

Guidance for municipalities - working from home during Covid-19 Pandemic

The ATIPP Office has received questions about whether it is appropriate to take personal information home during the Covid-19 Pandemic.

Section 64(1)(a) of the Access to Information and Protection of Privacy Act, 2015 states:

The head of a public body shall take steps that are **reasonable in the circumstances** to ensure that personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure

Under **normal circumstances**, we would recommend that employees avoid taking personal information home unless absolutely necessary, however, given that many municipalities are asking staff/councilors to work from home in an effort to reduce the spread of COVID-19, taking documents home may be required.

If a municipality decides that officials will work from home, the ATIPP Coordinator in conjunction with the Town Clerk/Manager/CAO should determine what records are necessary for employees and councillors to take home, and how those records (both paper and electronic) will be managed and secured. Ideally, the ATIPP Coordinator would draft a temporary policy.

The following are common sense guidelines for working at home during the pandemic:

- Where possible, you should use your work email account and devices to conduct official business.
- Personal information must only be accessed on a need to know basis (as always).
- Keep a record of personal information which is removed from the Office. A table is included on the next page to use for this purpose. Be as specific as possible when indicating the information removed. For example:

Bob Smith – February 2020 Tax invoices – Originals – removed 3/31/2020 – returned 4/28/2020

- Take phone calls in another room away from others in the home.
- Ensure computers and other devices are password protected/encrypted, and lock these devices when taking a break or finishing work.
- If accessing work using your home internet wifi, ensure your wifi is password protected.
- Keep paper records in a locked filing cabinet if one is available.
- Ensure computers and devices are not left in plain view while you are away from the home and ensure doors are locked.

IMPORTANT: Public bodies are still legally required to report all privacy breaches to the Office of the Information and Privacy Commissioner

This list is obviously not exhaustive, but rather a starting point – when creating a policy for your town, ensure to include any additional procedures that you are reasonably able to implement to ensure the personal information which staff and councilors have access to is securely protected.

If any questions arise please contact jacobkimball@gov.nl.ca

