MLA Guide to Protecting Personal Information

A guide to Part IV of FOIP for Members of the Legislative Assembly and their offices

April 2018

Office of the
Saskatchewan Information
and Privacy Commissioner

MLA Guide to Protecting Personal Information

A guide to Part IV of FOIP for Members of the Legislative Assembly and their offices

As of January 1, 2018, offices of Members of the Legislative Assembly (MLAs) and their employees are subject to Part IV of *The Freedom of Information and Protection of Privacy Act* (FOIP). In this document, they will be referred to as "MLA offices".

Subsection 3(3) of FOIP provides:

> **3**(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.

Constituents often entrust MLA offices with personal information. Part IV gives the citizen certain rights of protection and imposes obligations on MLA offices. As a result, MLA offices must take steps to protect personal information.

The only sections in Part IV that do not apply to MLA offices are sections 31 and 32. Section 31 deals with a person's right to access that person's personal information. Section 32 deals with a person's right to a correction of personal information.

Please note that Members of the Executive Council and their offices (Ministers' offices) are also subject to certain provisions in Part IV of FOIP. For more information, see our office's resource: *A Ministers' Guide to Protecting Personal Information*.

WHAT IS PERSONAL INFORMATION?

For a full definition of what is considered personal information, see subsection 24(1) of FOIP. However, subsection 24(1) of FOIP is not an exhaustive list. Generally, the following is considered personal information:

- Information about an identifiable individual;
- Information which is personal in nature;
- The personal views or opinions offered by an individual are the personal information of that person;
- The personal views or opinions of one individual about another person is the personal information of the other person; and
- Employment history.

WHAT IS COLLECTION OF PERSONAL INFORMATION?

Collection is a term used to describe the action of having gathered, obtained access to, acquired, received or obtained personal information.

Constituents regularly consult MLA offices on problems and issues they have with government and/or the health system. In that process of asking for help, they may provide documents or give verbal information, which contains considerable sensitive personal information. This is an example of a collection.

Before collecting any personal information, the MLA office should pause and assess the purpose for collecting this information; and determine whether this information is necessary for such a purpose.

Section 25 of FOIP provides:

> **25** No government institution shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the government institution.

It is important that the MLA office consider the purpose for collecting personal information. In most cases, it is going to be information required to solve the problem that the citizen has. MLA offices should also keep in mind the data minimization principle and only collect specific personal information that is required for the identified purposes. For example, consider which information and documents that may not be needed such as tax returns, doctor's reports, financial statements, laboratory tests and non-relevant correspondence.

When an MLA or a constituency assistant speaks with a citizen, have the citizen consent to the collection of personal information. For more information on consent, please see below.

Once an MLA office collects personal information, it is up to the MLA office to protect the personal information. For more information, see *What is my duty to protect?* below.

Further, section 26 requires MLA offices to collect personal information directly from the subject individual, except in the circumstances listed in subsections 26(1)(a) to (h) of FOIP.

What is use of Personal Information?

A use of personal information means a reference to or a manipulation of personal information by the MLA office, but does not include disclosure to another person or organization.

Section 27 of FOIP requires that MLA offices take reasonable measures to ensure the personal information used is as accurate and complete as possible.

Section 28 of FOIP provides:

> **28** No government institution shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except:
>
> (a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose; or
>
> (b) for a purpose for which the information may be disclosed to the government institution pursuant to subsection 29(2).

MLA offices can only use personal information in three circumstances:

1) If it has the consent of the subject individual. See the section on consent below.
2) For the purpose it was collected or a use consistent with that purpose. As mentioned in the section on the collection of personal information, MLA offices must have identified an authorized purpose for collecting personal information before it is collected.
3) In circumstances described in subsection 29(2) of FOIP or *The Freedom of Information and Protection of Privacy Regulations* (the Regulations).

Using personal information for any other purpose is not authorized under FOIP.

WHAT IS DISCLOSURE OF PERSONAL INFORMATION?

Disclosure is the exposure of personal information to a separate entity, not a division or branch of the MLA office in possession or control of that information.

Subsection 29(1) of FOIP provides:

> **29**(1) No government institution shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 30.

MLA offices should only disclose personal information in three circumstances:

1) If it has the consent of the subject individual. See the section on consent below.
2) For the purpose it was collected or a use consistent with that purpose. As mentioned in the section on the collection of personal information, MLA offices must have identified an authorized purpose for collecting personal information before it is collected. (See subsection 29(2)(a) of FOIP.)
3) In circumstances described in subsections 29(2), section 30 of FOIP or the Regulations.

