UNIVERSITY OF HULL

Managed Device and BYOD Policy

Classification:	Policy
Version Number:	1.0
Status:	Final
Approved by (Board):	Approved
Approval Date:	11 October 2022
Effective from:	11 October 2022
Next Review Date:	Annual
Document Authors:	Steph Jones, Nigel Kavanagh
Document Owner:	Security & Architecture Manager (Acting), ICT (Nigel Kavanagh)
Department/Contact:	support.hull.ac.uk
Summary:	This policy relates to the use of managed and personal ('BYOD') devices when accessing University services, systems, and information.
Scope:	All University staff and third-parties
Collaborative provision:	Not mandatory
Assessment: (where relevant)	Not applicable
Consultation: (where relevant)	Not applicable
Relevant legal frameworks:	See relevant section of overarching Information Governance and Assurance Policy
Related documents:	Information Governance and Assurance Policy, Information Security Controls Policy and sub-policies, Data Protection Policy
Published locations:	Public website (www.hull.ac.uk)
Document Communication and Implementation Plan:	Available upon request.

All printed versions of this document are classified as uncontrolled.
A controlled version is available from the university website.

Managed Device and BYOD Policy

1. Introduction

1.1. It is critical that the University can safeguard its information assets. This is done by placing controls on devices that are used to access services, systems, and information in a secure manner.

1.2. The University promotes and understands the benefits of information technologies to enable its members to achieve their academic and business objectives, however, this also has to be balanced against the University acting as a Data Controller under Data Protection law when it comes to the appropriate and secure handling and processing of information.

2. Purpose

2.1. This policy relates to managed and personal ('Bring Your Own Device', 'BYOD') devices used to access University services, systems, and information and ensures that they do so in a secure manner.

2.2. This policy supports the overarching **Information Security Controls** policy and its sub-policies as well as the **Data Protection** and **Information Governance and Assurance** policies.

3. Scope

3.1. This policy applies to all University staff, postgraduate students involved in research, and third-parties accessing University data.

3.2. This policy applies to all University owned devices (whether 'managed' or not) and staff owned personal ('BYOD') devices.

3.3. This policy covers all University information and systems being accessed electronically through either the on-campus networks or by remote means.

4. Risks

4.1. **Data Protection:** The University is bound by Data Protection legislation that specifies that technical and organisational measures shall be taken to safeguard data from loss, destruction or damage.

4.2. **Compromise:** Personal ('BYOD') devices create challenges and risks around security that need to be managed effectively to protect the University network and its managed systems.

5. Managed Device Policy

5.1. All members of University staff are required to use a managed device. A managed device is one which is owned by the University and is controlled by ICT for adherence to security best practice and to deliver a consistent experience which is supportable and meets the requirements of the organisation and its partners. This includes, but is not limited to, data security, software patching, application delivery, and anti-malware protection.

5.2. The use of University-owned devices which are not managed will only be approved as an exception for very specific needs where a managed device is assessed as unsuitable. Such exceptions will be made on a case-by-case basis and must be agreed through ICT.

5.3. Any exceptions will be subject to specific conditions for their particular use case. These will normally include requirements that the devices are appropriately secured and will detail time limits on their use before being subjected to a review. A device which is not managed may still be enrolled onto some ICT management systems to ensure compliance with this policy.

5.4. Only managed devices can be fully assured for the purposes of accreditation when used to fulfil the requirements for research projects, grants, and tenders.

6. BYOD Device Policy

6.1. Personal ('BYOD') devices may not have the capability to access certain University information and systems. ICT are under no obligation to modify systems or the network, or to assist those with personal devices, in order to be able to do so.

6.2. If a personal ('BYOD') device is used to access University information and systems, the owner must observe a number of security measures. They will:

- Familiarise themselves with their device and its security features in order to ensure the security of University information;
- Take all reasonable steps to prevent theft and loss of data and will uphold the wider University policies relating to:
  - **Data Protection Policy;**
  - **Data Classification and Handling Policy;**
  - **Data Retention Policy;**
  - **Data Breach Policy**
- Control access to the device either through fingerprint or biometric scanning, password or PIN;
- Ensure that a device or screen lock is enabled after a period of inactivity (no longer than 10 minutes is recommended);
- Enable a 'remote wipe' capability if the device supports it;
- Keep the device operating system, operating system security patches and any installed applications updated. It is recommended that these updates and patches are enabled such that they are automatically downloaded and installed;
- Not use a device that has been 'jailbreaked' or 'rooted' as this can compromise the integrity of the security of the device;
- When using a personal (home) network, the router default administrator password must be changed from its default;

- When using a public network, the staff member should exercise care that the connection is trusted and secure;
- On leaving the University, or the device changing ownership, the staff member must ensure any University data or email configurations are securely wiped;
- If the device is lost or stolen, then the staff member must be report it to ICT.
- Be required to use Microsoft Outlook to access University email accounts, this includes any device capable of running a supported version of the Microsoft Outlook application or Outlook.com via a supported web browser.

6.3. A range of technical controls will be implemented by ICT to ensure that personal ('BYOD') devices are in compliance with this policy.

6.4. ICT will not monitor the content of personal ('BYOD') devices, but they will be subject to security posture checking to identify whether they pose any risk. Posture checking includes detecting the operating system version and whether it is supported, detecting whether critical security updates may be missing, and the presence (or lack of) anti-malware software.

6.5. In the event that a security incident occurs, ICT will reserve the right to disable associated devices and user accounts from accessing the network and systems without notice.