Hybrid working and working off campus: your responsibilities

Now that working from home and from the office is more common for a lot of us, it is important to know your information security and governance responsibilities when handling University devices and data, including personal data, wherever you may be working. 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. It is your responsibility to ensure that data is held securely and that the confidentiality of the data is maintained when working off campus and when travelling between campus and your home. Data and devices must not be left unattended, for example, in a car overnight.
2. If you haven't already done so, complete the University of Aberdeen Information Security & Governance Awareness training.
3. Follow the guidance in the University's Data Protection Policy when handling any personal data.
4. Be vigilant when opening emails. Do not click on links or open attachments in unsolicited email.
5. Report any suspicious or phishing emails using the "Report Phishing" button in Outlook, Outlook Web Access or your mobile application.
6. Report any suspicious calls or activities to the IT Service Desk – servicedesk@abdn.ac.uk
7. Data breaches can still happen when working off-campus – if you think one has occurred, please contact dpa@abdn.ac.uk Please do this as soon as possible, as there may be occasions where we need to report to the ICO within 72 hours.
8. Report the loss or theft of a University device to the IT Service Desk – servicedesk@abdn.ac.uk
9. If you now have shared office space which includes people outwith your team, be aware that some discussions and calls may need to be held elsewhere, as they are not entitled to hear the content.
10. 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. Do not use unauthorised tools such as 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. 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.

Personal devices

1. As stated in the University of Aberdeen Homeworking Policy, University owned and managed devices must be used for regular or permanent homeworking.

2. For irregular or ad-hoc University work, for example checking emails outside of standard working hours, a personal device can be used with the following guidance:
    i. Ensure work-related files and emails remain in University managed systems, e.g. M365, OneDrive for Business, SharePoint, MS Teams or shared network drive.
    ii. Make sure you have a strong password on your device. Read our top tips on creating a strong password.
    iii. Ensure your device is using a supported operating system and all security updates are installed as soon as they are released.
    iv. Use Multi-Factor Authentication wherever possible and where it is mandated.
    v. Encrypt your personal device where possible.
    vi. Please keep work information separate from your own personal information on your personal device.

Using your University device at home

1. Do not, under any circumstances, give family and friends access to University equipment.
2. Do not make unauthorised alterations/changes to a University device. This includes downloading and installing applications and software that are not approved.
3. Restrict personal use of work devices at home
4. If you have a University device, take a note of the asset number. In the event it gets stolen, you can pass the asset number to the Police/service desk.

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 secure and away from family and friends whilst working at home.
3. Try to work separately from family and friends when at home – 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. Set your device to auto-lock after it has been inactive for a period of time.
6. If you have confidential waste, do not dispose of it in household waste/recycling. Retain it until you are next in the office and dispose of in the confidential waste bin.
7. Any paper records gathered whilst at home should be kept securely and those that do not need to be retained, should be returned to campus when possible and placed into confidential waste.
8. Where possible minimise the amount of paper based documents you take home. Only take home sensitive information which stritly necessary to do your job. Ideally, think of alternative ways of accessing the data such as scanning onto your University device.

Travelling between Work and Home

1. Do not leave papers and University devices in cars where they can be visibly seen.
2. Do not store papers and University devices in cars overnight, take them into your home.

3. When travelling between Work and Home, transport your University Device and papers in a sealed bag or rucksack. Avoid the use of open handbags or shopping bags**.**
4. Reduce the amount of travelling when you have papers and University devices on your person, for example go straight home/to work where possible.

You'll find further related guidance on the Working from Home StaffNet page.

Questions?

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

Information Security Team
Servicedesk@abdn.ac.uk or 01224 273337

Information Governance Team
dpa@abdn.ac.uk or 01224 273175