**Generic content for message to employees to raise awareness of privacy obligations**

**Personal Information and Privacy Breach Awareness**

The following is an example of an internal message that can be shared to federal employees to:

1. Strengthen awareness about what constitutes “personal information” under the *Privacy Act;* and,
2. Remind them of their obligation to protect the personal information that is collected in federal programs and activities
3. Provide information about the steps to take if they think a privacy breach has occurred.

The message is intended for employees of federal institutions that are subject to the *Privacy Act* and is designed to be customized as required in order to best communicate with the employees in your institution.

-------------------------------------------------------------------------------------------------------------------------------

**Protecting Privacy is Everyone’s Responsibility**

As federal employees, we are responsible for protecting the personal information that we collect in our programs and activities. This includes personal information about the Canadians we serve, about our colleagues, and even about ourselves.

**What is considered “personal information”?**

The *Privacy Act* defines personal information as “information about an identifiable individual that is recorded in any form”. Personal information can range from an individual's nationality, age or marital status to their medical records, IP address, browser history, or fingerprints. More examples of the types of information considered to be personal under the *Privacy Act* can be found [here](https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html#h-3).

Federal institutions collect personal information in many contexts, for example:

* collecting personal information such as name, address, age, nationality, etc. from applicants in order to determine eligibility for federal programs and benefits;
* obtaining a citizen’s Social Insurance Number or other identifying number assigned to an individual in order to establish a login credential for federal services offered online;
* receiving and replying to e-mails and letter mail containing information about an individual’s application status for a federal program or benefit;
* obtaining name, address, age, nationality, fingerprints, financial information, or other personal information when applying for federal security clearance;
* entering performance-related information in the federal government Public Service Performance Management Application, and;
* collecting details about pay and benefit entitlements of government employees.

**How should I protect personal and other sensitive information?**

As a <insert institution name> employee, you are responsible for following Treasury Board of Canada Secretariat (TBS) policies and guidance relating the protection of personal information. This includes ensuring personal information is:

* kept out of public sight in your workspace;
* shared only with colleagues who have a need to know
* secured by using proper labelling, storage in approved locked containers, and is only transmitted physically or electronically by approved means (including the use of appropriate encryption)
* protected by using strong passwords for your login and screensaver;
* protected in systems and databases through access controls that ensure only authorized employees can access the information

Failure to protect personal information can result in a privacy breach.

**What is a privacy breach?**

A privacy breach is the improper or unauthorized creation, collection, use, disclosure, retention or disposition of personal information.

**How is a privacy breach caused?**

Most often, privacy breaches are caused by the improper use or disclosure of personal information. A breach may occur within an institution or off-site. It can be the result of unintentional errors, by a failure to protect personal information under your control, or by malicious actions by employees, third parties, or bad actors.

**What are my obligations if I suspect a privacy breach has occurred?**

If you suspect or learn that a privacy breach has occurred, the first step is to contact the ATIP Office <insert alternate details here if applicable>. This group will advise you on what actions to take and will liaise with other internal stakeholders, depending on the nature of the breach.

The first priority will be to stop and contain the breach, which may entail actions such as:

* <insert alternate details here if applicable>
* Removing, moving or segregating exposed information or files to prevent further wrongful access;
* Shutting down the web site, application, or device temporality to permit a complete assessment of the breach and resolve vulnerabilities, and;
* Attempting to retrieve any documents or copies of documents that were wrongfully disclosed or taken by an unauthorized person

***Do not hesitate or wait to report a possible privacy breach. The sooner a privacy breach is identified and reported, the more likely it is that the injury can be prevented or minimized.***

After breach containment measures are taken, the ATIP office <insert alternate details here if applicable> will work to ensure that:

* <insert alternate details here if applicable>:
* A full assessment of the breach is conducted;
* Affected individuals and other internal and external stakeholders are notified of the breach, as appropriate;
* Mitigation and prevention measures are taken to safeguard against similar future breaches, and;
* Lessons learned from the breach are shared appropriately.

More information about privacy breaches and how they should be managed is available on our website <insert institution’s link>. If you have not yet done so, please familiarize yourself with the information, procedure, and contact information contained in this guidance so that you can be ready to react in a timely manner in the event of a privacy breach.

Thank you for your continued vigilance and for remembering that ***protecting privacy is everyone’s responsibility.***