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/](https://training.abdn.ac.uk/)
2. Follow the guidance given 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. If you think a data breach 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, e.g. OneDrive for Business, SharePoint, MS Teams, ZendTo.
2. You must use your University email account for all work related email communication. Do not use a personal email account.
3. Do not download University of Aberdeen data to a personal device; this includes USB devices. Please use OneDrive for Business, SharePoint, MS Teams or shared network drives.
4. Respect any restrictions specified by external data providers or research funders on accessing, using or storing data, such as restrictions on 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. Make sure you have a strong password on your device. Read more about [tips on creating a strong password](#).
6. Use Multi-Factor Authentication wherever possible.
7. Set your device to auto-lock after it has been inactive for a period of time.
8. 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. Always lock your computer whenever you step away from it.
5. If you have confidential waste, do not dispose of it in household waste/recycling. Retain it until your return to work and place it in the confidential waste bin.
6. At the end of your working day, store your laptop and any work-related paperwork away and 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