Using BYOD or Self-Managed

Guidance when using a "bring-your-own-device" at work, or when you manage the configuration of a computer yourself.

**Your responsibilities**

If you are using a self-managed computer, 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 University Supported Desktop, or is not automatically configured by a service in your School counts as "self-managed".

This "automatic configuration" needs to be of the kind that keeps your computer up-to-date on a regular basis. If the computer is configured 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 laptops and many desktops are not configured using Supported Desktop. You still have a responsibility to protect all the information they carry. With a self-managed computer you have the responsibility to configure it as strongly and safely as practical. Follow the link to "How to protect" above.

**Department/College-managed computers**

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

**BYOD**

A BYOD (Bring Your Own Device) is any computer or device that you own, that is used for any kind of University business. If you do University work on it, you are responsible for ensuring it is configured securely.

**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.