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 (*refer to the last page of this document if you need help determining whether your device is a BYOD or not*). '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 Guidelines to Follow

- **Backups**- To reduce the risk of losing information, make sure that it is backed up on a regular basis.
- **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.
- **Lock your devices**- Any personal device must contain a level of security in line with our existing IT infrastructure, this will include passcode protection and automatic locking when idle.
- **Think before you click**- Take care what you click on. Phishing is the most common kind of attack.
- **Configure devices and computers securely**- Keep software up to date and configure your security.
- **Use Anti-Virus**- Anti-virus software protects your computer from software viruses, and prevents you from accidentally passing them to people you work with.

- **Security for mobile phones and tablets**- Devices are easily lost, broken and stolen. Make sure you backup, lock, configure “find my device”, and enable remote wipe.
- **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.
- **Secure Deletion**- When you dispose of a computer or a laptop or any kind of device, you must ensure the drive(s) are securely deleted.
- **Agreed Work Hours-** You should only complete work on your own device during your own working hours or as agreed with your Line Manager.
- **Illicit images and materials**- This type of material should not be stored or shared on your personal device if it is used as a BYOD.
- **Driving-** You should not use your personal device for work purposes whilst driving.
- **College Policies-** All College IT Policies will apply to all work completed and correspondence sent via your personal device for work purposes.
- **Data Protection-** Whilst using your BYOD all data collected will be kept in accordance with the Data Protection Act.
- **Misuse-** Misuse of College information, data and/or software provided by the College will be treated a gross misconduct which will result in formal disciplinary action being taken up to and including dismissal.
- **Associated Costs-** Personal devices remain the responsibility of the employee and all associated costs for the device and the running of the device shall remain with the employee.
- **Maintenance-** The responsibility for the upkeep of the device and any liability or risks associated with the use of the device for business purposes remain with the employee.
- **College Liability-** The College accepts no responsibility for any loss or damage to personal devices that are the result of employee failure to observe rules, procedures, or instruction, or, as a result of your negligent behaviour.
- **Personal Liability-** The employee assumes full liability for risks including, but not limited to, the partial or complete loss of College and personal data due to operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- **End of Employment-** Upon termination of employment all data and business software is to be returned to the College.
- **Remote Access-** Access to the College’s infrastructure will be in line with current security levels and user profiles.
- **Device Approval-** Any personal device that has not been checked and approved for use by a member of the I.T. team must not be connected to the College’s network.
- **Device Access and Usage-** Any College data and confidential information available on a personal device should be accessed by the authorised user only and this should be in line with the existing IT and Data Protection policies. No access to the device or College’s network will be permitted for third party users.
- **Non-Standard Devices-** The College will not allow any device to connect to the network which has been jailbroken, altered or tampered with in any way. Any device that subsequently becomes jailbroken, altered or tampered with will have all access to the network revoked.
- **Lost or Stolen Devices-** If your personal mobile device is lost or stolen you must advise the I.T. Department immediately in order to ensure access to the College’s network is deactivated.
- **Remote Wipe-** Personal devices must be wiped remotely in cases of a suspected confidentiality breach, lost or stolen device or termination of employment. The College holds no responsibility with regards to any loss of personal photos and/or applications as a result of this action.
- **Monitoring-** The personal device should be made available for monitoring upon request by the I.T. Department. Every effort will be taken to ensure that personal data is not accessed on the device, however in the event that this is not possible no records of the information will be stored and that data will not be used unless required by law.
- **Policy Breach-** Any breach of this policy may result in formal disciplinary action being taken up to and including dismissal.

How To

Here’s what you need to do to meet the requirements on common mobile 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.

