, virus scanners and audit capabilities in digital systems.

Physical Safeguards are physical measures, policies, and procedures to protect personal information and related 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 approaches.

Section 24.1(a) of FOIP indicates that an office must protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;

Integrity refers to the condition of information being whole or complete; not modified, deleted or corrupted.

Confidentiality implies a trust relationship between the person supplying information and the individual or organization collecting or using it.

Section 24.1(b) of FOIP indicates that an office must protect against any reasonably anticipated:

- threat or hazard to the security or integrity of the personal information in its possession or under its control;
- loss of the personal information in its possession or under its control; or
- unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control;

Threat means a sign or cause of possible harm.

Hazard means a risk, peril or danger.

Security means a condition of safety or freedom from fear or danger.

Unauthorized access occurs when individuals have access to personal information that they do not need-to-know, either by accident or on purpose. This would also qualify as either an unauthorized use or unauthorized disclosure.

A need-to-know is the principle that an office should only collect, use or disclose personal information needed for the purposes of the mandated service. Personal information should only be available to those employees in an organization that have a legitimate need-to-know that information for the purpose of delivering their mandated services.

An unauthorized collection occurs when personal information is collected, acquired, received or obtained by any means for purposes that are not allowed under sections 25, 26, 27, 28 or 29(2) of FOIP.

Unauthorized use refers to the use of personal information for a purpose that is not authorized under sections 27, 28 or 29(2) of FOIP.

Unauthorized disclosure refers to the act of revealing, showing, providing copies, selling, giving, or relaying the content of personal information in ways that are not permitted under sections, 29 or 30 of FOIP.

Section 24.1(c) of FOIP indicates that an office should have education programs in place for their employees which addresses the MLA's or Minister's office's duties under FOIP safeguards the office has established, the need-to-know and consequences for violating FOIP. The IPC has indicated that annual training is best practice.

See more information on safeguards, see the Considerations about Certain Safeguards section at the end of this document.

What Happens if there is a Breach of Privacy?

Once a privacy breach occurs, it is nearly impossible to undo it. The focus of dealing with a privacy breach should be retrieving the personal information (if applicable), notifying affected individuals and preventing future breaches.

Consult the IPC resource *Privacy Breach Guidelines for Government Institutions and Local Authorities* for information on what to do if there is a privacy breach.

What is my Purpose for collecting Personal Information?

Constituents and organizations consult MLAs and Minsters on problems and issues they have with government and/or the health system. In that process of asking for guidance, they may provide documents or give verbal information which contains considerable sensitive personal information or personal health information.

Before collecting any personal information the office should pause and assess the purpose for collecting this information and whether this information is necessary for such a purpose. The collection should be in line with sections 25, 26 and 27 of FOIP. Offices should refrain from collecting more personal information or personal health 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.

Am I able to Use or Disclose Personal Information?

Offices should consider future uses and disclosures of the personal information at the time of collection.

Uses might include tracking issues in the constituency office or the party, using contact information for constituency news letters or holiday greetings, etc.

Disclosures might include discussing the personal information matter with other organizations in an attempt to find resolution of a complaint, discussing a matter in the Legislature or in the media, etc.

It is best practice to obtain written consent from the individual before any collections, uses or disclosures of personal information occur. If consent is not obtained, collections, uses and disclosures of personal information must be authorized by sections 25, 26, 27, 28, 29 or 30 of FOIP.

Specific scenarios and how FOIP applies

Scenario 1

A family, who has just moved to Saskatchewan, calls to inquire how to obtain a health services card. The constituency assistant connects them with eHealth Saskatchewan. The only personal information collected was the mother's name and contact information. She is satisfied with the help she has received and requires nothing further. Can her contact information be added to the MLA's personal holiday card list?

The collection and use must be authorized by sections 25, 26, 27 of FOIP. Otherwise, the constituency assistant should obtain informed consent from the mother.

Scenario 2

A constituent calls with a complaint about a certain government program. He describes the many steps he has taken to resolve his issue to no avail. The MLA agrees to contact the program

on the constituent's behalf. When the MLA contacts the program, she is referred to a different, but related government program for additional information.

Section 29(2)(a) of FOIP allows the MLA to disclose information, without consent to the government program for the purpose for which the information was obtained or compiled by the MLA or for a use that is consistent with that purpose. The MLA can also collect information for these reasons. Acquiring specific consent is still best practice.

Scenario 3

A constituent calls an MLA to inform him/her that a high school student in the community has raised a large sum of money for a great cause. The MLA wants to make a member's statement in the legislature, congratulating the teen.

