



UNIVERSITY_{OF}
WINCHESTER

Bring Your Own Device Policy
01.06.2026

Document Title:	Bring Your Own Device (Student)
Responsible Role and Department:	Director of KDS Knowledge & Digital Services
Approving Body:	University Leadership Team (ULT)
Date of Approval:	29 th April 2026
Date Effective From:	01 June 2026
Review Date:	31 st July 2029
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
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. It is a sub-policy of the IT Acceptable Use Policy.	

TABLE OF CONTENTS

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

1. Scope

- 1.1. The University understands 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, including the University Guest wifi network. The policy also covers students and staff of other institutions who use the Eduroam network while connecting with your own institutional login.
- 1.3. This policy should be read alongside the IT Acceptable Use Policy.

2. Use of personal devices

- 2.1. Before connecting any device to University wireless or other available networks you must ensure:
 - 2.1.1. For PCs/Macs (in halls), laptops, etc. 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](#). The recommendations and suggestions on this page will meet the University requirements. Those using mobile devices should pay particular note to that section based on your operating system.
 - 2.1.2. For phones or other smart devices, you must ensure that you are running the current operating system and follow all platform-specific recommendations for Android and iOS that are linked to from the National Cyber Security Centre page lined above.
 - 2.1.3. For wearables and other devices, you must ensure you connect as designed by the manufacturer and install any updates as they are released.
 - 2.1.4. You have read and adhered to all relevant policies. Those students living on campus and planning to use devices that connect to the network (including smart TVs, smart speakers, games consoles, personal assistants etc.) must register these devices using the University ClearPass system. This protects your privacy and ensures other people are unable to "hijack" your device(s). For more information on how to set-up and register devices visit the [Intranet](#).
 - 2.1.5. If your studies or research require you to access resources which require additional review, where you may be accessing resources or services dealing with sensitive materials, this must be registered with Knowledge & Digital Services (KDS) before you attempt to connect to any site that may be flagged. Email [ServiceDesk](#) for advice and assistance.
 - 2.1.6. 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.
 - 2.1.7. You are not permitted, at any point, to install, wear or use any technology that undertakes "surveillance". This includes, but is not limited to, "nannycam", smart glasses, hidden cameras, hidden microphones, tracking devices (e.g. AirTags) on any property other than your own personal belongings, tracking apps on other peoples devices (without explicit permissions which must be immediately removed on request).

- 2.1.8. While some wearable technology is acceptable in all situations. Those passive systems that monitor you as an individual fall into this category (e.g. smartwatch / fitness trackers / health jewelry / smart clothing / "hearables"). At no point is it permissible to use smart glasses or similar tools in spaces like gyms, changing spaces, shared bathrooms (halls), or any toilet across campus.
- 2.2. Users must ensure they reduce all the risks associated with 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 in international locations). 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, inappropriate use, or access to information. Users therefore must ensure the following:
- 3.1.1. 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 solution(s).
- 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
 - Google Drive / Google One
 - Dropbox
 - 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. This would normally be where students are creating very large video or sound files where saving to a nonphysical drive can cause delays or possible corruption during the action of saving the file.
- 4.1.2. Information on devices should be kept only long enough to complete the specific need. As soon as this is the case information should be copied to their OneDrive and then fully deleted and made 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. If malicious code is detected, you will not be able to access anything on the infected device.

- 4.2. Should you lose a removable drive holding any University material you must immediately report this to ServiceDesk.

Equality Impact Assessment	
Summary of process undertaken to determine equality impacts:	An initial screening was carried out to identify potential impacts on protected groups. Relevant data and stakeholder feedback were reviewed to assess risks and opportunities. Where necessary, mitigation actions were proposed to ensure fairness and compliance with the Equality Act 2010. The assessment will be monitored and updated as needed.
University Committee (name/ date) where equality impacts discussed (may be Committee of approval, or another):	University Leadership Team
Identified equality impact(s) on colleagues and students (i.e. any specific impacts related to this policy that may cause disadvantage for people due to one or more particular protective characteristic)	
Protected Characteristic	Impact(s) identified and any action(s)/mitigation(s) to address these impact(s), as necessary.
Age	No impact identified
Disability	No impact identified if an individual student has adjustments that require use of devices outside of this policy they will be treated on a case-by-case basis and the Student, Student Support and Success and Knowledge & Digital Services will have an agreed individual technical package put in place. Any agreement will balance the needs of the individuals against the rights of others in our community
Gender Identity	No impact identified
Marriage/Civil Partnership	No impact identified
Pregnancy and Maternity	No impact identified
Race (incl. nationality)	No impact identified
Religion and Belief	No impact identified
Sex	No impact identified
Sexual Orientation	No impact identified