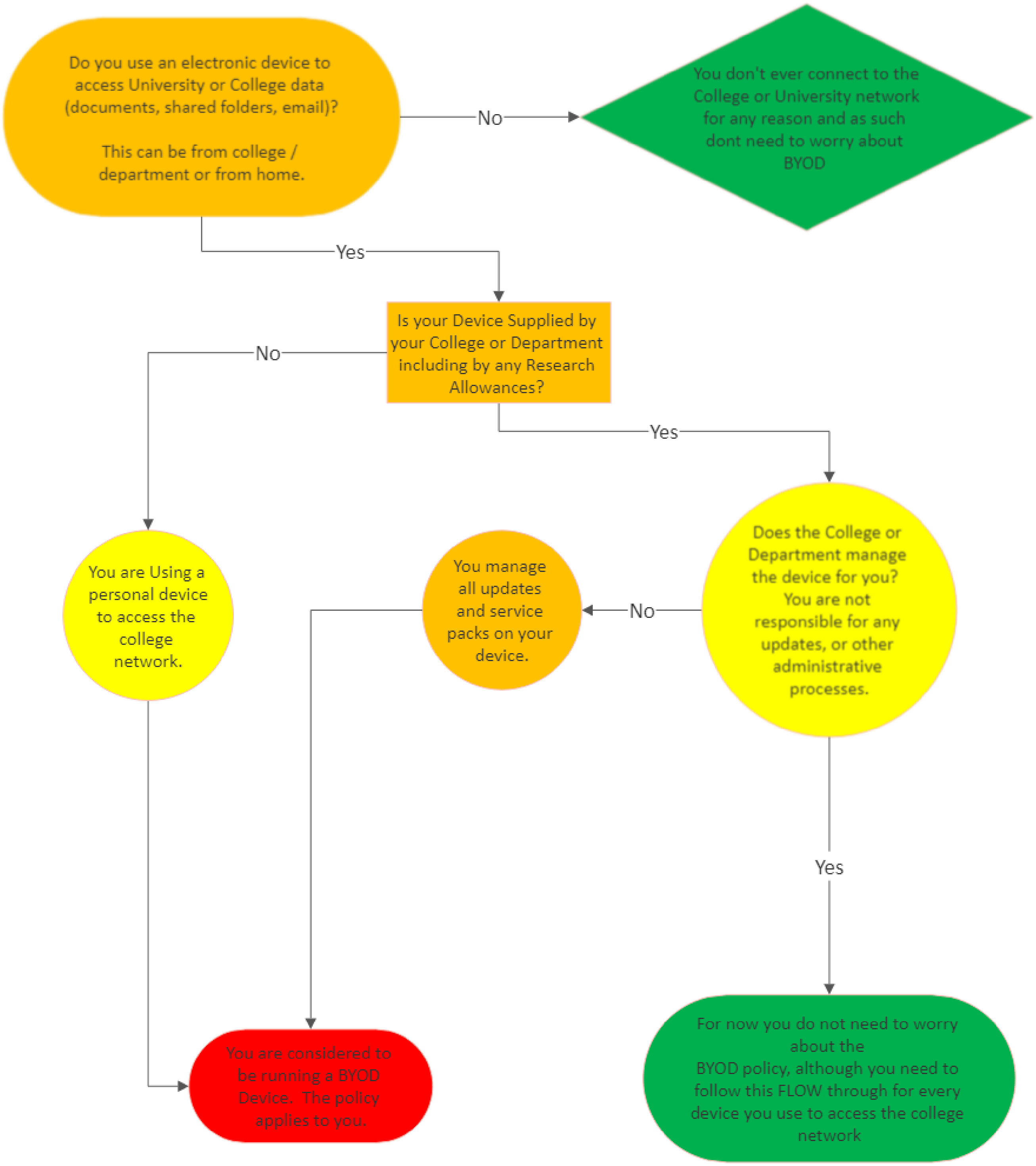
Encryption

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.

Is Your Device considered a BYOD?



Do you use an electronic device to access University or College data (documents, shared folders, email)?

This can be from college / department or from home.

No

You don't ever connect to the College or University network for any reason and as such dont need to worry about BYOD

Yes

Is your Device Supplied by your College or Department including by any Research Allowances?

No

You are Using a personal device to access the college network.

Yes

Does the College or Department manage the device for you? You are not responsible for any updates, or other administrative processes.

No

You manage all updates and service packs on your device.

You are considered to be running a BYOD Device. The policy applies to you.

Yes

For now you do not need to worry about the BYOD policy, although you need to follow this FLOW through for every device you use to access the college network