Section 26 of FOIP requires that personal information be collected, where reasonably practicable, directly from the individual except in specific circumstances listed in the section. The MLA should contact the teen or the parents/guardians to collect the information. Consent for the disclosure of the information in the legislature should also be obtained.

Scenario 4

A woman dies as a result of a perceived failure of the health system. The son of the woman contacts an MLA with his concerns about the health system. The son is not the woman's personal representative. The personal representative is the woman's daughter who feels that the woman would have wanted to keep the details of her death private. Should the MLA collect the information?

The information being collected is that of the deceased woman. She is unable to consent to the collection, use and disclosure of her personal health information. Pursuant to section 59 of FOIP, the woman's rights can be exercised by her personal representative but only if the exercise of the right or power relates to the administration of the individual's estate. Otherwise, the collection, use or disclosure must be authorized by sections 25, 26, 27, 28, 29 or 30 of FOIP.

What are Best Practices for Obtaining Consent for the Collection, Use and Disclosure of Personal Information?

When the office speaks with a citizen, have the citizen consent to your collecting, using and/or disclosing information and keep a record of that consent on your file (either hardcopy or electronic). It is best if consent is given in writing, but email or verbal consent is also acceptable. MLAs should ensure consent provided verbally is properly documented and retained.

In FOIP consent is sometimes required for the collection, use or disclosure of personal information.

Where consent is required, section 18 of the FOIP Regulations requires that the consent:

- must relate to the purpose for which the information is required;
- must be informed;
- must be given voluntarily; and
- must not be obtained through misrepresentation, fraud or coercion.

The statutes also provide that:

- a consent may be given that is effective for a limited period.
- consent may be express or implied unless otherwise provided.
- an express consent need not be in writing.

See section 18 of the FOIP Regulations.

For more information about informed consent, please refer to the IPC resource *Best Practices for Gathering Informed Consent & the Content of Consent Forms*.

See also our sample *Consent Form* for use by Members of the Legislative Assembly.

Considerations about Certain Safeguards

Storage of Personal Information

Offices that collect personal information have a duty to ensure it is stored securely. Information provided to offices will be stored in two types of media:

- 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 hard drives, copier and printer hard drives, removable solid drives including memory, disks and USB flash drives, mobile phones and magnetic tapes.

Personal information, either hard copy or electronic, should be stored in a manner that restricts access to this information. Only employees that need the information to perform their job, also known as need-to-know, should have access to the personal information. Offices should also ensure personal information are stored either in locked cabinets or saved in a secure network drive. Records should not be stored in personal devices, home filing cabinets, or other personal storage.

Retention of Personal Information

MLAs that are also serving as cabinet ministers, will handle two types of records: ministerial records and private records. *The Archives and Public Records Management Act* defines ministerial records as:

> A record created or received by a minister of the Government of Saskatchewan that relates to the office of that minister and to the administration of the public affairs of Saskatchewan, but does not include:
>
> (a) record that is of a personal or political nature; or
>
> (b) record that pertains to constituency business;

The Archives and Public Records Management Regulations, provide further guidance on the definition of ministerial record at subsection 3(1):

> 3(1) For the purposes of the definition of "ministerial record" in section 2 of the Act and in these regulations, "a record created or received by a minister of the Government of Saskatchewan that relates to the office of that minister and to the administration of the public affairs of Saskatchewan" includes:
>
> (a) a record of internal deliberations involving a minister of the Government of Saskatchewan and his or her staff on matters directly relating to that minister's portfolio or any previous portfolio of that minister;
>
> (b) a communication between ministers of the Government of Saskatchewan on matters relating to the portfolio of the minister who is categorizing the record;
>
> (c) a copy of a record from the ministry over which the minister of the Government of Saskatchewan presides that provides information or context for an item or issue being dealt with by that minister;
>
> (d) a communication on a matter directly relating to the portfolio of a minister of the Government of Saskatchewan with persons outside the Government of Saskatchewan;
>
> (e) a record concerning any administrative matter respecting the portfolio or office of a minister of the Government of Saskatchewan;
>
> (f) a record relating to the activities of a minister of the Government of Saskatchewan as a member of the Executive Council and its committees if that minister has made notes on the record or marked the record in any manner;
>
> (g) a record that expresses viewpoints of a minister of the Government of Saskatchewan on any Government-related issue, whether or not that issue is directly related to that minister's portfolio.

