LEGISLATIVE ASSEMBLY
of BRITISH COLUMBIA

MEMBERS'
Privacy Guide

HOW TO MANAGE AND PROTECT PERSONAL INFORMATION

Office of the Law Clerk and Parliamentary Counsel
October 2024

Purpose

Members of the Legislative Assembly ("Members") receive a range of information in the course of their work from constituents, their constituency office staff, caucus staff, staff of government ministries and agencies, interest groups, fellow Members, and others in a variety of forms (letters, emails, texts, phone messages, etc.). This guide provides Members (and their constituency office staff) with information on how to manage and protect the personal or sensitive information they may receive or create in relation to their work as a Member, and to bring awareness to the supports available within the Legislative Assembly Administration.

In this document, a reference to a Member in relation to the Member's constituency office functions, includes the Member's constituency office and constituency office staff who assist the Member in carrying out the Member's constituency duties and responsibilities whether employed by the Member, retained on contract by the Member, or engaged as a volunteer by the Member.

This document is a guide containing recommended general best practices. The information contained in this document does not constitute legal advice. For legal advice or guidance in relation to a specific situation, please contact privacy@leg.bc.ca.

Government Records

This guide does not provide guidance with respect to management of records or protection of personal information created or received by a Member in their capacity as a member of the Executive Council. For questions regarding the management of records or protection of personal information created in a Member's role as a Minister or Minister of State, please refer to the following resources of the Government of British Columbia or consult with ministerial staff:

> Records Management Guides: Guidance for managing Minister's office records, and government information management requirements.
>
> Privacy & Personal Information in the Public Sector: Guidance for ensuring ministries meet legislative obligations and the government's responsibilities for protecting privacy.

Legislative Assembly Privacy Management and Accountability Program

The Office of the Law Clerk and Parliamentary Counsel is responsible for the Legislative Assembly's Privacy Management and Accountability Program. Through training and guidance on privacy related matters, the program ensures there are responsible and consistent privacy practices across all departments of the Legislative Assembly. The Office of the Law Clerk and Parliamentary Counsel is also available to provide privacy law advice, guidance and training to Members, as well as to caucus staff, upon request.

For questions about the Privacy Management and Accountability Program or assistance with privacy related matters, please contact privacy@leg.bc.ca.

In This Document

(Click on topics below to jump to relevant page)

What is Personal Information?

Personal information is recorded information about an identifiable individual, other than business contact information (information intended to allow an individual to be contacted at their place of business).

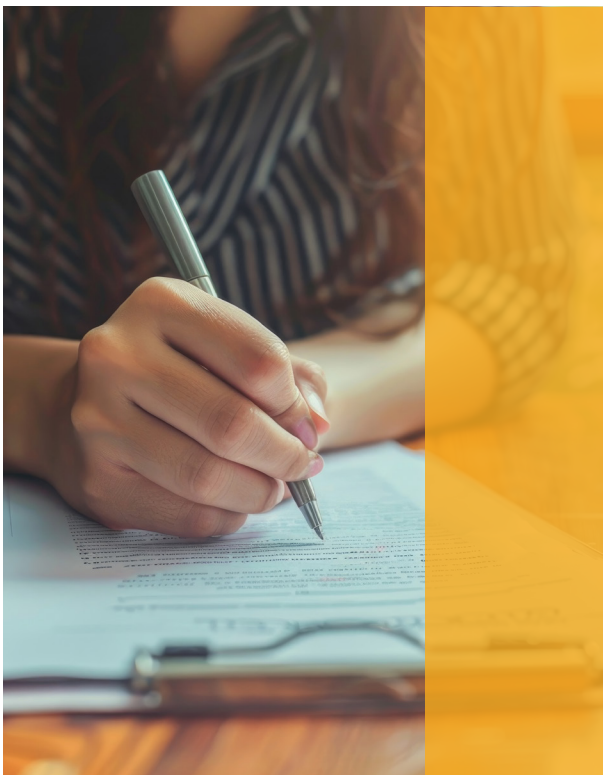
Personal information includes, but is not limited to:

- Name, age, gender, weight, height
- Home address, personal email address, personal phone number
- Religion, race, ethnic origin, sexual orientation
- Medical information and health care history, including physical or mental disability
- Employee ID number
- Marital or family status
- Educational, financial, employment information
- Criminal history
- Personal views or opinions

An individual does not need to be directly identified for the information to constitute personal information.

