

Remote workplace tips for protecting personal information



Measures to control and prevent the spread of Covid-19 will involve more people working remotely than usual.

Companies generally make provision to control the flow of personal information within office networks and physical spaces; however, when employees work remotely, it becomes more difficult to ensure that personal information remains protected.

One of the conditions of the Protection of Personal Information Act (POPIA or POPI Act) is accountability, requiring companies to ensure adherence to all the principles of the POPI Act.

Many companies endeavour to comply with the POPI Act; however, in a remote working environment, the employees are responsible for ensuring that they do not violate any of the provisions stipulated in the current company policies that set expected behaviour for information protection and security.

All employees are responsible for the safe and secure handling of all hardcopy records and information taken off-site or accessed from an off-site location, including but not limited to electronic files.

The purpose of this blog is to provide you with general guidelines to adopt to ensure that employees protect the privacy and confidentiality of such records when working remotely.

May records be removed from the office?

Employees may only remove records from the office with the required approval from a manager when it is absolutely necessary for the purpose of carrying out their duties. If possible, only copies should be removed, with the originals left in the office. Records should also be signed out on a sheet which includes the employee's name, a description of the records and the date on which the records were removed.

How should paper records be stored?

Paper records should be carried in a locked briefcase or sealed box and remain under the constant supervision of the employee.

- When an employee travels by car, paper records should always be locked in the trunk and not opened or reviewed while travelling on public transportation. This is also a requirement for laptops, computers and wireless technology such as digital assistants and cell phones.
- When working remotely, paper records should be stored in a locked filing cabinet or desk drawer when they are not being used, also during meals and other breaks. The cabinet or desk should only contain work-related records.
- Securely dispose of all personal information when no longer needed.

How should you protect laptops, computers and wireless technology?

Access to laptops, computers and wireless technology should be password controlled, and any personal information on the hard drive should be encrypted. Other reasonable safeguards, such as anti-virus software and personal firewalls, should also be installed.

Employees should only use software that has been approved by their institution's IT department.

- When working remotely, a laptop or computer should be logged off or shut down when unattended.
- Do not share a laptop and wireless technology that is used for work purposes with other individuals, such as family members or friends.
- Securely remove all information from the laptop, computer and wireless technology when no longer needed.

How to use telephones and voice mail when working remotely

When in transit or working remotely, employees should avoid using cell phones to discuss personal information. Cell phone conversations can easily be overheard or intercepted by individuals using scanners or other devices.

If an employee works remotely on a regular basis, a separate phone line and password-controlled voice mail box should be set up. Do not disclose the password to any unauthorised individual.

How to handle video-conferencing facilities

If recording, all participants must be notified of the purpose thereof and consent to the meeting being recorded.

- Any personal business information must be removed from view when using camera view or screen sharing.
- Cameras and microphones should be turned off when not in use.

What is the best practice for using emails?

Follow the organisation's policies relating to the use of emails.

- Use work email accounts for work-related emails involving personal information. If you have to send personal emails, make sure that the contents and attachments are encrypted and avoid using personal information in subject lines.
- Before sending an email, ensure that you are sending it to the correct recipient, particularly emails involving large amounts of personal information.

What to do in case of a breach

The loss or theft of personal information should be reported without delay to the employee's immediate manager, IT department and the Information Officer. On investigation, it may be recommended that the company notify any individuals whose personal information had been lost and take steps to contain the loss of the information.

The following are *a few tips to ensure computer or cyber security* when working away from the office:

- Turn it off – When you are not using a device, turn off the Wi-Fi and Bluetooth connectivity.
- Consider high-level security – Encrypting a laptop and using secure VPN will help to protect information.
- Keep your items on you – Do not leave hardcopies or electronic devices unattended.
- Switch on the “Find My Device” mode – This can help you to locate a device if you accidentally leave it behind or it is stolen.
- Use secure cloud-based services – Apply solid security measures to protect personal information.
- Use caution with USBs – Never use a USB device unless it had been cleared by your company's IT team and ensure that no-one plugs a USB device into your computer.
- Create complex passwords – Passwords should consist of sentences or difficult-to-identify sequences of numbers and words. Auditing passwords frequently will provide additional safety.
- Recognise phishing emails – Do not accept software updates that are triggered from a website or email, such as Java or Adobe Flash.
- Be aware of who might be listening to your conversations. If you are discussing personal information, move to a private area.
- Do not send or open secure data when using a public Wi-Fi network.

Conclusion

Covid-19 brings several new challenges and remote working will become a permanent practice and way of working post Covid-19. This will pose unique challenges to business owners to implement additional measures to ensure information is protected. Companies should ensure that employees understand both their responsibility to protect personal information and the steps they must take in order to do so. “The best policy in the world will not prevent a data breach unless employees know what it says and understand both how to put it into practice and why it is important to do so.”

SERR Synergy assists businesses in compiling Data and Information Protection Reports.

Our professional legal team ensures that physical information and cybersecurity risks of organisations are identified and managed to maintain the confidentiality, integrity and availability of data. We provide various policies for organisations to implement in order to ensure compliance in such a way that it provides business value to our clients and allows for improvement in efficiencies and effectiveness by meeting the compliance requirements.

About the Author: Retha van Zyl completed her BCom Hons (Economics and Risk Management) studies at the North West University. She joined our team in January 2016 and currently holds the title ‘Information Compliance Advisor’. She specialises in POPI and PAIA compliance, which includes compiling and submitting PAIA Manuals to the Human Rights Commission. She also compiles the Data and Information Protection Report to identify risks associated with information security and drafts Information Security policies for procedural compliance in each department within an organisation.

Sources:

<https://mobiusconsulting.co.za/how-to-maintain-corporate-privacy-in-a-home-based-office/>

<https://www.workflowmax.com/blog/how-to-keep-your-data-safe-when-working-remotely>

<https://www.ipc.on.ca/wp-content/uploads/resources/wrkout-e.pdf>

<https://www.bcit.ca/files/its/pdf/iapo-prtoecting-personal-confidential-information.pdf>

https://www.kpu.ca/sites/default/files/downloads/protecting_personal_info_outside_office1534

https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/02_05_d_46_dpd/

<https://dataprotection.ie/en/protecting-personal-data-when-working-remotely-0>