Using BYOD or Self-Managed Computing Devices

This document is meant to give guidance when using your BYOD (Bring Your Own Device), or when you manage the configuration of a computer yourself that is used to access College/University Data or systems. ‘Device’ in this context includes (but is not limited to) the following:

- Desktop Computers
- Laptop or notebooks
- Mobile phones
- Tablets / iPads

BYOD

A BYOD is any computer or device that you own, that is used for any kind of College/University business. If you do College/University work on it, you are responsible for ensuring it is configured securely.

Your responsibilities

If you are using a self-managed computer or computing device, you have a responsibility to configure it securely.

Click here to go to Universities infosec guidance: Protect my Computer

Self-managed computers

Any computer or device you use that has not been configured by the College’s/Department’s ICT Department, or is not automatically configured by a service provided by the College’s/Department’s ICT Department counts as "self-managed".

You are required to ensure your devices are configured as to automatically update themselves. This "automatic configuration" needs to be of the kind that keeps your device up-to-date in regards to firewall, virus and spam protection and operating system updates on a regular basis. If the device has been configured only once at the time it is allocated to you, it is quite likely to count as self-managed and you need to take responsibility to keep it securely configured.

Many devices for academics are purchased on research allowances and are considered self-managed. You have a responsibility to protect all the information they carry. With a self-managed device, you have the responsibility to configure it as strongly and safely as practical. Follow the link to "Protect my Computer" above.

Department/College-managed computers

Some Departments have their own methods for managing the configuration of devices for staff, for their labs, and in some cases for students. Check with your College/Department computer support team if you are not sure if a device you are using counts as self-managed.

Basic Steps to Follow

1. **Backups** - To reduce the risk of losing information, make sure that it is backed up on a regular basis.
2. **Encryption** - Encrypt your phone, encrypt your laptop, use encryption on your USB sticks. Encrypting your devices will protect University information if they are lost or stolen.
3. **Lock your devices** - Configure your devices to lock using passwords or PINs automatically, or when you put them to sleep.
4. **Think before you click** - Take care what you click on. Phishing is the most common kind of attack.
5. **Configure devices and computers securely** - Keep software up to date and configure your security.
6. **Use Anti-Virus** - Anti-virus software protects your computer from software viruses, and prevents you from accidentally passing them to people you work with.
7. **Security for mobile phones and tablets** - easily lost, broken and stolen. Make sure you backup, lock, configure “find my device”, and enable remote wipe.

8. **Social Media** - be careful what you post - posts could reveal information about yourself that could be used to your disadvantage or contravene your contract of employment. Also be aware that downloads could contain malware.

9. **Protect from theft, loss or breakage** - Don’t make it easy for your devices to be stolen, or to lose our valuable information if the device breaks.

10. **Secure Deletion** - When you dispose of a computer or a laptop or any kind of device, you must ensure it is securely deleted.

**How To**

Here’s what you need to do to meet the requirements on common devices:

**Set a PIN of at least 4 digits**

- Settings > Passcode is set
- Settings > Security > Screen Lock is set to “PIN” or “Password”

**Configure auto-lock**

- Settings > General > “Auto-Lock” is not set to “Never”
- Settings > Security > “Automatically Lock” is set to “5 minutes” or less

**Set up remote wipe**

- Settings > iCloud > Find My iPhone is turned on
- Phone is signed into Google account and location services are turned on

**Reputable Apps**

- Only install apps from the Apple App Store, Google Play store, your handset’s vendor or your mobile network provider.

**Receiving security updates**

- Check that your device is currently supported by the manufacturer, e.g. Apple or Samsung, and monitor this periodically. You can often find lists of supported devices on the manufacturer’s website.

**Updates installed promptly**

- Respond to prompts to apply updates within one week of availability and regularly apply updates to all apps.

**Encryption**

- Apple Devices are automatically encrypted when a PIN code is used
- As there are many flavours of Android based operating systems you will need to refer to your devices operating manual to find instructions on encrypting your device.

**The College’s ICT Department has software that is able to manage your mobile devices (phones and tablets) to ensure they are kept up-to-date, are virus protected, are PIN protected and allow for remote wipe. If you want to be enrolled into this system, please contact the ICT Department.**