**Protecting Personal Information When Working Remotely**

**Context**

This guidance is intended to support public servants to protect personal information and prevent privacy breaches when working remotely.

Working remotely has become the new norm for many public servants. While this offers new opportunities to explore more digital ways of working, working remotely has changed the way public servants create and manage information, and collaborate with others. The changes have presented new challenges to established workplace processes, information management practices, service delivery, and internal collaboration that are usually protected within the security of Government of Canada facilities and network environments.

When working remotely, the *Privacy Act* and federal privacy policies, outline the requirements for federal institutions and employees to protect the personal information under their control. This includes when working remotely. Additionally, under the *Policy on Service and Digital*, privacy must be addressed in the context of any plan or strategy to manage departmental information or data.

The information provided below offers some tips and helpful resources to protect personal information and prevent privacy breaches when working remotely.

|  |
| --- |
| **Privacy Breaches**  A privacy breach is the improper or unauthorized creation, collection, use, disclosure, retention or disposal of personal information.  **What to do if you suspect a privacy breach has occurred:**  You must report any suspected privacy breach to your institution’s ATIP office and follow your institution’s plans and procedures for privacy breach management. The ATIP office will be able to provide you with more specific information and the next steps.  The table below outlines scenarios and considerations to guide you in preventing and managing potential privacy breaches when working remotely. |

**Related References:**

* [Interim Policy on Privacy Protection](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510)
* [Policy on Government Security](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578)
* [Directive on Service and Digital](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32601)
* [Guidelines for Privacy Breaches](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26154)

Other content specific links are found directly in the text below.

|  |
| --- |
| **Scenario 1:** In remote work situations, employees may use new digital collaboration or productivity tools to connect with others or advance their work. |
| ***What to consider?***  *It is important to note that some personal information about public servants such as your name, title, classification, work email address and work phone number is not considered to be protected personal information by the Privacy Act.*  *Important information and tips about the use of collaboration tools can be found in the* [*Guidance for the Secure Use of Collaboration Tools*](https://www.gcpedia.gc.ca/gcwiki/images/2/28/Guidance_for_the_Secure_Use_of_Collaboration_Tools.pdf) *and on the* [*Secure Remote Working wiki*](https://wiki.gccollab.ca/Secure_Remote_Working)*.* |
| ***Q: Do I have to provide personal information such as my personal phone number or personal email address in order to use digital collaboration tools in the workplace?***  A: No. Productivity or collaboration tools used in carrying out your duties and functions as a public servant should only require work-related contact information.  ***Q: When using collaboration tools or virtual meeting tools, I may need to discuss sensitive personal information about an identifiable individual. Is that appropriate?***  A: It is often necessary to discuss sensitive personal information in the course of your duties and functions as a public servant. For example, Labour Relations employees discuss sensitive personal information with managers. When using digital tools to communicate personal information, before using a new tool, contact your IM, security and privacy officials to ensure that the specific tool is appropriate in your situation.    ***Q: I am invited to use a virtual meeting tool that uses video images. I am not comfortable sharing my video image. Does the Privacy Act have any requirements that I should be aware of?***  A: An image is personal information when it is about an identifiable individual and recorded in any form. Therefore, if your image is being recorded through the tool it must be protected in accordance with the *Privacy Act* and related policy instruments.  If you are not comfortable using the video features of a virtual meeting tool you should first discuss your concerns with your manager. They will be able to provide you with more assistance on the best way forward. Often, virtual meeting tools have features that allow for participation without using the video feature.  ***Q: I have installed home assistants (Google, Alexa, etc.) throughout my house, can I still telework?***  A: Yes, but you should take precautions against inappropriate disclosures of personal information at all times when working remotely. This may include removing or turning off the passive listening device from your workspace. The *Privacy Act* and government security and privacy policies require the protection of personal information and passive listening devices could pose an additional risk. Please contact your institution’s ATIP office and Chief Security Officer for further information. You can also visit the [GetCyberSafe](https://www.getcybersafe.gc.ca/cnt/rsks/ntrnt-thngs/hm-en.aspx) website for tips on securing your online devices at home. |

