Bring your own device policy (student)

February 2020

UNIVERSITY OF WINCHESTER

Document Title:	Home and Mobile working policy
Document Author:	Fiona Greig
Responsible Person and Department:	Fiona Greig Library & IT Services
Approving Body:	SMT
Date of Approval:	17 Feb 2020
Date Effective From:	*17 Feb 2020*
Review Date:	***31 July 2021***
Indicate whether the document is for public access or internal access only Indicate whether the document applies to collaborative provision? *(Strikethrough text, as appropriate)*	**Public Access** ~~**Internal Access Only**~~ ~~**Applies to Collaborative Provision**~~

Summary:

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.

TABLE OF CONTENTS *(right-click table below and select 'Update Field' and, if given option, 'Update entire table').*

1. Scope 4

2. Use of personal devices 4

3. University provided mobile devices **Error! Bookmark not defined.**

4. Storage 4

5. Removable devices and media 5

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. While understandable the use of non-University provided devices increases the level of risk of data loss, theft and inappropriate use.

1.3. This policy applies to all University students and other authorised users.

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.

2.1.2. You have read and adhered to all relevant policies and where required, registered your device with Library & IT Services.

2.1.3. Before connecting any device to University wireless or other available networks you must ensure you have installed suitable encryption software for the storage and access to University provided information.

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 Library & IT Services on environments, off campus or international locations where you may be unsure of the risks you may be facing.

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 provisioned cloud storage (e.g. OneDrive students are expected to utilize these services 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:

- 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.