# Acceptable Use Policy

**Document Reference:** IT-POL-107

**Document Classification:** Policy

**Data Classification:** Public

**Version number:** 4.0

**Relevant CIS Control(s):** Not Applicable

**Status:** Approved

**Approved by (Board):** University Leadership Team

**Approval date:** 03 June 2025

**Effective from:** 03 June 2025

**Review Frequency:** Annual

**Next review date:** 03 April 2026

**Document author:** Cyber Security

**Document owner:** Director of Technology

**Contact:** IT Services

**Collaborative provision:** No

State whether this document is applicable to the University's collaborative partners

**Related documents:** IT-POL-107a: Acceptable Use Policy (Guidance)

**University document:** No

*A University document applies across the institution, is approved by a committee of Council or Senate and is held in the University Policy Directory on SharePoint.*

**Published location:** Public Website

- The University has adopted the principles of Designing for Diverse Learners, and all policy documents should be written with reference to these principles. Further information is available at the Designing for diverse learners website.
- An Equality Impact Assessment (EIA) must be considered for all new and amended policies. Further information is available from the EIA section of SharePoint.
- This document is available in alternative formats from policy@hull.ac.uk.

# Acceptable Use Policy

## Table of Contents

# Acceptable Use Policy

## 1 Introduction

1.1 This document details the policies that apply to anyone using *IT resources* 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**.

1.3 A glossary of technical terms, which are defined in pink, underlined, and italicised, can be found at the end of this policy. Clicking on each term will take you to its definition.

1.4 If there is any part of this policy that requires clarification, please seek assistance from IT Services.

## 2 Scope

2.1 This policy, and all policies referenced herein, applies to all members of the University community, including faculty, students, administrators, staff, alumni, authorized guests, delegates, and independent contractors (the "End user(s)" or "you") who use the University's *IT resources*, also known as enterprise assets.

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

## 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 resources*, you remain subject to the same laws and regulations as in the physical world.

3.4 Your conduct must comply with legal, statutory or contractual obligations when using *IT resources*. 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 resources*, available at www.hull.ac.uk/policies. This includes the terms specified in this policy and applies when being used on or off campus – for example, when working from home.

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

3.8 The creation of information must be labelled and classified according to the guidelines described in the **Data Classification & Handling Policy**.

3.9 Similarly, any information that you send, receive, store, and process must be protected from unauthorised access – including, for example, another individual observing your screen or viewing what you have printed. This applies to digital and physical copies.

3.10 If you handle personal data, as defined under data protection legislation, or other types of confidential or sensitive information as defined by the University's internal policies, you must take all reasonable steps to safeguard it. You must also comply with the University's organisational policies, including the Data Protection Policy available on the University website. These standards also apply when handling the University's intellectual property, including research data and outputs.

3.11 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.

3.12 Measures must be taken to ensure that University portable / mobile devices – for example, laptops, tablets, and smartphones – are as protected and secure as possible. This applies when being used on and off campus.

3.13 Similarly, when using University devices off campus, they must access the University services via the use of a *VPN*, or other appropriate *encryption* standards. This does not apply to services that are accessed over the internet.

3.14 Mobile devices must *encrypt* stored data at rest.

3.15 *IT resources* 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.

3.16 When conducting University of Hull business, you must only use authorised IT devices. Personal devices that have been registered in the university's Mobile Device/ Application Management (*MDM* / *MAM*) platform are classed as authorised.

3.17 You must obtain authorisation to take University *IT resources* out of the United Kingdom. Authorisation can be obtained by completing this form.

3.18 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.

3.19 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.

3.20 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.

3.21 Where a password is required to access *IT resources*, it should be strong and unique, as outlined in the **Password and Multi-Factor Authentication Policy**.

3.22 You must observe the University's **Information Governance Assurance Policy** and associated sub-policies and guidance, available on the University website.

3.23 You must complete cyber security training and be aware of what *phishing* is, and how to determine if a message is legitimate or not.

3.24 If you receive any *phishing* emails, text messages, or phone calls, these must be reported to phishing@hull.ac.uk, and/or by using the reporting buttons found in Outlook.

3.25 Likewise, should you observe any cyber security incidents, or have any cyber security concerns, you should report these to the IT Service Desk.

3.26 Upon reporting a cyber security incident, you must comply with the instructions provided to you from IT Services.

3.27 You must return all university supplied IT assets, and any *organisational data*, upon contract termination, or when requested.

3.28 You must secure the physical environment around your workstation and lock your computer(s) when leaving your work area.

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

## 4 Internet Usage

4.1 Internet access has been provided for university business purposes.

4.2 Whilst personal use is permitted, it should be restricted and in accordance with section 7: Personal Use of this policy.