Depending on the context, a collection of seemingly innocuous information, when combined from different sets of data, can create the potential to identify an individual, constituting personal information.

Personal information is collected in the day-to-day interactions a Member has with the public, businesses and public bodies. Personal information may also be collected in interactions with other Members and their staff. The possible risks that disclosure of the information may pose to the individual the information is about, should be considered prior to any disclosure.



Why is the Protection of Personal Information Important?

Privacy has been described as "a fundamental right."[1] At its core, informational privacy is a person's right to control who knows and has access to their personal information. When an individual loses this control, they may feel violated and vulnerable.

The inability to control one's own information may also pose additional risks to the individual such as bodily harm, humiliation, damage to reputation or relationships, loss of employment, loss of business or professional opportunities, financial loss, identity theft, negative effects on a person's credit record, as well as damage to or loss of property.

[1] https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/ar_202324/

Privacy Legislation

FOIPPA

The *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, (FOIPPA) is British Columbia's public sector privacy legislation, which applies to all public bodies. FOIPPA establishes a right, with limited exceptions, for the public to access records in the custody or under the control of a public body and sets out rules for the collection, use and disclosure of personal information by a public body.

FOIPPA does not apply to the Legislative Assembly or to a Member's work as a Member; however, FOIPPA may be looked to as a guide to best practice for the Legislative Assembly. It is recommended that Members familiarize themselves with the provisions of FOIPPA that relate to collecting, using, storing, disclosing, and destroying personal information.

- FOIPPA applies to the work of a Member who is a member of the Executive Council when acting in their capacity as a Minister or a Minister of State.

- FOIPPA will also apply to a Member when acting as a member of a committee or task force reporting to a Minister or to a Member carrying out a function on behalf of a Minister (e.g., as a Parliamentary Secretary).

- FOIPPA applies to any public bodies that a Member may be in contact with when helping a constituent. Anything that is shared with a public body may be subject to an access request under FOIPPA. See the resources section for Legal Services guidance on dealing with outside entities.

Privacy Act

The *Privacy Act*, R.S.B.C. 1996, c. 373, creates a tort (a civil wrong) if a person wilfully and without any right, violates an individual's privacy. This can happen by sharing personal information without proper authorization or by accessing personal information without any specific business purpose.

- The Privacy Act is a law of general application in British Columbia and could be applicable if a Member wilfully violates someone's privacy, thereby exposing the Member to civil liability.

- This liability could extend to circumstances where an outside party has unlawfully obtained access to personal information that the Member's constituency office holds; so appropriate safeguards, including staff training, are crucial.

Collection of Personal Information

Members will obtain personal information of many individuals during the course of their work. This information may be collected from discussions or written communication with those individuals but may also include notes that a Member has taken.

When collecting personal information, it is advised that only the minimum amount of information needed, be collected. By doing so, fewer records are created for the Member to manage, and this reduces the amount of information that may be exposed in a privacy incident.

When a constituent reaches out to a Member as their representative, they are providing implicit consent for the Member to collect, use, and disclose personal information in a manner that a reasonable person would expect. However, it is recommended that constituents are informed of the information that the Member's constituency office will be collecting and the purpose for the collection (e.g., the information is collected to better assist the constituent with the matter).

Did You Know?

Video surveillance systems collect personal information. That is why Member's constituency offices are provided a sign noting that the constituency office is being monitored for security purposes. Please ensure that this sign is posted in a visible, unobstructed location near the entrance of the office.

Notice and Consent

- If a constituent emails a Member's constituency office, the response should outline that information contained in the email will be saved by the constituency office to assist the individual with the matter that they have written about.

- If a constituent attends a Member's constituency office in person, it is recommended that the constituent be asked to sign a consent form describing the issue they are seeking assistance with, what information the office may be collecting, why the office is collecting it, and how the information will be used.

- If the constituent is not comfortable signing a consent form, it is acceptable to obtain verbal consent. In such cases, a note of what information was discussed as part of that consent, and that the constituent verbally provided the consent, should be noted.

If consent is obtained, the Member should ensure that, in all cases, the constituent is informed that they can revoke their consent at any time and can request that the their file be closed; however, they should also be informed that, depending on the nature of the issue the Member's constituency office is assisting with, failure to provide consent may mean the Member and their constituency office staff are unable to assist them.

Use of Personal Information

Once personal information is collected, it should only be used for the purpose for which it was collected or for a consistent purpose (i.e., in a manner that a reasonable person would expect).

