January 2022

UNIVERSITY OF
WINCHESTER

Document Title:	Bring your own device policy
Document Author:	Fiona Greig
Responsible Person and Department:	Fiona Greig Knowledge & Digital Services
Approving Body:	University Leadership Team Senate
Date of Approval:	May 2023 (University Leadership Team) (University Senate)
Date Effective From:	*1st August 2023*
Review Date:	***31 July 2024***
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.

Contents

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. This policy applies to all University students and all authorised users who are provided direct access to our systems or networks. The policy also covers students and staff of other institutions who use the Eduroam network 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 you are living on campus and are using devices that connect to the network including smart devices like TVs, games consoles and "personal assistant devices" must register these devices using the University ClearPass system. This protects your privacy and ensures other people are unable to "hijack" your devices. For more information on how to set-up and register devices visit the Intranet.

2.1.3. If your studies or research require you to access resources which require additional review this should be registered with KDS (e.g. where you may be accessing resources or services dealing with sensitive materials). Email ServiceDesk for advice and assistance.

2.1.3. We have provided each University user 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 where they are accessing University resources and services. Advice and guidance should be sought from Knowledge & Digital Services on the risks of using networks away from the University (off campus or international locations) where you may be unsure of the risks you may be facing. This may be a particular issue for our Apprentice students or those who are studying while on placement. 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 Your University OneDrive should not be synchronised with any other storage solutions.

3.1.3. 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.

4.1.4 Any device plugged into a University computer will be scanned before you are able to use the device.

4.2 Should you lose a removable drive holding any University material you must immediately report this to Servicedesk@winchester.ac.uk