4.3 Whilst security measures have been put in place to minimise the risk of, for example, a cyber-attack or data breach, you should remain vigilant whilst using the internet and take every step possible to protect the University, and any *organisational data* from danger.

4.4 Appropriate conduct when using *IT resources*, extending to online activity including social networking platforms, are subject to university policies and regulations available on the University website.

4.5 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.

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

4.7 You must not use the internet to access material that has been deemed as inappropriate, as described in the **Web Filtering Policy**. Note that what is regarded as inappropriate is subject to change.

4.8 You must not request that any personal goods and services are delivered to the University.

4.9 You must not impersonate the identity of another individual when using the internet.

4.10 Using *IT resources* is subject to logging and monitoring.

4.11 **Social Media Usage**

4.11.1 When referring to the University on social media, it must be stated that you are posting on your own behalf.

4.11.2 You must not use social media on behalf of the University of Hull, unless you have been properly authorised to do so.

4.11.3 Similarly, you must not use personal accounts, including social media accounts, to post on behalf of the organisation.

## 5 Electronic Messaging

5.1 This section of the policy refers, but is not limited, to SMS text messages, messaging applications, web chats, and social media platforms. This section also applies to messages that have been deleted.

5.2 When utilising messaging tools, they should be only be used for legitimate university purposes.

5.3 Electronic messages are classed as *organisational data* and are therefore owned by the University.

5.4 Consequently, the University has the right to monitor and audit electronic messages, as described in section 8: Expectations of Privacy. The **Acceptable Use Policy (Guidance)** explains the purposes for auditing and monitoring *IT resources*, including electronic messages.

5.5 Care must be taken to ensure that messages containing sensitive information are only sent to the intended recipients.

5.6 Organisational messages should be handled as official communications and therefore be treated accordingly.

5.7 Messages must not be set to auto-forward. This includes forwarding messages from a University account to a personal account.

5.8 Consideration must be given to the size of messages and mailboxes.

5.9 You must not send unnecessary messages to large distribution groups.

5.10 You must not send spam (unsolicited bulk email), or messages for commercial purposes.

5.11 You must not send messages that would bring the University of Hull into disrepute.

5.12 You must ensure that messages do not contain offensive material, in alignment with point 6.13, or do not infringe copyright.

5.13 If you receive any junk messages, including *phishing* attempts, you must not reply to them.

5.14 Similarly, you must not open, send or forward messages that contain *malware*.

5.15 You must report abuse, or violation of messaging systems – including receiving *malware*, to IT Services.

## 6 Prohibited Use

6.1 You must not use *IT resources* without due authority. This is usually granted through the creation of a University user account and subsequent issuance of a user ID and password, or other IT Services credentials, and through the registration of an additional authentication factor.

6.2 University user accounts must not be used for personal use, and you must not store personal information on *IT resources*.

6.3 You must not attempt to access *IT resources* that you have not been given appropriate authorisation to access. If you cannot access a service, and believe you have a business justification, please contact the appropriate service owner or IT Services.

6.4 For end users that have been issued a privileged (or administrative) user account, it is prohibited to use a privileged user account when conducting "business as usual" (BAU) activities, for example, email or using a web browser.

6.5 *Organisational data* must not be accessed with a personal user account. A personal user account has not been created by the University and will not be protected by the same level of security measures as your university account.

6.6 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.

6.7 You must not do anything to jeopardise the confidentiality, integrity, or availability of *IT resources* by, for example, doing any of the following without approval:

- Damaging, reconfiguring, or moving equipment, except where appropriately authorised (e.g., a university-provisioned laptop). This includes the removal of asset stickers, or any other identifying marks.
- Installing software on *IT resources* other than in approved circumstances.
- Reconfiguring or connecting unauthorised equipment to the University's network.
- Setting up servers or services on the network without the express approval of IT Services.
- Deliberately or recklessly introducing *malware*.
- Attempting to disrupt, disable, or circumvent IT security measures, including anti-virus software.
- Attempting to impair the operation of the university, or external *IT resources* through, for example, a denial of service (DOS) attack or penetration testing exercise.

6.8 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.

6.9 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.

6.10 You must not allow anyone else to use your IT credentials (including your username and password). Nobody, not even IT Services, has the authority to ask you for your password and you must not disclose it to anyone.

6.11 You must not attempt to obtain or use anyone else's credentials (including another individual's username and password).

6.12 You must not impersonate someone else or otherwise disguise your identity when using *IT resources*, including sending anonymous messages.

6.13 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.

6.14 You must not infringe copyright or break the terms of licences for software or other material, for example, when sending messages or conducting activities on behalf of the University.