|  |
| --- |
| **Scenario 2:** In remote working situations, employees may bring hard copy documents containing personal information about an identifiable individual into their home environment. |
| ***What to consider?***  *To prevent privacy breaches from occurring in your telework environment you should have a dedicated area where you can reduce the entry of incidental visitors (E.g.: family members, guests, workers). Documents with personal information should be stored appropriately and, when no longer needed, destroyed appropriately. Please refer to the* [*Directive on Security Management - Appendix J: Standard on Security Categorization*](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32614)*,* *and/or contact your institution’s information management and security offices for further detail.*  *Keep in mind that, as per the Directive on Service and Digital, CIOs are to ensure that* ***digital systems******are the preferred means*** *of creating, capturing and managing information.* |
| ***Q: What is the security designation of personal information?***  A: That depends on the nature of the personal information. For instance, contact information about an identifiable individual is typically designated as Protected A while contact information about an identifiable individual who is a confidential informant for law enforcement is typically considered Protected C.    Regardless of the security designation of the personal information, any inappropriate creation, collection, use, disclosure, retention or disposition of the personal information is a privacy breach.  ***Q: How do I know the proper techniques for securing and transporting hard copy records containing personal information?***  A: Information specific to the secure storage, transport, transmittal and destruction of documents when working remotely is best obtained from your manager or alternatively, your institution’s security and IM offices. It will be important that the carrying case, lock, mode of transportation, and the at-home storage be appropriate for the security designation of the information. The following [link](https://www.canada.ca/en/government/publicservice/covid-19/managing-government-information-working-remotely.html) also has further guidance on managing information while working remotely. |

|  |
| --- |
| **Scenario 3:** In remote working situations, employees may need to deliver services in a new way, while continuing to protect personal information. |
| ***What to consider?***  *To protect against privacy breaches while delivering services remotely you should consider how the change to the delivery model affects the flow (creation, collection, use, disclosure, retention, disposal) of personal information and its management, and work with your ATIP office to determine if these changes require a Privacy Impact Assessment. Please refer to the requirements in the* [*Interim Directive on Privacy Impact Assessment*](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309) *or contact your institution’s Access to Information and Privacy Office for further detail.* |
| ***Q: How does changing service delivery from an in-person model to a remote model affect the management of personal information?***  A: That depends on the institution as well as the program or service and tools employed in the process. For instance, some services may use new technology or third-party providers to deliver information to the service recipient. This could result in a new and possibly unauthorized creation, use, disclosure, retention or disposal of personal information causing a privacy breach. For example, if a third-party kept a copy of the data used in the service for their own commercial purposes, this could be considered an unauthorized retention or use of personal information causing a privacy breach. Alternatively, a new tool or technology could require the collection of additional personal information. If not directly related to the program or activity this new collection could constitute a privacy breach. To assess changes to business processes and their impact on the management of personal information, service delivery programs should work with their information management offices and ATIP offices to determine whether a Privacy Impact Assessment is required.  ***Q: How do I know if the new changes to a business process are aligned with privacy requirements?***  ***A:*** Privacy Requirements are found in the *Privacy Act*, TBS Privacy Policies, and institution-specific legislation and policies. Please work with your information management and ATIP office to discuss any changes to business processes that affect the management of personal information to ensure privacy will continue to be protected. |

|  |
| --- |
| **Scenario 4:** In remote situations employees need to ensure that they are saving records to the appropriate corporate repositories. |
| ***What to consider?***  *Inappropriate retention and disposition of personal information can lead to privacy breaches. To prevent this from occurring in your remote working environment you should ensure that you are saving records of business value to your approved corporate repository. This includes classifying them appropriately according to your corporate file plan and attributing the appropriate security designation to each record and ensuring that the repository is accredited to store, at a minimum, the same designation as the document. Please refer to the* [*Directive on Service and Digital*](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32601) *or contact your institution’s information management and security offices for further detail.* |
| ***Q: Can I save records containing personal information locally on my work computer when working remotely?***  A: No. Your work computer is not an official corporate repository. There may be times when it is necessary to do so, but this should only happen when necessary and for a limited period. For example, should you lose network connectivity and need to save the record, saving the record locally is permitted provided that when you connect to the network again, the record is saved in the appropriate repository.    ***Q: Are there any special electronic repositories in which to save personal information?***  A: It depends. Personal information can be saved in any electronic corporate repository if it is accredited to the level of the security designation of the record and otherwise meets Government of Canada information management requirements. In most cases, personal information is appropriately saved into the approved repository. An exception to this could be when the security designation of the personal information exceeds the accreditation of the repository. For example, when saving personal information about a confidential informant. Corporate repositories are typically not appropriate in this case, but the information must nonetheless be managed as a strategic asset. In this scenario, your institution’s information management office can provide you with more detailed instructions. |