JULY 2020

PRIVACY
FACT SHEET

Working from home during the COVID-19 pandemic

Many government and public sector organizations had to close their offices with little advance notice because of the public health crisis brought on by COVID-19. People are working from home, many in makeshift conditions that were never planned or anticipated. This creates the potential for new challenges and risks to privacy, security, and access to information

Although this is an unprecedented and rapidly changing situation, Ontario's access and privacy laws continue to apply. As a result, your organization must take timely and effective steps to mitigate the potential risks associated with this new reality. This fact sheet outlines some best practices to consider when developing a work-from-home plan that protects privacy and ensures access to information.

WORK FROM HOME POLICIES

You should work with your information technology, security, privacy, and information management staff to review and update any existing work-from-home policies to adequately address the risks to access, privacy and security, as they may have evolved since originally drafted.

If you do not have such policies in place, you should create them by adapting your existing privacy, security, and data access policies to the unique features of the current context where virtually everyone is working from home.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

COMMUNICATING WITH YOUR STAFF

You should remind your staff:

- that the legislative requirements and corporate policies and practices related to access, privacy, security, and information management continue to apply when working from home
- to immediately report any information security incidents and privacy breaches (that is, when personal information is lost or stolen, or collected, used, or disclosed without authorization)

You should provide your staff with:

- updated contact information for key individuals who can provide technical, and administrative support (for example, information technology, security, records management, freedom of information, and privacy staff)
- alerts to fraud, phishing scams, and other malicious cyberattacks, and practical guidance on how to identify and defend against them (for example, how to pick up on some tell-tale signs of fraudulent emails and reminders not to click on attachments or links from unknown sources)
    - See the IPC's *Protect Against Phishing* Fact Sheet for best practices, **https://www.ipc.on.ca/wp-content/uploads/2019/07/fs-tech-protect-against-phishing-e.pdf**

REMOTE ACCESS TO NETWORKS AND INFORMATION

If possible, enable secure remote access to your networks, databases, and email accounts (for example, by requiring staff to use strong access controls such as multi-factor authentication, and a virtual private network (VPN) with end-to-end encryption).

Where secure remote access is available, prohibit your staff from:

- using unsecured WiFi
- removing personal information from the office (electronic and/or hardcopy) without prior approval

In light of the heightened risks associated with your staff working from home, you should review your organization's access controls to ensure staff only have access to the minimum amount of personal information they need to do their jobs.

TECHNOLOGICAL DEVICES AND RELATED SOFTWARE

Work-issued devices

You should identify the specific technology and other resources (such as laptops, mobile phones, secure USB drives, printers, software applications, etc.) your staff requires to carry out their functions at home.

Ideally, your organization should provide them with the software and hardware they need when working from home. This will greatly reduce the privacy and security risks that can arise when staff use their own personal devices, such as non-industry standard or out-of-date security software, and shared devices.

Your work-issued devices should have up-to-date security software, applications, and other necessary resources installed to ensure that your staff can do their jobs while protecting privacy and security.

Work-issued devices and installed software should be properly configured, preferably by your information technology staff. If the use of external communication platforms and cloud service tools is permitted or required, ensure that your staff understands how to safely install, configure, and use them. For example, video conferencing sessions should have password-restricted access controls and appropriate limits on screen sharing and recordings.

Staff should not download or install programs or apps on work-issued devices without prior approval. Many popular programs and apps are known to have security vulnerabilities that can expose your organization to unnecessary risk.

Personal devices

If you are not in a position to issue technology equipment and related resources to everyone and some staff must use personal devices for work-related purposes, consider what measures should be in place to strengthen the protection of the information accessed, used, and saved on those devices. For example, the security software installed on home computers may not be equivalent to the software used at your office and may require upgrading.

If your staff must use their personal devices for work purposes:

- remind them to take appropriate precautions to protect personal information, including ensuring necessary security features are installed, anti-virus software is enabled and updated, and WiFi connections are secure
- in the absence of secure remote access tools, require staff to appropriately segregate and secure all work-related records stored on any shared device used at home (for example, save password

protected files on personal devices in a separate location from personal records so other family members cannot access them)

- develop a plan to manage the secure destruction of work-related records following applicable retention periods

COMMUNICATING BY EMAIL

To the maximum extent possible, ask your staff to use only work-issued email accounts.

Remind your staff to take steps to protect any records containing personal information before sending emails, by:

- securing personal information on work-related or personal devices (for example, by encrypting or password protecting document attachments and sharing passwords separately through a different channel or message)
- if securing personal information is impossible, obtaining prior consent from the individual to whom the personal information relates before sending
- verifying the recipient's identity and making sure to correctly address emails to avoid misdirection (for example, by sending test emails in advance to ensure they reach the intended recipient)
- verifying that emails only contain content relevant to the intended recipient

HOME WORKSPACES

Advise your staff to set up a private workspace in their home or at a location to be agreed upon with their manager.

Require staff to take all reasonable measures to ensure screen content is not viewable and phone or video conversations involving personal or other sensitive information cannot be overheard by others in the home or other agreed-upon workspace.

