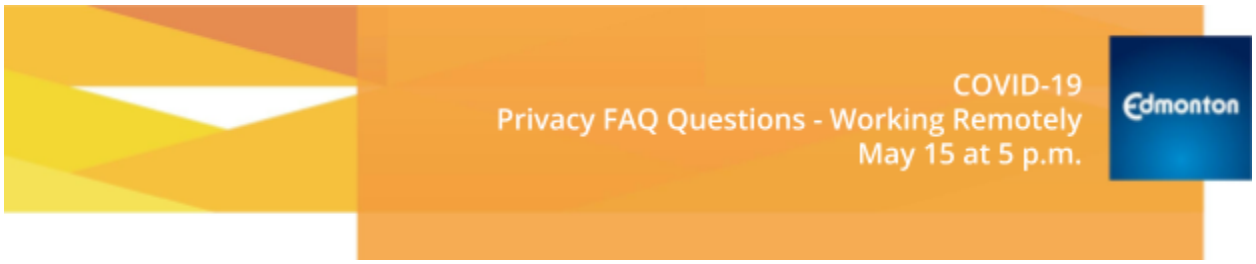

Can I use my personal phone for work purposes?

Yes, the City has a program to support use of personal devices when working from home. It is recommended that supervisors review these documents with their staff:

Use of Personal Devices for Work

Use of Personal Devices for Work - FAQ and Definitions

Protection of Mobile Sensitive Data

Acceptable Use of Communication Technology

Is information on my personal device subject to FOIP?

FOIP applies to City records not to personal devices. City records stored on your device may be subject to a FOIP request. However, staff using their personal device should use Google Apps and the Application Portal, neither of which automatically download documents or information to your device. If an employee does need to download to their device for transitory purposes (e.g. to attach and send a document via email, or temporarily download and edit a Word document), the document should be stored in the appropriate Google Drive or network drive and deleted from the device. If you are aware that you have had City information housed on your device recently, you can manually clear the device's cache as an additional protective measure.

Employees should not store City records on personal devices. If a copy of a record is downloaded to a personal device for a limited purpose, the copy should be deleted immediately, along with any other transitory City records. It is the employee's responsibility to ensure City records are not stored on personal devices, and all transitory records are routinely deleted.

What are some practical privacy tips to keep information secure when working at home?

- Do not let family/friends access or log onto work devices
- Lock devices when stepping away
- Ensure removable storage devices (e.g. portable harddrives, USB flash drives etc.) are password protected

- Do not share passwords with anyone, including family/friends.
- Protect screens when you are accessing City IT applications
- Do not leave paper files or electronic devices in vehicles
- Document and track the location of paper files or other portable storage devices (such as USBs)
- Secure paper files at home
- Do not dispose of paper records that contain personal information in home/public garbage or recycling bins. City information must be securely disposed of in City gray bins or securely shredded in home shredders
- Ensure that work devices are not synced to personal networks that may be accessible to other users of your network
- When you are using a personal device for work purposes, ensure it also cannot be viewed by other users of your network

What information about my employees can I collect to support working from home?

The FOIP Act allows collection of personal information that is required to support City work. During this time, supervisors may need to collect:

- Emergency contact lists
- Work from home status
- Competencies and information to assign individuals work different from their usual job

When collecting this type of information:

- Only collect the information necessary
- Check permission settings
- Limit access to documents to only those who “need to know”

Can I create emergency contact lists?

Yes, emergency contact lists are necessary for emergency situations. Contact lists should:

- Contain the least amount of personal information necessary
- Should only be used for emergency situations, and not for other purposes
- Should be shared only with those who “need to know” the information (generally limited to leadership)

Double check the security settings on contact lists.

Can I take paper files home?

Some business areas may need to use paper files while working from home. If files must be taken home:

- Obtain permission from your supervisor, and document why paper files must be transported
- Take home only the paper files which are needed
- Track checkout, transport, and return of paper files
- Do not leave paper files in vehicles
- Secure paper files stored at home

How can I remotely monitor staff while maintaining privacy?

The level of monitoring should be reasonable to the circumstances, the nature of the work duties, and the past performance of the employee. Supervisors can remotely track attendance in a number of ways including:

- Telephone and Google check-ins
- Time-tracking
- Maintaining location and assignment tracking forms

Do I need to notify staff when personal information is being collected?

Even when collecting personal information from employees, a collection statement is required. Collection statements are important because they inform employees about the purpose for which their personal information will be collected, used, and potentially disclosed.

The following is an example of a collection statement when collecting personal contact information:

> Personal information is collected for the purpose of emergency preparedness and will be used to contact you in the event of an emergency to provide instructions. Collection is authorized under section 33(c) of the *Freedom of Information and Protection of Privacy* (FOIP) *Act* and is managed and protected in accordance with the Act. Questions about the collection, please contact title, address, 780-XXX-XXXX, and [optional] email address.