UNIVERSITY OF HULL

Acceptable Use Policy

Document Classification:	Policy
Data Classification:	Public
Version Number:	3.0
Status:	Approved
Approved by (Board):	University Leadership Team
Approval Date:	21 November 2023
Effective from:	21 November 2023
Next Review Date:	Annual
Document Authors:	IT Services – Cyber Security
Document Owner:	Director of Cyber Security
Department/Contact:	IT Services / support.hull.ac.uk
Summary:	This document details the policies that apply to anyone using IT provisioned systems and services to ensure that they are used safely, lawfully, and equitably.
Scope:	All University members and third parties using University owned or provisioned systems and services.
Relevant CIS Control(s):	Not applicable
Relevant legal frameworks:	See relevant section of overarching Information Governance and Assurance Policy
Related documents:	To be read in conjunction with IT Services Acceptable Use Policy (Guidance)
Published locations:	Public website (www.hull.ac.uk)
Document Communication and Implementation Plan:	Available upon request.

1 Introduction

1.1 This document details the policies that apply to anyone using IT Services' provisioned systems to ensure that they are used safely, lawfully, and equitably.

1.2 This policy should be read in conjunction with the accompanying **Acceptable Use Policy (Guidance)** and overarching **Information Governance and Assurance Policy**.

2 Scope

2.1 This policy applies to all University members, third parties, and visitors using university owned *enterprise assets*. Figure 1[1], below, defines what is meant by an enterprise asset and provides examples – although it should be noted that this list is not exhaustive.

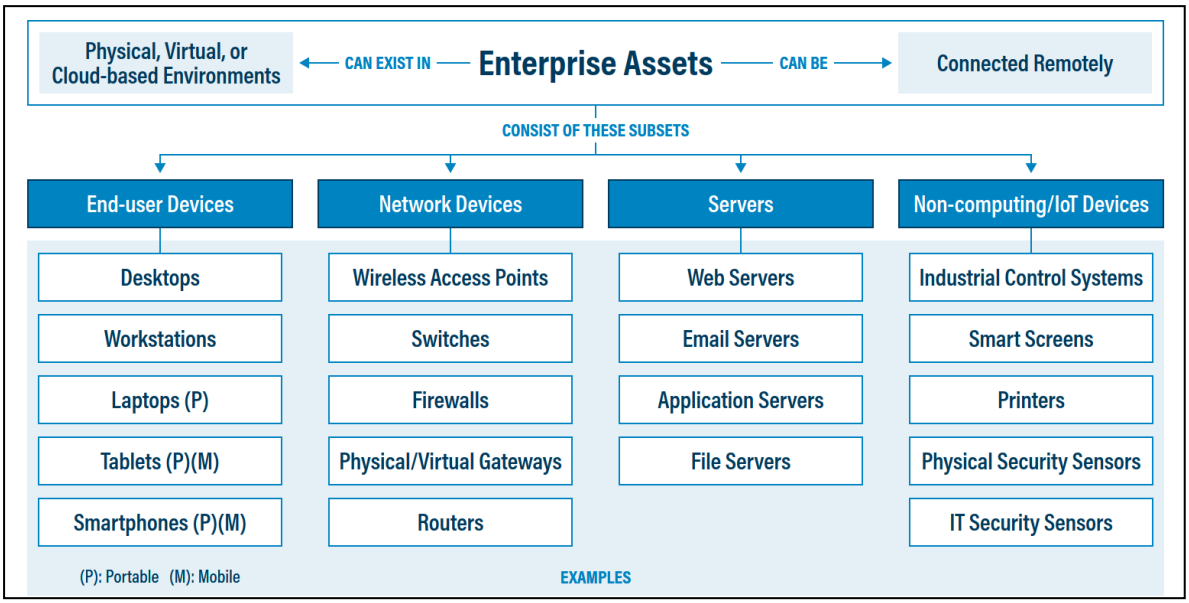

Figure 1:Enterprise Asset definition according to CIS Controls v8

2.2 This policy includes remote connections to the University's enterprise assets, as well as accessing the internet on university provisioned Wi-Fi networks.

2.3 For the purposes of this policy, the terms "you" and "your" are used to refer to all University members, third parties, and visitors.

3 Acceptable Use

3.1 The acceptable use policies are issued under the authority of the University Leadership Team. The Executive Director of Infrastructure Services is responsible for their interpretation and enforcement and may also delegate such authority to other people.

3.2 You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of these policies. If you feel that any such instructions are unreasonable or are not in support of these policies, you may appeal to the Executive Director of Infrastructure Services or through the University complaints procedures.

3.3 When using IT Services' systems, you remain subject to the same laws and regulations as in the physical world.

[1] https://www.cisecurity.org/insights/white-papers/acceptable-use-policy-template-for-the-cis-controls

3.4 It is expected that your conduct is lawful. In the UK, ignorance of the law is not a defence for unlawful conduct.

3.5 When accessing services located in a different country than where you reside, you must abide by the local laws of the country where you reside, as well as the laws applicable in any country where the service, or part of it, is located.

3.6 You are bound by the University's general regulations and policies when using IT Services systems, available at www.hull.ac.uk/policies.