Disclosure of personal information for any other purpose would be an unauthorized disclosure.

Sharing personal information between different MLA offices or with a Ministers' office would constitute a disclosure of personal information and must be authorized by the individual's consent, sections 29 or 30 of FOIP or the Regulations.

WHAT SHOULD I DO IF THERE HAS BEEN AN UNAUTHORIZED COLLECTION, USE OR DISCLOSURE OF PERSONAL INFORMATION?

An unauthorized collection, use or disclosure of personal information is a privacy breach. For more information on how to investigate a privacy breach, see the Office of the Information and Privacy Commissioner's (IPC) resource: *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

In instances where there is an unauthorized use or disclosure in an MLA office, there may be an obligation to report that unauthorized use or disclosure to the person whose personal information was used or disclosed. Section 29.1 of FOIP provides as follows:

> **29.1** A government institution shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the government institution if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

It should be noted that this section becomes active where it is believed the breach "creates a real risk of significant harm". For further information, see IPC blog *Real Risk of Significant Harm*.

Further, the IPC can investigate privacy related concerns related to MLA offices. This occurs most often when a citizen brings a concern to the Commissioner.

Section 33 of FOIP provides:

> **33** The commissioner may:
>
> (a) offer comment on the implications for privacy protection of proposed legislative schemes or government programs;
>
> (b) after hearing the head, recommend that a government institution:
>
> (i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and
>
> (ii) destroy collections of personal information that is collected in contravention of this Act;
>
> (c) in appropriate circumstances, authorize the collection of personal information in a manner other than directly from the individual to whom it relates;
>
> (d) from time to time, carry out investigations with respect to personal information in the possession or under the control of government institutions to ensure compliance with this Part.

For more information about the IPC's investigation process, please see *Privacy Breach Guidelines for Government Institutions and Local Authorities* and the *Rules of Procedures*.

WHAT IS MY DUTY TO PROTECT?

Section 24.1 of FOIP imposes a duty on MLA offices to protect personal information in its possession or control. It requires that MLA offices have administrative, technical and physical safeguards in place to protect personal information.

Section 24.1 of FOIP provides:

> **24.1** Subject to the regulations, a government institution shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or

(iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and

(c) otherwise ensure compliance with this Act by its employees.

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 information management service providers (IMSP), 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.

Note that personal information in the possession or control of MLA offices can exist in different types of records such as:

- 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 and mobile phones. This also includes information stored in the cloud. Examples are e-mails, text messages and other electronic documents.

Subsection 24.1(a) of FOIP

Subsection 24.1(a) of FOIP indicates that an MLA 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.

Subsection 24.1(b) of FOIP

Subsection 24.1(b) of FOIP indicates that an MLA 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 access 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 depending on the circumstances.

A need-to-know is the principle that an office should only collect, use or disclose personal information needed for the purposes for which it is was collected. Personal information should only be available to those employees in an organization that have a legitimate need-to-know that information for fulfilling the purpose for which it was collected.

Subsection 24.1(c) of FOIP

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

Information Management Service Providers

IMSP is defined in subsection 2(1)(e.1) of FOIP as follows:

> **2**(1) In this Act:
>
> …
>
> (e.1)"information management service provider" means a person who or body that:
>
> (i) processes, stores, archives or destroys records of a government institution containing personal information; or
>
> (ii) provides information management or information technology services to a government institution with respect to records of the government institution containing personal information;

Any time an MLA office engages an IMSP to provide service, it is necessary to apply section 24.2 of FOIP. This will mainly arise when an MLA office contracts with a technology company to maintain computers or with a company that will destroy files.

Subsection 24.2(1) provides:

> **24.2**(1) A government institution may provide personal information to an information management service provider for the purposes of:
>
> (a) having the information management service provider process, store, archive or destroy the personal information for the government institution;
>
> (b) enabling the information management service provider to provide the government institution with information management or information technology services;
>
> (c) having the information management service provider take possession or control of the personal information;
>
> (d) combining records containing personal information; or
>
> (e) providing consulting services.

Where an MLA office engages an IMSP, it is necessary to enter into a written agreement.

