UNIVERSITY OF HULL

Devices and Network Connection Policy

Classification:	Policy
Version Number:	1.0
Status:	Approved
Approved by (Board):	Information Governance Committee
Approval Date:	19 April 2021
Effective from:	19 April 2021
Next Review Date:	Annual
Document Authors:	Steph Jones, Security and Assurance Specialist, ICT
Document Owner:	Head of Service Assurance, ICT (Stewart Doyle)
Department/Contact:	support.hull.ac.uk
Summary:	This document outlines the policy relating to connecting devices to the University network.
Scope:	All University members and third-parties using both University owned devices and personal devices on the network.
Collaborative provision:	Not applicable
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 Security Controls Policy
Published locations:	Not yet published
Document Communication and Implementation Plan:	Available upon request.

Devices and Network Connection Policy

1. Introduction

1.1. This document outlines the policy relating to connecting devices to the University network.

1.2. This policy should be read in conjunction with the overarching **Information Governance and Assurance Policy** and **Information Security Controls Policy**.

2. Scope

2.1. This policy applies to all University members and third-parties using both University owned ('managed/imaged' and 'un-managed/un-imaged'), and personal ('BYOD') devices on the network.

2.2. Devices include, but are not limited to, desktop workstations, laptops, tablet, servers, mobile phones, wireless devices, specialised equipment (such as EPOS systems), cameras, video conferencing systems, and telephony.

2.3. A network connection is defined as any physical and logical connection between a device and the University network infrastructure, provisioned by the ICT department.

3. Connection Policy

3.1. ICT reserve the right to monitor traffic on the network for the purpose of protecting the integrity and performance of the network.

3.2. ICT reserve the right to immediately disable a connection when the integrity or performance of the network is threatened or degraded by the attached device.

3.3. ICT will subject all devices connected to the network to regular asset discovery scans and may subject them to vulnerability scans.

3.4. Any computer or device that has been disconnected from the network must not be reconnected until permission to do so has been granted by ICT.

3.5. University owned devices will be provisioned with an ICT installed 'image'. The use of University owned devices which are 'un-managed/un-imaged' must be prior approved as an exception through ICT.

3.6. Both University owned 'un-managed/un-imaged' devices and personal devices must be maintained with the latest critical updates and have supported anti-malware protection.

3.7. Servers must not be connected to the network without permission having been granted by ICT. ICT reserve the right to disable any such systems from the network.

3.8. A network that is not installed and operated by ICT is deemed to be a private network and is not allowed to be connected to the University network without prior approval from ICT.

3.9. ICT reserve the right to control the quantity of bandwidth allocated to any device connected to the network.

3.10. ICT will impose network access controls where applicable to protect the network.

3.11. Applications such as peer to peer file-sharing, bitcoin mining, and network scanning are not permitted on the network without prior approval from ICT.