3.7 You must abide by the terms and conditions of use published by any other organisation whose services you access.

3.8 When using services via Eduroam Wi-Fi (the roaming access service for international research and education institutions), you are subject to both the regulations and policies of this University and the institution where you are accessing services.

3.9 Software licences procured by the University will also set out terms and conditions for the user which should be adhered to. If you use any software or resources covered by a CHEST (Combined Higher Education Software Team) agreement, or Microsoft Licensing, you are deemed to have accepted their respective terms and conditions of use.

3.10 IT systems are provided for use in furtherance of the mission of the University of Hull, for example to support a course of study, research or in connection with your employment by the institution.

3.11 Use of certain licences is only permitted for academic or administrative use and may be subject to the terms and conditions laid out by the licensing authority.

3.12 You must take all reasonable precautions to safeguard any IT credentials (for example, a user ID and password, email address, smart card, multi-factor authentication (MFA) factors or other identity hardware) issued to you.

3.13 If you handle personal, confidential, or sensitive information, you must take all reasonable steps to safeguard it and must observe the University's **Data Protection policy** and information governance and assurance guidelines, available at www.hull.ac.uk/policies.

3.14 You must observe the University's **Information Governance Assurance Policy** and associated sub-policies and guidance, available at www.hull.ac.uk/policies.

3.15 Appropriate conduct when using IT Services' systems, extending to online activity including social networking platforms, are subject to university policies and regulations available at www.hull.ac.uk/policies.

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

3.17 IT Services reserve the right to control the quantity of bandwidth allocated to any device connected to the network.

3.18 You must return all university supplied IT assets, and any associated data, upon contract termination.

3.19 You must secure the physical environment around your workstation and lock your computer(s) when stepping away from your work area.

3.20 Further information can be found in the **Acceptable Use Policy (Guidance)**.

4 Prohibited Use

4.1 You must not use IT Services' systems without due authority. This is usually granted through the issuance of a user ID and password, or other IT Services credentials, and through the registration of an additional authentication factor.

4.2 Breach of any applicable law or third-party terms and conditions of use will also be regarded as a breach of these IT acceptable use policies.

4.3 IT infrastructure is all the underlying systems and services that constitutes the IT function. You must not do anything to jeopardise the confidentiality, integrity, or availability of the IT infrastructure by, for example, doing any of the following without approval:

- Damaging, reconfiguring, or moving equipment.
- Installing software on IT Services' systems other than in approved circumstances.
- Reconfiguring or connecting equipment to the network other than by approved methods.
- Setting up servers or services on the network without the express approval of IT Services.
- Deliberately or recklessly introducing malware.
- Attempting to disrupt or circumvent IT security measures.
- Attempting to impair the operation of the university, or external IT Services' systems through, for example, a denial of service (DOS) attack or penetration testing exercise.

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

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

4.6 You must not allow anyone else to use your IT credentials. Nobody has the authority to ask you for your password and you must not disclose it to anyone.

4.7 You must not attempt to obtain or use anyone else's credentials.

4.8 You must not impersonate someone else or otherwise disguise your identity when using IT Services' systems.

4.9 You must not infringe copyright or break the terms of licences for software or other material.

4.10 You must not attempt to access, delete, modify, or disclose information belonging to other people without their permission, or explicit approval from the University.

4.11 You must not access, create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist without the explicit approval from the University. The University of Hull has procedures to approve and manage valid activities involving such material.

4.12 You must not send spam (unsolicited bulk email).

4.13 You must not deliberately or recklessly consume excessive IT Services' resources, such as processing power, bandwidth, or consumables.

4.14 You must not use IT Services' systems in a way that interferes with others' valid use of them.

4.15 You must not attempt to monitor the use of IT Services' systems without explicit authority.

5 Personal Use

5.1 Limited use of IT Services' systems for personal activities is permitted – if it does not infringe any policies, including this policy, and does not interfere with others' valid use.

5.2 This is a privilege that may be withdrawn at any point. Use of IT Services' systems for non-institutional commercial purposes, or for personal gain, requires the explicit approval of the Executive Director of Infrastructure Services.

5.3 For further information, refer to the **Acceptable Use Policy (Guidance)**.

6 Expectations of Privacy

6.1 When using enterprise resources, you shall have no expectation of privacy. Access and use of the Internet, including communication channels, are not confidential, except in certain limited cases recognized by law.

6.2 IT Services will subject all devices connected to the network to regular asset discovery scans and will subject them to vulnerability scans.

6.3 The University of Hull monitors and records the use of IT systems; the purposes of which can be found in the **Acceptable Use Policy (Guidance)**.

7 Infringement

7.1 Infringing these policies may result in the withdrawal of services or sanctions under the institution's disciplinary processes. Offending material will be taken down.

7.2 Remedial action (e.g., ensuring IT Services' systems are free from malware) and/or training may be required before access is restored.

7.3 Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.

7.4 The University of Hull reserves the right to recover from you any costs incurred because of your infringement.

7.5 You must inform the Executive Director of Infrastructure Services if you become aware of any infringement of these policies.

8 Version History

Version	Date	Reviewed By
2.0	19 April 2021	Steph Jones, Stewart Doyle
3.0	19 September 2023	Hollie Huxstep, Carl McCabe, Nigel Kavanagh