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

6.16 You must not deliberately or recklessly consume excessive *IT resources*, such as processing power, bandwidth, or consumables.

6.17 You must not use *IT resources* in a way that interferes with others' valid use of them.

6.18 You must not attempt to monitor the use of *IT resources* without explicit authority.

## 7 Personal Use

7.1 Limited use of *IT resources*, including internet use, for personal activities is permitted – if it does not affect legitimate organisational purposes, infringe any policies, including this policy, and does not interfere with others' valid use.

7.2 University user accounts must not be used for personal use. This includes, but is not limited to, using your university email address to register for online banking and shopping websites.

7.3 In addition to the above, *IT resources* must not be used to store personal information, for example files and photographs.

7.4 University user accounts, and *IT resources* (including emails and teams messages), may be subject to disclosure to Rights Requests under either the Freedom of Information Act 2000 or the Data Protection Act 2018.

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

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

## 8 Expectations of Privacy

8.1 When using *IT 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.

8.2 *IT resources*, including university user accounts, must not be used for personal use. The University of Hull, in conjunction with IT Services, reserves the right to monitor, audit, and record the use of IT systems; the purposes of which can be found in the **Acceptable Use Policy (Guidance)**.

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

8.4 Those authorised to audit and monitor shall only do so with appropriate authorisation and where there is a legitimate business requirement.

## 9 Infringement

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

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

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

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

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

## 10 Glossary of Terms

10.1 *Encryption* = The process of encoding a message or information in such a way that only authorized parties can access it[1]. This provides an additional level of security, even greater than that of a password, by scrambling a file, for example, so that they cannot be opened unless correctly *decrypted*. This is like the use of a lock and key, where the use of a pseudo-random encryption key is generated by an algorithm. Encryption itself does not prevent interference but does hide the actual content of a file from a would-be interceptor. Data can be encrypted whilst it is in its 'rest state' (i.e., stored on a disk), whilst it is being transmitted from one device to another, and whilst it is 'in use' (i.e., being processed)[2].

[1] https://www.cloudflare.com/learning/ssl/what-is-encryption/
[2] https://cloud.google.com/docs/security/encryption-in-transit

10.1.1 *Decryption* = The process of using a 'key' to unscramble information. An authorized recipient, who possesses the key (encryption algorithm), can easily decrypt the message with the key provided by the originator[3]. It is theoretically possible to decrypt the message without possessing the key, but considerable computational resources and skills are required to 'crack'.

10.2 *IT Resources* = Also known as an enterprise asset, these refer to a resource, owned by an enterprise (the University of Hull), with the potential to process or store data[4]. These include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services. 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.

