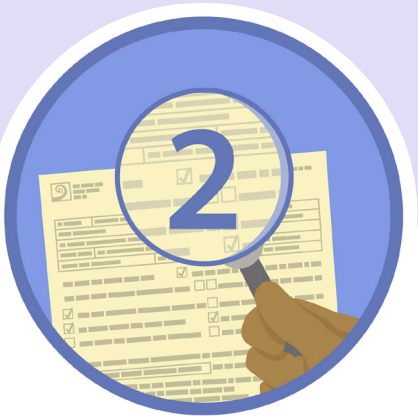
Module 2:
Protection of Privacy
TIP SHEET



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.

There is a privacy breach notification requirement in FOIPPA. If there is a reasonable risk of significant harm to an individual as a result of a breach, the head of the public body must notify the affected individual and the Office of the Information and Privacy Commissioner (OIPC). 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.