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

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 it0 ( )] TJ

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

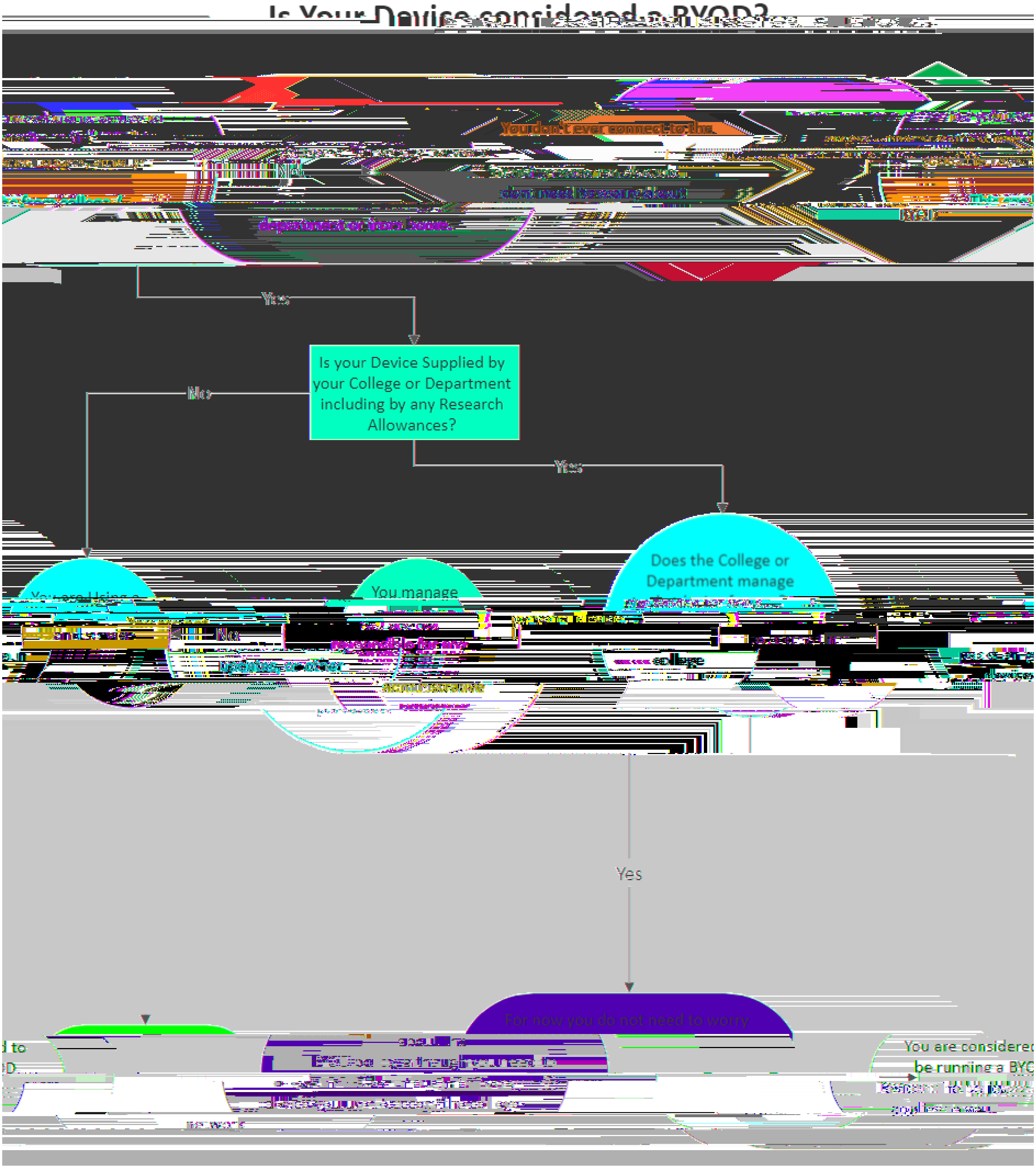
Settings > Passcode is set

Settings > Security > Screen Lock is set to "PIN" or "Password"

Configure auto-lock

Settings > General > "Auto-Lock" is not set to "Never"

Is Your Device considered a BYOD?


You don't ever connect to the
don't need to worry about
department or from some.
BYOD
Yes
Is your Device Supplied by your College or Department including by any Research Allowances?
No
Yes
You are Using a
and service
No
You manage
responsible for any
updates, or other
administrative
Does the College or Department manage
college
device
Yes
For now you do not need to worry
d to
D...
network
You are considered
be running a BYC