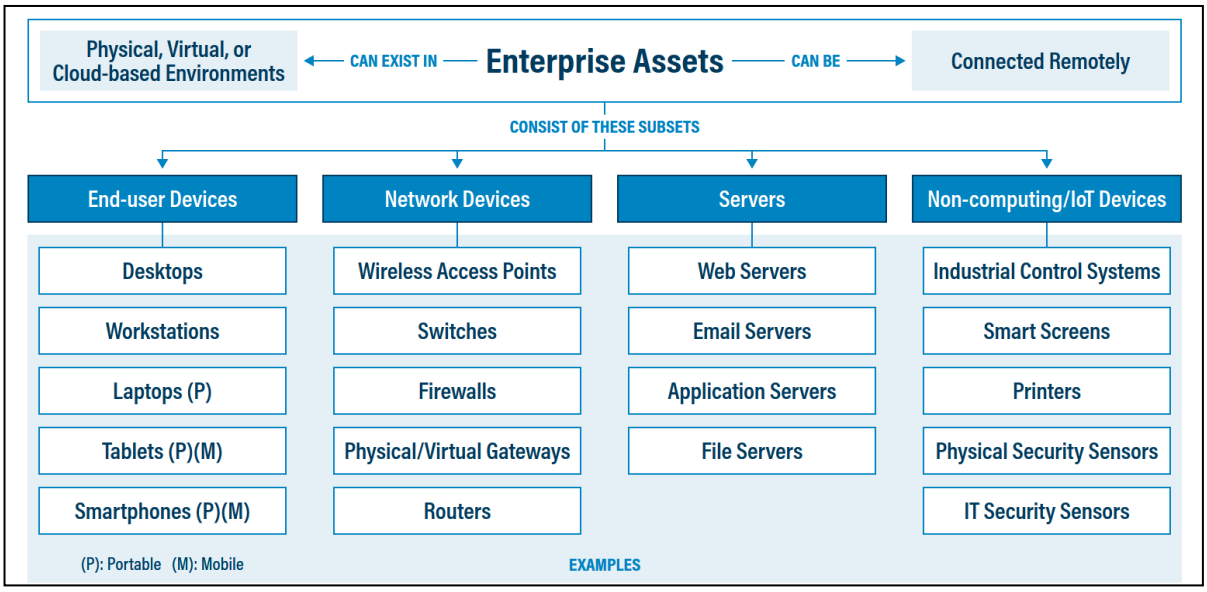


*Figure 1:Enterprise Asset definition according to CIS Controls v8*

10.3 *Malware* = Any malicious software (truncated to 'malware') used to disrupt computer operation or subvert security. There are lots of different types of malware, including viruses, trojans, worms, rootkits, keyloggers, and ransomware. It is usually spread by visiting websites of a dubious nature, downloading files from untrusted sources, opening email attachments from people you do not know or inserting media that has been created on compromised desktops.

[3] https://www.techtarget.com/searchsecurity/definition/cryptography
[4] CIS Controls Acceptable Use Policy Template (https://www.cisecurity.org/insights/white-papers/acceptable-use-policy-template-for-the-cis-controls)

10.4 *Mobile Application Management* = Often referred to as MAM, this approach allows the University to define and centrally manage cyber-security and data compliance policies to protect application data regardless of the device that is being used[5] [6]. This balances the usability of *BYOD*s against securing *organisational data* and minimising data breaches.

10.4.1 *Personal Device (BYOD)* = A 'Bring your own Device' (BYOD) may also be referred to as a personal device. This term is used when University staff, postgraduate students involved in research, third parties, and visitors use their own personal end-user device, as described in figure 1, to access University resources, services or systems, and data[7]. Whilst the device is the sole responsibility of the end user, it is important to remember that the University still owns the organisational data and resources that are used to complete the business function[8].

10.5 *Mobile Device Management* = Also known as MDM, this is a device-centred management approach[9]. MDM is a more in-depth approach when compared to *Mobile Application Management (MAM)* in that MDM can manage device configuration, device features and infrastructure services in addition to application (and therefore *organisational data*) management[10]. This approach allows the University to define and centrally manage cyber-security and data compliance policies in more depth, compared to MAM solutions. Given that the university has full control on the security controls baselines that are implemented, MDM is used to provide a higher level of assurance on devices that have been recognised as accredited.

10.6 *Organisational Data* = Electronic data owned by the university; this can include any research data, office documents, financial data, and even email.

10.7 *Phishing* = The process of coercing individuals in to revealing sensitive information or performing an action for criminal reasons[11]. Attackers will attempt to influence users to do something they would not normally do, by pretending to be somebody else.

10.8 *VPN* = A VPN (virtual private network) provides secure connectivity between devices in physically separate locations[12]. This allows for secure access to university resources, even when not physically on campus, and decreases unauthorised access attempts.

---

[5] https://www.trio.so/blog/mobile-application-management/
[6] https://learn.microsoft.com/en-us/mem/intune-service/fundamentals/what-is-intune
[7] https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device
[8] https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device
[9] https://learn.microsoft.com/en-us/mem/intune-service/fundamentals/what-is-intune
[10] https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/mobile-device-management
[11] https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering?v2=1
[12] https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks

## 11 Responsible, Accountable, Consulted, and Informed (RACI) Matrix

11.1 A form of a responsibility assignment matrix (RAM) commonly used in project management[13]. A RACI matrix defines who is involved in the successful completion / implementation of a project, task, or in this case, a policy[14]. A brief definition of each role is given in the table below.

11.2 The table below outlines the roles that are involved in ensuring this policy is adhered to, enforced, and kept up to date.

| | Definition | Role |
|---|---|---|
| Responsible (R) | Answerable for the correct completion of the task | IT Services |
| Accountable (A) | Delegates and must sign off (approve) the work that those *responsible* provide | Executive Director of Infrastructure Services |
| Consulted (C) | Provide input based on how this will impact their domain of expertise | Information Governance Committee |
| Informed (I) | Those who are kept up to date on progress | University Leadership Team |

## 12 Version Control

| Version | Author | Date approved | Relevant section(s) |
|---|---|---|---|
| 2.0 | Steph Jones, Stewart Doyle | 19 April 2021 | All |
| 3.0 | Hollie Huxstep, Carl McCabe, Nigel Kavanagh | 19 September 2023 | All |
| 4.0 | Hollie Felice, Carl McCabe, Nigel Kavanagh | 09 April 2025 | All |
| | | | |

[13] https://www.forbes.com/uk/advisor/business/software/raci-chart/
[14] https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/