MESSAGE FROM THE NUNAVUT INFORMATION AND PRIVACY COMMISSIONER ON PROTECTING PRIVACY WHILE WORKING FROM HOME

As the GN and Nunavut public bodies respond to public health risks posed by the Covid-19 Pandemic, and shift service delivery to a "work from home" model, employees must be aware that client's rights to privacy have not changed. The provisions of the *Access to Information and Protection of Privacy Act* and basic privacy principles continue to apply to the collection use and disclosure of personal information (PI). The Act that recognizes that there may be emergent situations in which information can be collected, used and disclosed in ways that would not otherwise be acceptable, but this must still be **limited** to that which is **needed** to achieve the **reasonable** purpose of the collection, use or disclosure.

The obligation of the GN to protect and secure personal information does not change. Employees should continue to apply best practices and when handling PI. Employees must ensure that the collection, use or disclosure is limited to that which is necessary and reasonable to ensure the completion of their work.

Employees should be aware of and continue to apply these principals. Employees should also take certain measures necessary to protect PI while working from home. Employees continue to be responsible for the privacy and security of information they use while they work from home, and to take steps to prevent unauthorized access, loss and theft of PI.

Wherever possible:

- Paper records containing PI should not be taken out of offices. If records need to be removed from the office they must be protected using approved protocols for transporting paper documents (double secured, displaying the contact information of the originating department, marked confidential). Never leave electronic devices or papers unattended during transport
- Only electronic devices that have been approved by management should be used.

- Any electronic device used should be appropriately protected and updated.
- Use only approved means of storing and transmitting PI (don't use gmail, Hotmail or Dropbox)
- All electronic devices should be encrypted, whenever possible.
- Paper records and electronic devices on which PI are stored should be secured at all times when not in use (this means locked in a location only accessible by the employee, e.g. filing cabinet)
    - PI needs to be protected at all times when in use to prevent unauthorized access:
    - Ensure information used at your work station is not viewable by others
    - Transmit information securely - this includes ensuring privacy for phone conversations
    - Secure information at the end of the day, even if you are not planning on leaving home
- Do not permit family members, or others to use electronic devices that are used for work purposes
- Do not share or allow to be shared your password to electronic devices used for work purposes
- Your organization should establish protocols to ensure tracking of paper records if it is necessary for these to leave the office, as well as tracking of issued electronic devices.
- Do not use any personal electronic device, application, or network without prior approval. Employees should be aware that use of personal devices, non-standard applications and other networks significantly increases risks of PI being intercepted by third parties, or otherwise compromised. GN approved devices, applications, and networks should always be used unless otherwise authorized.
- The "bad guys" are already taking advantage of the Covid-19 crisis. While working from home be **extra vigilant** of attempts by malicious actors who may attempt to trick well-meaning employees into disclosing passwords, clicking on links or attachments that could introduce malicious viruses or software into electronic devices and networks. If you receive communication that demands immediate action or you question the source or the content of the message you should **STOP**, and get advice before proceeding. Contact your manager or follow normal protocols for flagging malware or phishing schemes. **DO NOT** respond to

the malicious communication, do not click on links or attachments, and **DO NOT FORWARD** any communication you are wary of. Don't help the bad guys.

The Covid-19 virus will disrupt how we normally work, but the protections and rights related to privacy have not changed. At this time we thank all employees for respecting client's and coworker's rights and for taking measures as appropriate to continue to appropriately protect PI.

Our office will also be working remotely at this time, but will continue to provide limited services until we return to regular working conditions. If you have questions about access to information or privacy please contact your manager. You may also contact us by email at admin@atipp-nu.ca . Please be aware that because of restricted work conditions there may be delays in receiving responses from our office..

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner

* **Please note this document is meant as general guidance for employees, and is not legal advice nor official position statement.**