# Personal devices and remote working

*Modern connectivity means we can work almost anytime and anywhere. But how can we make sure our data is protected when working remotely on personal devices?*

Improvements in connectivity and our increasing use of portable devices mean it's never been easier to work remotely.

However, despite the convenience of remote working, its very flexibility can leave us more exposed to security attacks and data breaches.

So, just how *do* we protect our personal data, and University data, when working remotely on personal devices?

Here are our top tips for staying safe.

## Device security

If you use your own laptop, tablet or phone for work, **you** are responsible for making sure it meets the following minimum protections:

- **Password protection**: Biometric protection is good. Passwords are better. See our Passwords user guide for advice on creating a strong password.
- **Encryption**: Make sure you know how to use your device's built-in encryption tools, for example BitLocker on Windows and FileVault on Macs. Or investigate third-party encryption tools. Most newer phones have encryption built into their operating systems.
- **Antivirus/Firewall software**: Make sure you install it, enable it, and keep it up to date.
- **Software patches**: Make sure you apply them and that you enable auto updates.
- **Access**: Be aware of others who may have access to your device, including children who could accidentally damage it.

## Data Storage, Transfer and Backup

Never use an unencrypted USB drive to copy data off the University network for use on personal devices.

We recommend using the University's Remote Access services. The VDI provides secure, authenticated access to your H: Drive or shared Network Drive on personal devices.

Or, provided you are not working on highly sensitive or confidential data, use your University OneDrive for Business (see our guidance for Staff and for Students).

And if you *must* use a USB drive, make sure you encrypt it first using BitLocker to go (Windows) or Disk Utility (Mac). By doing so, if you ever lose your USB drive, the information on it cannot be accessed by unauthorised users.

## Working in Public

When working in public spaces, such as cafés, airports and crowded trains:

- Be wary of shoulder surfers and eavesdroppers!
- Keep devices out of sight when not in use.
- Never leave your device unattended, even momentarily. When staying in hotels, store your device in a safe if available.
- Beware of using public WiFi, such as coffee chains or airport networks. Attackers can set up 'Evil Twin' networks that imitate popular network names and intercept data in transit. Use a 4G connection where possible and make sure web traffic is encrypted (look for https in the address).

## Device Disposal

When it's time to upgrade, make sure you dispose of your old device **securely**.

After backing up any files you want to keep, wipe all data from the hard disk. If you are reselling or trading-in your device, be aware that basic system restores/factory resets are **not** guaranteed to protect data. In many cases, data can be easily recovered using off-the-shelf tools. While you can mitigate this using encryption and by overwriting with junk data, we recommend seeking expert help as the process varies widely by device and OS.

If you're throwing your device away, we recommend you destroy the hard disk entirely.

## Find out more

You'll find more information on protecting your personal devices in Toolkit's Information Security resource.