

Bring your own device policy (student)

January 2022



UNIVERSITY OF
WINCHESTER

Document Title:	Bring your own device policy (student)
Document Author:	Fiona Greig
Responsible Person and Department:	Fiona Greig Knowledge & Digital Services
Approving Body:	UMG Senate
Date of Approval:	
Date Effective From:	<i>1st January 2022</i>
Review Date:	31 July 2023
Indicate whether the document is for public access or internal access only Indicate whether the document applies to collaborative provision? <i>(Strikethrough text, as appropriate)</i>	Public Access Internal Access Only Applies to Collaborative Provision
<p>Summary:</p> <p>This policy sets out clearly what is required when using your own mobile device (phone, tablet, laptop etc.) on the University network (wired or wireless). Effective implementation of this policy will minimise the risk of data loss and/or inappropriate use or access to University electronic resources and information.</p>	

Contents

1. Scope	3
2. Use of personal devices	3
3. Storage	3
4. Removable devices and media	4

1. Scope

- 1.1. It is recognised by the University that students will need to use a range of devices to successfully complete their studies. Many students find it easier to use their own devices at least some of the time. This policy, alongside the Network Security Policy, provide the guidance to undertake this safely and securely.
- 1.2. The use of non-University provided devices increases the level of risk of network compromise, unauthorised network access, data loss, theft and inappropriate use.
- 1.3. This policy applies to all University students and all other authorised users who are provided direct access to our systems or networks, including Eduroam while connecting with your own institutional login.

2. Use of personal devices

- 2.1. Before connecting any device to University wireless or other available networks you must ensure:
 - 2.1.1. You have installed a suitable anti-virus and malware protection software. For more information about these visit the National Cyber Security Centre's [advice page](#).
 - 2.1.2. You have read and adhered to all relevant policies and, where required, registered your device with Knowledge & Digital Services (KDS). This is mainly for those students living in University accommodation and connecting smart devices like TVs, games consoles and "personal assistant devices". For more information on how to set-up and register devices visit the [Intranet](#). However, if your studies or research means you may be accessing resources require additional review this should also be registered with KDS. Just email [ServiceDesk](#) for assistance.
 - 2.1.3. We have provided you a OneDrive space for encrypted and secure storage. You should use this exclusively for all University related work, including drafts, sharing with teammates etc. If you choose not to use OneDrive you must ensure you have installed suitable encryption software for the storage and access to University provided information. You must do this before connecting any device to University wireless or other available networks.
- 2.2. Users must ensure they mitigate the risks associated with the environment in which they may be working. Advice and guidance should be sought from Knowledge & Digital Services on environments, off campus or international locations where you may be unsure of the risks you may be facing. Just email [ServiceDesk](#) for assistance.

3. Storage

- 3.1. Devices with synchronised online storage present considerable opportunities for data loss or inappropriate use or access to information. Users therefore must ensure the following:
 - 3.1.1. Where the University has provided OneDrive students are expected to use this in favour of any other storage option.

3.1.2. No sensitive or important information should be synchronised to or stored on cloud based storage that has **not** been provided by the University. This includes but is not limited to:

- iCloud
- GoogleDocs
- Drop box
- Skydrive
- SugarSync

4. Removable devices and media

4.1. Storage mediums and devices such as USB sticks, external hard drives, flash card and any other portable drives carry considerable risks in transporting, storing or transferring information and so :

4.1.1. Should not be used unless absolutely necessary to temporarily store information.

4.1.2. Information on such devices should be retained only long enough to fulfil the specific need. As soon as the requirement is completed the information should be fully deleted and unrecoverable from that device.

4.1.3. Encryption should be applied to all such devices. You can purchase USB devices with built-in encryption – these are expected to be used.