If, for example, a person has written to note a concern about the rise of hate-crimes against their religious community and is seeking a Member's help, they would reasonably expect that the Member may contact them regarding the issue. However, using the individual's personal information relating to their religion to send a card to celebrate a holiday or another matter related to their faith would be inappropriate, as the person would not expect their information to be used in this way.

Disclosure of Personal Information

If assisting a constituent requires disclosure of the constituent's personal information to a private organization, public body, or another individual, verbal consent or written notice may not be enough.

It is recommended that the Member seek the constituent's consent in writing and inform the constituent of:

- The purpose of the disclosure
- What information will be disclosed
- Where the information will be disclosed

The issues for which a constituent may seek assistance may be highly sensitive. It is therefore important that a Member ensure that the utmost discretion is used when talking about these issues or this person, especially in a public setting. Members should ensure that they have received the consent of the individual before sharing or discussing their identity, personal information, or anecdotal story.

A Member may find themself in a situation where there are compelling circumstances that require disclosure of personal information for safety or security purposes. This could include circumstances involving a child protection issue or suspected criminal conduct that require disclosure to a law enforcement agency. Members may contact Legal Services at legalservices@leg.bc.ca for advice prior to making any such disclosure. In the event the disclosure is required before a Member can contact Legal Services, a Member may contact Legal Services after the disclosure to discuss the situation.

Members may contact privacy@leg.bc.ca with questions or concerns about potential disclosures.

Dealing With Public Bodies

At times, providing assistance to a constituent may require that a Member contact a public body in order to collect information on behalf of the constituent. Section 33(3)(e) of FOIPPA allows a public body to release an individual's personal information to a Member assisting the individual in resolving a problem.

- The public body will generally require a signed Certificate of Authority before it will release personal information.
- If the constituent is seeking assistance on behalf of another individual, a Third Party Consent to Disclose Personal Information to an MLA may be required.

Important: A form only authorizes the public body to release personal information about the person indicated on the form. If the record contains any personal information about a third party, the record in whole or in part could be withheld.

By collecting information from a public body, a Member may receive highly sensitive personal information. It is important that a Member ensure this information is treated as confidential and copies are not kept longer than necessary to assist the constituent. A Member should ensure there is appropriate review of each request to ensure that proper authorization from the constituent was obtained.

A Member should only use personal information for the purposes of assisting the constituent or where consent for an alternative use is provided by the constituent. This information should not be disclosed to any other party except as required and appropriate to assist the constituent in resolving their issue.

The Government of British Columbia's Guideline for MLAs and Constituency Assistants provides guidance for requesting personal information on behalf of a constituent from a public body.

Safeguarding Personal Information

Once personal information has been collected, it is important to ensure that the information is reasonably safeguarded - the information should only be accessible to individuals with the proper authorization who need access to the information.

Physical records should be locked away in a filing cabinet and computers should be password protected and locked when left unattended. Special caution should be exercised when using unencrypted portable storage devices (i.e., external hard drives, flash drives, memory sticks). The Information Technology Department is available to assist Members in making sure that their office records system is well safeguarded.

Privacy incidents are most frequently caused by human error. Good privacy practices should be integrated into daily constituency office operations – including:

- Double checking that emails are being sent to the intended recipient
- Ensuring that personal information is not left in a visible location such as on a counter or near a window
- Only allowing staff access to files on a need-to-know basis

Limited Retention

When a constituent's matter has been resolved, or there has been no contact with the constituent for 12 months, the constituent's file should be closed. If there is a concern that the records should be preserved for legal purposes, please contact Legal Services at legalservices@leg.bc.ca. Any records containing personal information collected on behalf of the constituent, may be provided to the constituent.

When closing a file or destroying a constituent's personal information at the request of the constituent, it is critical that all copies of the constituent's personal information is securely destroyed and that all possible locations the information may have been stored be checked, including:

- Email communications with the individual or about the individual
- Customer Relationship Management software (CRM)
- Digital files saved on a computer or external device
- Text or messenger communications
- Physical records

A Member can retain any records that the Member or the Member's constituency office staff generated, business contact information, any signed certificates of authority, and signed consent forms. These records may be maintained by the constituency office as long as they are needed for legal, operational, or other business purposes.

Questions or concerns regarding safeguarding or destroying records may be directed to Client Care who will liaise with the relevant departments.