Remind your staff to:

- secure work-issued and personal computing devices when not in use or when left unattended
- never leave their computing devices visible and unsecured outside the home
- not work in public places where there are higher risks of eavesdropping and equipment loss and theft
- appropriately use password protection and encryption on their devices

PAPER AND OTHER FORMATS OF RECORDS

Remind your staff to take appropriate precautions to protect paper records and other formats containing personal information (for example, photos, audio or video recordings, hard drives and USBs), including by:

- not leaving personal information unattended or unsecured when away from the workspace
- securely storing all records containing personal information regardless of the format
- not printing records containing personal information, unless necessary
- not throwing out paper records containing personal information (for example, by putting them in the garbage or recycling)
- securely retaining personal information, if unable to follow required secure destruction protocols at home, until such time as access to secure shredding services can be obtained

Your organization should develop a plan to ensure the secure destruction of any records with personal information, regardless of format, following applicable retention schedules. The plan may include allowing staff access to office shredding facilities when it is safe to do so.

ACCESS TO INFORMATION RIGHTS

Your organization's obligations to enable access to information and ensure reasonable measures are in place to document and preserve records continue to apply when your staff are working from home.

To ensure that your organization complies with these obligations, you should remind your staff:

- that all work-related records continue to be subject to access to information laws, regardless of whether they are retained on work-issued or personal computing and storage devices
- to record business activities, including keeping accurate records of all key business decisions and retaining all business records
- of the importance of good record management practices, such as the use of approved file naming conventions so records can be managed properly and easily located
- to digitize and transfer all business records to work-related systems and repositories, as soon as possible
- to appropriately back-up business records if using personal computing and storage devices

LONGER-TERM STRATEGY

To continue meeting your evolving operational needs, while complying with applicable access and privacy legislation, your organization should create a long-term work-from-home strategy. Accompanying policies, practices, and remote training should address key issues such as:

- use of personal computing devices
- how to recover business records and other informational assets from staff who depart from the organization during the pandemic
- secure transfer and retention of records including personal information
- secure disposal of records and devices, including personal devices, used for work-related purposes during the pandemic
- migration of records and devices back to the office, and update of corporate files and record repositories
- managing freedom of information requests including requirements to conduct a reasonable search for records
- monitoring and evaluating the effectiveness of access and privacy (including security) measures in a remote work context and enabling continuous improvement of such measures based on practical, learned experiences

RESOURCES

Office of the Information and Privacy Commissioner of Ontario

Safeguarding Privacy on Mobile Devices, May 2014, **https://www.ipc.on.ca/wp-content/uploads/Resources/safeguarding-privacy-on-mobile-devices-e.pdf**

Instant Messaging and Personal Email Accounts: Meeting Your Access and Privacy Obligations, June 2016, **https://www.ipc.on.ca/wp-content/uploads/2016/08/instant-messaging.pdf**

Communicating Personal Health Information by Email, September 2016, **https://www.ipc.on.ca/wp-content/uploads/2016/09/Health-Fact-Sheet-Communicating-PHI-by-Email-FINAL.pdf**

Protect Against Phishing, July 2019, **https://www.ipc.on.ca/wp-content/uploads/2019/07/fs-tech-protect-against-phishing-e.pdf**

Federal

Office of the Privacy Commissioner of Canada, *Privacy Tech-Know blog: Videoconferencing – Maintain your physical distance, but keep your personal information close*, May 1, 2020, **https://www.priv.gc.ca/en/blog/20200501/**

Alberta

Office of the Information and Privacy Commissioner, *Managing Records When Transitioning from Work to Home*, April 2020, **https://www.oipc.ab.ca/resources/managing-records-when-transitioning-from-work-to-home-advisory.aspx**

Saskatchewan

Office of the Saskatchewan Information and Privacy Commissioner, *Pandemic Binder: Statements and Blogs by the Saskatchewan IPC during the COVID-19 Pandemic*, **https://oipc.sk.ca/assets/pandemic-binder.pdf** [includes blog post about working from home]

Office of the Saskatchewan Information and Privacy Commissioner, *Best Practices for Transporting Personal Information (PI) and Personal Health Information (PHI) Outside of the Office*, April 2020, **https://oipc.sk.ca/assets/best-practices-for-transporting-pi-phi-outside-the-office.pdf**

Manitoba

Manitoba Ombudsman, Protecting Personal Information and Personal Health Information When Working Off-Site, **https://www.ombudsman.mb.ca/uploads/document/files/pn-bbt12-protecting-personal-and-personal-health-information-when-working-outside-the-office-en-1.pdf**

Québec

La Commission d'accès à l'information du Québec, *Sécurité de l'information et télétravail : employeur* (Français), May 2020, **https://www.cai.gouv.qc.ca/covid-19-questions-frequentes/securite-de-linformation-et-teletravail-employeur/**

La Commission d'accès à l'information du Québec, *Sécurité de l'information et télétravail : employé* (Français), May 2020, **https://www.cai.gouv.qc.ca/covid-19-questions-frequentes/securite-de-linformation-et-teletravail-employe/**

About the IPC

The role of the Information and Privacy Commissioner is set out in the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act*, and the *Personal Health Information Protection Act*. The commissioner is appointed by the Legislative Assembly of Ontario and is independent of the government of the day.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario