Module 1: **The Basics**

TIP SHEET

The Freedom of Information and Protection of Privacy Act (FOIPPA) is the privacy and access legislation that governs all public bodies in B.C. As a public body employee, contractor, or service provider, you must ensure that you manage information in accordance with FOIPPA.

Four domains of information management

Records management, access to information, privacy, and security all play an important role in the effective stewardship of information held by public bodies.

1. **Records management:** Records management is the system an organization uses to effectively capture and maintain information associated with business activities and transactions. Records include both print and digital records of such items as email, documents, maps, and handwritten notes.

2. **Access:** Public bodies are accountable to the public for ensuring access to records under the custody or control of the public body, with limited exceptions. This includes individuals' right of access to their personal information.

3. **Privacy:** Privacy is protected by public bodies treating personal information responsibly and lawfully. This includes ensuring personal information is collected, used, and disclosed appropriately.

4. **Security:** Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability of that information or system.

Where to go for help

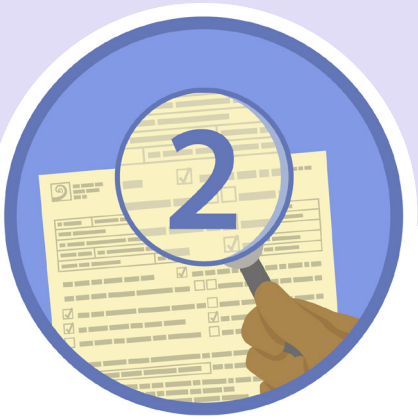
- **Your supervisor** can help you determine when and how you are authorized to collect, use, and disclose personal information in the course of your work.
- **Your privacy officer** is the point of contact for privacy in your organization and can help you understand and resolve privacy issues, as well as navigate such processes as completing Privacy Impact Assessments.
- **Your FOI coordinator** is an expert in access to information and can help you navigate responding to FOI (access) requests.
- **The corporate privacy office** within the Ministry of Citizens' Services provides services to government and the broader public sector, including privacy training and resources such as the Privacy & Access Helpline.
- **The Office of the Information and Privacy Commissioner (OIPC)** provides independent oversight and enforcement of B.C.'s access and privacy laws, including the Freedom of Information and Protection of Privacy Act (FOIPPA). The office also has resources on privacy and access for public bodies, organizations, and individuals.

Custody and control

FOIPPA applies to all records in the custody or under the control of a public body, unless explicitly out of scope of the Act.

- **Custody** of a record means physically possessing that record. It normally includes responsibility for, access to, and security of, that record, as well as managing, maintaining, preserving, and disposing of it.
- **Control** of a record refers to the authority to make decisions about how a record ought to be managed throughout its lifecycle. If a public body has control of a record, even if it does not have custody of that record, the record still may be subject to FOIPPA. For example, a public body's records that rest with one of its service providers would be under its control but may not be in its custody.

Protection of Privacy
TIP SHEET



The Freedom of Information and Protection of Privacy Act (FOIPPA) works to protect personal privacy by preventing the unauthorized collection, use, or disclosure of personal information by public bodies.

Personal information

Personal information is recorded information about an identifiable individual other than their business contact information. It includes information about an individual's education history, employment history, health history, and even their personal opinions. It may also, depending on the circumstances, include other information, such as the person's name, home address, and DNA.

Questions to consider when handling personal information:

1. Why do I need the personal information?
2. Am I authorized to collect the information at this particular time (for example, is all of it directly related to and needed for the task at hand)?
3. What am I doing to protect the information I handle?
4. Am I using the information for a purpose consistent with why it was collected? If not, have I obtained consent?
5. Am I authorized to share the personal information?

Authorities

If a public body wants to collect, use, or disclose personal information, it needs to have an authority under FOIPPA to do so. These authorities outline the specific circumstances in which public bodies can **collect**, **use, and disclose** personal information.

As a public body employee or service provider to a public body, you may only access personal information that your public body has **collected in circumstances where it is required for your work and authorized under FOIPPA**. You may not access it for your own purposes.

Privacy tools

Privacy impact assessment (PIA)	Helps identify possible impacts to individuals' privacy from new and existing initiatives
Information sharing agreements (ISAs)	Documents the terms and conditions of the exchange of personal information in compliance with legislation
Information Sharing Code of Practice	Supports responsible and lawful personal information sharing and the protection of personal information
Privacy schedule in contracts for service providers	Ensures service providers maintain the privacy standards for personal information set by FOIPPA

Disclosing and storing sensitive personal information outside of Canada

A public body must complete a supplementary assessment for disclosures outside Canada when a program, project, or system includes *sensitive* personal information that is *stored* outside Canada. For more information, see **Guidance on Disclosures Outside of Canada**.

Information incidents/privacy breaches

An **information incident** is an event (or series of events) involving the collection, storage, access, use, disclosure, or disposal of confidential or personal information that threatens privacy or information security, and/or contravenes law or policy.

An information incident that threatens privacy is called a privacy breach and includes the theft or loss of personal information, or the collection, use, or disclosure of personal information that is not authorized by FOIPPA. A privacy breach may be accidental or deliberate.

In future, there will be a requirement where if there is a reasonable risk of significant harm to an individual as a result of a breach, that the head of the public body notify the affected individual and the Office of the Information and Privacy Commissioner (OIPC). This is currently the requirement for ministry public bodies. Notification allows the individual affected by a privacy breach to take steps to mitigate possible harm.

Responding to an information incident/privacy breach

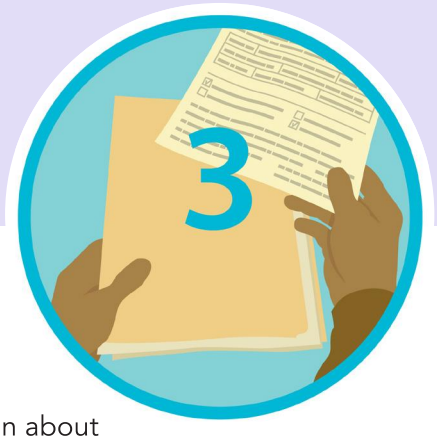
If you suspect an information incident/privacy breach has occurred, your first step is to immediately report the incident to the appropriate contact.

- **Public body employees** report to your supervisor, privacy officer, or other designated contact in your organization.
- **B.C. government employees, contractors or service providers** call 250 387-7000 or toll-free at 1-866-660-0811 (select option 3).

Once reported to the appropriate contact in your organization, they will help you through the remaining **steps to respond to the incident**.

In situations where containment of the information is possible (such as requesting an unintended recipient double-delete an email), consider making this request as soon as possible and advise the appropriate contact of steps taken.

Module 3:
Access to Information
TIP SHEET



Under the **Freedom of Information and Protection of Privacy Act (FOIPPA)**, individuals have a right to access:

- Their own personal information held by public bodies
- General information held by public bodies, including information about government operations, programs and services, with limited exceptions

Access to information is:

- A foundational democratic principle, supported by FOIPPA
- Permitted or required by law
- Granted based on a line-by-line review of the record to ensure that the information is legally appropriate for release to the person requesting it

Anyone, including individuals, political parties, media, law firms, businesses, researchers, interest groups, or other governments, may make an FOI request. An applicant may submit a request to access a record in any written format. If the applicant is making the request on behalf of another person, the applicant must also provide written permission from the other person (unless permitted by the **FOIPP Regulation**).

FOI exceptions to disclosure

While the public body's intention should always be to release information wherever possible, FOIPPA lists a number of **exceptions** to the release of information. These exceptions provide public bodies with the authority to sever (take out) information from a record before releasing it. The person who made the request retains the right to access the remainder of the record.

Mandatory exceptions	Discretionary exceptions
Public bodies **must** withhold information: • Subject to cabinet confidences • Harmful to the interests of an Indigenous people • Harmful to the business interests of a third party • Harmful to a third party's personal privacy	Public bodies **may** withhold information that is: • Subject to local public body confidences • Policy advice or recommendations • Legal advice • Harmful to: law enforcement; intergovernmental relations or negotiations; financial or economic interests of a public body; conservation of heritage sites; or, individual or public safety

Module 3: **Access to Information**
TIP SHEET

In general, once a public body receives a request, the public body:

1. **Reviews the request** to clarify and/or determine if the information being requested is already available to the public
2. **Confirms receipt of the request.**
3. **Assigns a file number or method** of tracking the request.
4. **Establishes fees** to charge for the request (if any). Public bodies must not use fees to discourage an applicant from proceeding with a request.
5. **Searches for the record** anywhere there is reason to believe recorded information relevant to the request might be stored—and document the details of the search.
6. **Retrieves the record.**
7. Completes a **line-by-line review** of the information to determine what information (if any) may or must be severed before release. See **FOI Exceptions to Disclosure**.

   If some information must be severed, the public body must give the reasons, in writing, for refusing access to that information, as well as:

   - The FOIPPA provision(s) on which the refusal is based
   - Contact information for an employee who can answer the applicant's questions
   - Information about how to ask the Office of the Information and Privacy Commissioner to review the decision.
8. **Provides results to the applicant** within a maximum of 30 business days from the time the request was received.

Third parties: A public body may receive a request for access to a record that, although in the public body's custody, was either not authored by the public body or relates to a third party. If the public body thinks there may be harm in giving access to that information, it should consider whether they may or must consult with the third party before making a decision.

Extensions: FOIPPA permits public bodies to take a 30-day extension for a number of reasons (s. 10). The Office of the Information and Privacy Commissioner (OIPC) may also authorize a public body to take an extension for periods longer than 30 days for the same reasons, or if the OIPC otherwise considers that it is fair and reasonable to do so.

Proactive disclosure: Public bodies are required to establish categories of records that are in their custody or control that are available to the public without an FOI request (s. 70 and 71) and to immediately disclose information where it relates to a risk of significant harm to people or the environment, or where disclosure is clearly in the public interest (s. 25).