Subsections 24.2(2) and (3) provide:

> **24.2**(2) Before disclosing personal information to an information management service provider, a government institution shall enter into a written agreement with the information management service provider that:
>
> (a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the personal information;
>
> (b) provides for the protection of the personal information; and
>
> (c) meets the requirements of this Act and the regulations.
>
> (3) An information management service provider shall not obtain access to, use, disclose, process, store, archive, modify or destroy personal information received from a government institution except for the purposes set out in subsection (1).

See the IPC's resource entitled *Best Practice for Information Sharing Agreements*.

Retention and destruction of personal information

Unlike Ministerial records, there are no statutory requirements for MLAs to transfer records to the Saskatchewan Archives Board, as they are personal property and not subject to *The Archives and Public Records Management Act*. Therefore, these records may be disposed of as each MLA

sees fit. For information on the Provincial Archives of Saskatchewan, see www.saskarchives.com.

It is a best practice to develop a records classification or records keeping system for MLA offices to ensure that all of the personal information that has been collected is accounted for.

Once a record classification is in place, it is also important to have a record destruction schedule in place. The longer personal information is kept, the longer there is a risk of a privacy breach. MLA offices may consider destroying personal information of citizens as soon as it is no longer required for the purpose for which it has been collected. MLA offices may need to keep employee personal information longer than personal information of a citizen. It is also best practice to have a copy of a record destruction schedule available for interested citizens.

Once a record destruction schedule is in place, MLA offices must take care to dispose of personal information in a secure manner. It is not best practice to simply throw it in the trash as a privacy breach may result.

There are a number of commonly accepted ways for MLA offices 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, an MLA office should also destroy all associated copies and backup files.

In instances where an MLA is planning a move, or is closing the constituency office, personal information should be securely transferred or safely disposed of. MLA offices should obtain written consent from the individual before transferring the records to another MLA, which would constitute a disclosure of personal information.

WHAT IS REQUIRED TO OBTAIN THE CONSENT TO COLLECT, USE AND DISCLOSE PERSONAL INFORMATION?

Section 18 of the FOIP Regulations describes the standard of consent when consent is required for the collection, use and disclosure of personal information.

Section 18 of the Regulations provides:

> **18**(1) If consent is required by the Act for the collection, use or disclosure of personal information, the consent:
>
> (a) must relate to the purpose for which the information is required;
>
> (b) must be informed;
>
> (c) must be given voluntarily; and

(d) must not be obtained through misrepresentation, fraud or coercion.

(2) A consent to the collection, use or disclosure of personal information is informed if the individual who gives the consent is provided with the information that a reasonable person in the same circumstances would require in order to make a decision about the collection, use or disclosure of personal information.

(3) A consent may be given that is effective for a limited period.

(4) A consent may be express or implied unless otherwise provided.

(5) An express consent need not be in writing.

(6) A government institution, other than the government institution that obtained the consent, may act in accordance with an express consent in writing or a record of an express consent having been given without verifying that the consent meets the requirements of subsection (1) unless the government institution that intends to act has reason to believe that the consent does not meet those requirements

Where consent is required it must:

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

It is also important to note that:

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

Express consent is informed and voluntary. Consent is informed when the individual knows the purpose for the collection, use and/or disclosure, that they can withhold or revoke their consent and the consequences of doing so. A consent is also revocable.

The following form has been developed for the use of MLA offices when collecting, using and/or disclosing personal information: MLA Consent form.

For more information on consent, see the IPC's resource: *Best Practices for Gathering Informed Consent and the Content of Consent Forms*.

COMMON SAFEGUARDS REQUIRED FOR COMPLIANCE WITH PART IV OF FOIP

MLA offices should consider the following safeguards:

- ✓ Does the office have a policy relating to the collection, use, disclosure and safeguarding of personal information?
- ✓ Have the employee in the office received privacy training? Training should include:
  - What is FOIP?
  - What is personal information?
  - What is a collection? A use? A disclosure?
  - What are best practices for the collection, use and disclosure of personal information?
  - What administrative, physical and technical safeguards are in place to protect personal information?
  - How to identify the purpose of collecting personal information?
  - What is consent? When is consent required? How do you obtain consent?
  - When and how should personal information be destroyed.
- ✓ Is there a record classification system?
- ✓ Is there a record destruction schedule? Does it outline how personal information should be destroyed?
- ✓ Is there a policy regarding the use of personal e-mail to conduct constituency business which involves personal information?
- ✓ Has each staff member in the office signed a confidentiality statement or agreement?

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 S4P 4B4

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