How to respect privacy and protect public sector information when working remotely

Summary
The Office of the Victorian Information Commissioner (OVIC) recognises that COVID-19 has caused significant impacts on the general public and Victorian Public Sector (VPS) agencies, and that many VPS employees are working remotely for the foreseeable future.

The threat landscape is changing on a day to day basis, and it is everyone’s responsibility to ensure that we protect public sector information and respect Victorians privacy when working remotely.

These tips have been prepared to help VPS employees to secure their organisation’s information and ensure that the privacy rights of all are upheld.

Tips

• **Understand the security value of the information you are accessing remotely**
  All VPS employees have a responsibility to protect public sector information, even when working remotely. Work with your team to understand the security value of the content you will be accessing remotely, and to identify and manage the associated risks.

• **Refer to your organisation’s policies and procedures**
  These protective measures should include ICT solutions and personnel and physical security controls. If you are unsure of how to secure the information you are accessing when working remotely, refer to internal policies and procedures.

• **Avoid working in public places and set up a private workspace where possible**
  It’s best to avoid working in public places. Be wary of others being able to look at your work device’s screen, overhearing work-related conversations, or accessing any work-related hard copy information you may be working on. Where possible, set up a separate workspace, away from other members of your household. Take work calls in a private room if you can or reschedule the call for a later time in the day when no-one is around.

• **Be conscious of what you say to members of your family, friends or household**
  Many VPS employees will not be used to working remotely for long periods of time. Understandably, you are likely to miss quickly and easily discussing work matters with your colleagues in the office. You should not, however, discuss any work matters with family members, friends or housemates. Set up regular ‘check-in’ sessions with your colleagues instead.

• **Use a secured WiFi network or ethernet**
  Avoid using public or unprotected WiFi networks. If you are using your home WiFi, check to see that the connection is secured by checking if your router has a password (many use “admin” as the password by default, which is not secure) and make sure your devices have run any firmware or software updates. Check to see if your WiFi has encryption enabled such as WEP, WPA or WPA2, which will further secure your network.

• **Only use workplace approved devices and accounts for work-related purposes**
  Refer to your organisation’s security policies and procedures for advice on the use of personal
devices and personal email accounts for work-related purposes. Where the use of a personal mobile phone is permitted, check the device settings to ensure privacy and security functions are enabled as appropriate. As an example, you may want to prevent your Caller ID from being displayed when making outgoing calls.

- **Only use workplace approved third party collaboration and communication platforms for work-related communication**
  Avoid using third-party collaborative tools or communication platforms that have not been approved by your organisation when communicating with colleagues or stakeholders about work-related matters. This includes things like messenger clients, video chat, email accounts and online communication boards. These can all be helpful tools, but they must be approved by your organisation.

- **Avoid inserting peripheral devices into your workplace device that require drivers to be installed**
  Some peripheral devices (e.g. mouse, keyboard, headset, printer, usb storage) require software (such as drivers) to be installed to access them. Refer to your organisation’s policy before inserting peripheral devices into your device which require you to install a driver or other software on your device.

- **Secure devices and documents when you leave them unattended and at the end of the day**
  When you step away from your workspace, secure the room or lock away hard copy documents securely. Similarly, lock your work device when you leave it unattended. Ensure you are following your organisation’s password policies, and never share the password with others. At the end of the day, log off and shut down your work device to ensure it gets relevant updates and to prevent others from accessing it. Store any work devices and any hard copy documents in a secure location and out of sight, to prevent unauthorised access or theft.

- **Notify your organisation of any incidents**
  If you become aware of lost, misplaced or stolen hard or soft copy public sector information, or work device(s) or personal device(s) that may have contained public sector information – notify your organisation. Let your organisation know if you experience unusual or strange behaviour on your device.

- **Be especially wary of phishing scams**
  Advice from the Victorian Government Chief Information Security Officer is that there has been a significant increase in malicious activity surrounding COVID-19. This activity includes false reports purporting to come from trusted sources such as government agencies and media outlets. Remain mindful when clicking on links and accessing digital content when working from home. If you receive a suspicious email, contact your organisation’s IT team in the first instance.

- **Be careful of what you post to social media**
  Check your privacy and security settings and be mindful about what you post. If you take pictures or videos while working remotely, ensure you don’t inadvertently capture work information or devices in the background. Similarly, refer to your organisation’s social media policies and procedures and refrain from discussing work related content that isn’t authorised for release to the public.

---

**Disclaimer**

This fact sheet does not constitute legal advice and should not be used as a substitute for applying the provisions of the Privacy and Data Protection Act 2014 (Vic.), or any other legal requirement, to individual cases.