Transferring Information to an Incoming Member

Upon the dissolution of a Parliament, Members cease to be a Member. Following dissolution and during the election period, limited assistance may be provided to constituents at the discretion of the outgoing Member, but no active or new case work may be undertaken.

At Dissolution

For any files that remain active (i.e., the Member's office has been contacted by the constituent within the last 12 months or their issue has not been resolved), it is advisable for the Member to seek the consent of the constituent to transfer their personal information to the next Member via a signed consent form. A Member who is seeking re-election may decide to hold off taking this step until the results of the election are known.

Consent to Transfer

In the event that the Member is not seeking re-election, or a new Member is elected, a consent form is required for the outgoing Member to transfer the file to the incoming Member. The continuity of service is for the sole benefit of the constituent.

- There may be cases where a constituent is unsure if they may want assistance from a new Member. The constituent should be advised that they can revoke their consent at any time (this is noted on the consent form, but it is recommended that this be clearly reiterated to them).
- In the event the constituent does not want their information passed on to the incoming Member, the constituent can request the return or destruction of any personal information the outgoing Member has collected from an organization or public body on their behalf.
- The outgoing Member should consider whether the notes, files, emails, and entries into CRM that comprise an active file should be released to the constituent, passed to an incoming Member, or destroyed.

All constituent files contained in digital accounts (e.g. email) or repositories (e.g. the cloud) provided by the Legislative Assembly Administration are slated for destruction by default following a general election. Therefore, if an outgoing Member does not have a constituent's consent to transfer an active file and the constituent has not requested that the Member return their records, any records that were in the custody of the outgoing Member will be destroyed by the Information Technology Department as part of the election transition process.

Note: In the event of a Member's resignation, recall, or death, Legal Services will provide advice, as appropriate, regarding the management of information and records of a Member's constituency office.

Privacy Incidents

A privacy incident occurs when personal information is disclosed, accessed, retained, used, or disposed of without authorization. A privacy incident can include the theft of a device or password that gives someone unauthorized access to personal information, accidentally sending an email, phone message, or documents containing personal information to the wrong person, or a person accessing information without a legitimate business need.

Consequences of a privacy incident can cause significant harm by:

- risking identity theft and possibly impacting current and future financial matters;
- compromising personal safety, especially where a residential address is disclosed; and
- harming the reputation of the individual whose personal information is improperly used or released.

If a Member believes that a privacy incident has occurred, the following steps are recommended:

1

Containment – Take steps to contain the incident. For example, if the incident is due to an email being sent to the wrong person, request that the recipient destroy the information, or if a package of materials was sent to the wrong recipient, attempt to have that package returned.

- If the disclosed information cannot be secured, contact Legal Services at legalservices@leg.bc.ca for advice.
- If the incident is due to a cyber incident (even if only suspected), please contact the Information Technology Department at servicedesk@leg.bc.ca.

2

Assessment – Once the incident has been contained, assess the severity of the incident. Consider the sensitivity of the information, how widespread the disclosure was, who may have accessed the information, and the risk of harm.

Privacy Incidents (cont.)

3

Notification – Once the potential harms are determined, determine who, if anybody, should be notified that their personal information was disclosed.

For example, an email sent to another Member in error who quickly confirms that the information was received in error, that it was not shared and immediately deleted may not necessitate a notification to the individual. However, if a paper file containing personal information (such as financial information) is lost or stolen, notification will likely be required.

In the event that notification is required, the impacted individuals should be told:

- the date the incident happened
- the date the incident became known
- a brief description of what occurred, including the nature of the information
- the contact information of a person that can help with the person's concerns
- what steps will be taken to mitigate the likelihood of future incidents
- what, if anything, the person can do to take steps to reduce the risk of harm

4

Prevention – Once the incident has been resolved, the Member should debrief with their constituency office staff and consider what lessons can be learned from the incident and how similar incidents can be prevented in the future.

The Privacy Analyst is available at privacy@leg.bc.ca to assist in the event of a privacy incident.

Resources

RELEVANT LEGISLATIVE ASSEMBLY MEMBER POLICIES AND RESOURCES:

- **Policy 7335 – Member Records**: Establishes requirements for the management of records collected or created by a Member
- **Policy 5410 – Information Security**: Addresses reporting information incidents
- **Policy 7410 – Appropriate Use of IT Resources**: Addresses rules for the use of and care required for Legislative Assembly provided IT resources
- **Guide to Dealing with Outside Entities**: Provides guidance for Members as they share records with outside organizations or public bodies that are subject to privacy and access laws