March 17, 2020

Tips for public bodies and organizations setting up remote workspaces

VICTORIA—Many public bodies and organizations are now setting up employees to work remotely in the wake of the COVID-19 outbreak. Care must be taken when doing this because it often means personal information leaves the worksite. Below are some tips for how to keep personal information safe when working away from the office.

Mobile devices

- Password protect your device
- Lock your device when not in use
- Ensure portable storage devices (such as USBs and portable hard drives) are encrypted and password protected
- Keep your software up-to-date

Emails

- Use work email accounts rather than personal ones for work-related emails involving personal data.
- Before sending an email, ensure you're sending it to the correct recipient, particularly for emails involving large amounts of personal data or sensitive personal data

Paper copies and files

- Only remove personal information from the office if it is necessary to carry out your job duties
- Take the least amount of personal information you need and leave the rest behind
- Securely store any paper files when not in use. This means locking files away and not leaving any files in your vehicle

General rules of thumb

- Avoid viewing personal information collected and used for work in public. If you must, take precautions to make sure no one else can view the personal information.

Resources for public bodies considering remote work options:
Protecting personal information away from the office
Mobile devices: tips for security and privacy

Resources for organizations considering remote work options:
Protecting personal information away from the office
Is a Bring Your Own Device (BYOD) program the right choice for your organization?
Mobile devices: tips for security and privacy