Working off campus: your responsibilities

When working from home, or another off campus location, it is important to know your responsibilities for handling University devices and data, including personal data. Below are reminders of your responsibilities and the actions you should take to ensure you are working safely and securely.

Understanding the risks and your responsibilities

1. If you haven't already done so, complete the University of Aberdeen Security Awareness training – https://training.abdn.ac.uk/
2. Follow the guidance in the University's Data Protection Policy when handling any personal data.
3. Be vigilant when opening emails. Do not click on links or open attachments in unsolicited email.
4. Report any suspicious emails, calls, or activities to the IT Service Desk – servicedesk@abdn.ac.uk
5. Data breaches can still happen when working from home – if you think one has occurred, please contact dpa@abdn.ac.uk as soon as possible.
6. Report the loss or theft of a University device to the IT Service Desk – servicedesk@abdn.ac.uk
7. While working remotely, please keep abreast of University IT security news by checking StaffNet and checking your University email inbox regularly.

Using systems and data

1. Only use University approved file sharing and collaborative tools to share information; OneDrive for Business, SharePoint, MS Teams and ZendTo. Avoid using unauthorised tools like DropBox or Google Drive. If you are in any doubt or require guidance please contact the IT Service Desk – servicedesk@abdn.ac.uk.
2. You must use your University email account or MS Teams for all work related communication. Do not use a personal email account.
3. Use OneDrive for Business, SharePoint, MS Teams or shared network drives to save University data.
4. Respect any restrictions specified by external data providers or research funders on accessing, using or storing data, such as restrictions on using cloud storage.
5. If you do not think you can comply with data handling policies while working at home, contact your line manager who can raise it with the Head of School or Director.

Using your personal device

1. Ensure your personal device has up to date anti-virus software – see StaffNet's IT Security and Anti-virus page for guidance.
2. Make sure you are using the most current version of your Operating system.
3. Make sure you install security updates regularly.
4. Back up your data.
5. When using the Virtual Private Network (VPN) on a personal device to access a file on your H drive or a shared drive, you must download a copy of the file to your personal device before you can edit it. Be aware of where you are downloading the file to. Once you are finished editing, you will need to upload the revised file to the VPN. You should then delete the file from your personal device. For full guidance, see page 5 of our Remote VPN guide in Toolkit.

6. Save work-related files on your University OneDrive for Business, SharePoint, MS Teams or shared network drive. If you cannot connect to the University network, save your work-related files in a designated 'Work' folder on your device and move the information onto the University network as soon as you can. You should password protect the folder as follows:
    - Using File Explorer, right-click on the file or folder you want to password protect
    - Click **Properties** at the bottom of the context menu
    - Under the **General** tab, click **Advanced…**
    - Tick the **Encrypt contents to secure data** checkbox, click **OK**, then **Apply**
    - You may be prompted to back up your encryption key. If so, simply follow the instructions in the wizard., you'll need it if you lose access to your encrypted files
7. Make sure you have a strong password on your device. Read our top tips on creating a strong password.
8. Use Multi-Factor Authentication wherever possible.
9. Set your device to auto-lock after it has been inactive for a period of time.
10. Encrypt your personal device where possible – see StaffNet's IT Security and Anti-virus page for guidance.

Using your University device at home

1. Do not, under any circumstances, give family and friends access to University equipment.
2. Do not make un-authorised alterations/changes to a University device. This includes downloading non-approved software/apps.

Good working practices

1. Work in an area where your screen and any papers are not visible to others.
2. Make sure you keep work-related data away from family and friends.
3. Try to work separately from family and friends – in another room if possible – especially when making calls.
4. When using the Share content feature in a MS Teams meeting, be aware of your audience, what the contents of your screen are, and whether it is appropriate to share. For guidance, see Microsoft Teams support.
5. Always lock your computer whenever you step away from it.
6. If you have confidential waste, do not dispose of it in household waste/recycling. Retain it until your return to work and place in the confidential waste bin.
7. At the end of your working day, store your laptop and work-related paperwork out of sight.

You'll find further guidance on working from home and remote access solutions on Toolkit's Working from Home resource.

Questions?

If you have questions about any of the guidance in this document, please contact:

- Gary Fisher, Information Security Manager
  gary.fisher@abdn.ac.uk or 01224 273337
- Information Governance Team
  dpa@abdn.ac.uk or 01224 273175