The Archives and Public Records Management Act defines ministerial records as public records. As such, these records will need to be retained and transferred to the Provincial Archives of Saskatchewan based on the statutory requirements provided in that Act.

Unlike ministerial records, there are no statutory requirements for MLAs to transfer private records to the Provincial Archives of Saskatchewan, such as records relating to constituency business, as they are considered private records and are not subject to *The Archives and Public Records Management Act*. Therefore, these records may be disposed of based on internal records management policies and procedures developed by the MLA's office. As part of this process, however, MLAs should consider the transfer of records of historical value to the Provincial Archives of Saskatchewan through a private records agreement.

It is crucial that in-house records management protocols be established to ensure that ministerial records are organized, maintained and stored separately from records defined as private. Ministerial records are managed in accordance with the Ministerial Records Schedule #480, approved by the Public Records Committee in 2012. For a copy of the schedule or further guidance on managing ministerial records, MLAs should contact the Provincial Archives of Saskatchewan. The introduction to the schedule provides information on managing records in a Minister's Office as well as examples of ministerial records and private records that may assist MLA offices in classifying records.

A list of the examples provided in this resource for private records are reproduced below for your convenience:

> In accordance with the preamble to Schedule #480 the following are examples of political and personal records:
>
> **Political records**: records created and maintained by the minister (and his/her aides) relating to participation in elections, party caucus deliberations, party conventions and conferences, fundraising events, and party organization and administration. Typically these types of records would include the following activities:
>
> - Caucus
> - Party convention
> - Party leadership
> - Constituency nomination
> - Election campaign records (including publications)
>
> **Personal records:** records created and accumulated by the minister that relate to his/her personal interests and activities and do not relate in any way to his/her official portfolio responsibilities.

In assessing what is the appropriate retention of personal information, MLAs 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 a 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).
- If retaining personal information any longer would result in a prejudice for the concerned individual, or increase the risk and exposure of potential data breaches, the MLA should consider safely disposing of it.

MLAs no longer running for office, 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 MLA. If there are records of a sensitive nature or containing personal information, the MLA should get written consent from the individual before transferring the records.

MLAs need to make informed choices about how long to keep personal information and when and how to dispose of it. MLAs may find it necessary to retain constituency employee personal information longer than sensitive personal information from a citizen who has a complaint or issue. The capacity and desirability to retain massive amounts of personal information indefinitely increases the risks and consequences of a potential data breach.

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.

When performing ministerial duties, our office strongly encourages MLAs to use the Government of Saskatchewan email system that is supported by the Ministry of Central Services. Questions about security and records management arise if and when MLAs use non-government email accounts to do government-related activities. The Ministry of Central Services has the mandate, resources, and expertise to support and manage the Government of Saskatchewan email system, including ensuring the security of email accounts.

When MLAs are performing their constituency work, it is also encouraged that those emails are only sent from their MLA issued email address. This is to allow a clear division between ministerial records and private records for records management purposes.

While we encourage that emails be sent and received from the appropriately designated account, should an MLA receive information in their MLA office or MLA email address records created or received may qualify as ministerial records. Ministers should ensure records are classified based on the nature of the record.

MLAs should also refrain from using personal email accounts for ministerial or constituency work. Any emails sent from a personal email account relating to ministerial or constituency matters will still need to be classified and retained appropriately.

Securely disposing of personal information/personal health information

MLAs that have determined personal information is no longer needed to be retained based on requirements in *The Archives and Public Records Management Act* and/or established in-house records management protocols, the information must be disposed of in a secure manner.

There are a number of commonly accepted ways to properly dispose of personal information depending on the form in which it is being stored. The goal is to irreversibly destroy the media which contains personal information so that this information cannot be reconstructed or recovered in any way. When going through the process of disposal, MLAs should also destroy all associated copies and backup files.

There are several ways in which personal information can be securely destroyed 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 and melting.

Use of third parties to dispose of personal information

MLAs should assess the risks and benefits of destroying personal information on-site or off-site. If MLAs do 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.

When considering using a third party to dispose of personal information MLAs should take into account the sensitive nature of the information and take steps to manage the risks accordingly.

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

If MLAs decide to contract out, it should keep in mind that he/she remains responsible for the information to be disposed of. Best practices when dealing with third parties include:

- Requiring a written contract with the contractor,
- Privacy protection clauses in the contract to ensure the third party provides a level of protection that you are comfortable with; and,;
- Monitoring and auditing clauses to ensure track record and quality control.

Contact Information

If you have any questions or concerns, please contact us:

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

503 – 1801 Hamilton Street | Regina SK S4X 4H7

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