IT BRING YOUR OWN DEVICE (BYOD) POLICY

1 PURPOSE

1.1 Keele University recognises the benefits of a more agile approach to working, potentially including using a personally owned device. However, these potential benefits need to be balanced with the requirements to protect the University data, systems and networks from security breaches and data loss, whilst ensuring compliance with regulatory requirements and ensuring the highest achievable security standards.

1.2 Using a personally owned device introduces several risks, which include:

- Unauthorised disclosure of University information through a device that is vulnerable to being compromised or hacked.
- Increased risk to University systems or data through devices that are not up to date with software, for example introducing vulnerability through compromised software.
- Increased risk to University systems or data through devices that have none or limited security software installed; devices that have misconfigured software installed.

1.3 Users are responsible for the security and maintenance of these devices and the aim of this policy is to ensure that individuals wishing to use a personal device to access Keele information can do so appropriately, safely, and in line with regulatory obligations.

1.4 This policy is part of the University approach to Information Security and should be read together with other IT and Governance policies on Policy Zone, or as defined in section 7 of this policy.

2 SCOPE

2.1 This policy applies to people, denoted as 'users':

- Any user using a non-University owned or administered device to access systems, store or transmit Keele University Data. This includes all staff, faculty, and other authorised users (visitors, emeritus, contractors, Post

Graduate Researchers, other affiliates), who use personal devices to access or process University data.

2.2 Bring Your Own Device (BYOD) is denoted as ‘Personal Device’ and encompass various devices such as smartphones, tablets, laptops, and home desktops

3. POLICY

3.1 Users must use a Keele managed device first and foremost to perform tasks in connection with their official role at the University, if available.

3.2 Any data accessed and stored via a Keele system remains the sole property of Keele University irrespective of device ownership; this includes, but is not limited to, email, any data stored or accessed at the University and via any system, business telephone calls, official social media posts, documents created on a device during active employment or special standing (e.g., Sponsored, Emeritus or Honorary).

3.3 Users are responsible for the security and maintenance of their Personal Device, including patching, anti-virus, and password protection.

3.4 Personal devices must not be connected to the University wired network, unless express permission has been given by Information and digital Services.

3.5 A user must keep their personal device (Phone, Laptop etc.) and software (e.g. Microsoft Windows, Apple MacOS, Android, Adobe etc.) up to date with current supported software releases as often as possible.

3.6 A user should install all vendor security updates to their personal device as soon as they are available, and a user must have an active Antivirus and / or Malware software or built in Operating System features capable of scanning at regular intervals and when accessing files.

3.7 A personal device must not be “jailbroken” or “rooted” (extra privilege outside the manufacturers design), and only official builds of Operating Systems are allowed.

3.8 Passwords, codes or phrases to access a personal device should be complex enough not to be able to be easily guessed, of sufficient length, and follow the NCSC guidelines here.

3.9 The use of privileged accounts meant for system administration by IT Staff is not allowed from a personal device.

3.10 A user is solely responsible for the maintenance, costs and any support of their personal device. The University accepts no responsibility for maintaining, repairing, insuring, or otherwise funding non-University devices or liability for data loss by using any Keele systems.

3.11 The University reserves the right to refuse, prevent or withdraw access to services and data where it considers there may be an unacceptable risk to security, data or University policy.

3.12 A user must ensure that all Keele data is handled in accordance with the Data Classification & Handling Policy.

3.13 Information classified as “Highly Confidential” must not be downloaded to the personal device or personal cloud storage unless permission has been given by the information asset owner. This includes colleagues using assistive technology where a Keele device must be used.

4 GOVERNANCE

4.1 **You must immediately report any loss or theft of a personal device used to access Keele system or data to the IT Service Desk in line with the data protection policy as if the device were Keele managed.**

4.2 University data accessed from personally owned devices is subject to the Freedom of Information Act (FOI) and Subject Access Rights (SAR) under the Data Protection Act (DPA) and any information recorded when using a University system must be provided to Legal and Governance by or other Law enforcement body on official request.

4.3 Users must follow this policy document when considering using a personal device in connection with their role. A breach of the Data Protection Act can lead to the University facing significant fines from the Information Commissioner’s Office and substantial reputational damage.

4.4 Any member of staff found to have deliberately breached this policy may be subject to disciplinary measures, having access to the University’s facilities being withdrawn, or even criminal prosecution. More detailed information may be found in the University’s Data Protection Policy.

4.5

5 MONITORING

5.1 The University will not monitor the content on personal devices; however, the University reserves the right to monitor and log any data traffic transferred between a device and University systems or network.

5.2 Where necessary, the university reserves the right to disconnect, or limit device access as part of an active ongoing investigation or as part of an observed security threat from security monitoring systems.

6 ROLES AND RESPONSIBILITIES

6.1 All users, as defined in section 2, are required to abide by this policy and all associated guidance, processes and procedures aligned to this policy.

6.2 As a general principle, the policy will be reviewed by the Head of Cybersecurity and Operations after three years or where operational and / or legislative requirements change. Any revisions will be approved in accordance with UEC and Council procedures, where applicable.

7. RELATED POLICIES AND PROCEDURES

7.1 This policy focuses on the use of personal devices to access University data. You are strongly urged to read the below complimentary policies on Policy Zone to gain a complete picture of your responsibilities.

- IT Acceptable Use Policy (AUP).
- Records Management Policy.
- Information Security Policy.
- Records Retention Schedule.
- Freedom of Information Act (FOI) Policy.
- Data Classification and Handling Policy.
- Data Protection Policy.
- Information Governance Framework.

8. DOCUMENT CONTROL INFORMATION

Document Name	IT Bring Your Own Device Policy (BYOD)
Owner	Head of Cybersecurity & Operations, IDS
Version Number	1.0
Equality Analysis Form Submission Date	18/03/2025
Approval Date	25 March 2025
Approved By	University Executive Committee
Date of Commencement	25 March 2025
Date of Last Review	25 March 2025
Date for Next Review	25 March 2028
Related University Policy Documents	See Section 7.1
For Office Use – Keywords for search function	