UNIVERSITY OF HULL

Acceptable Use Policy (Guidance)

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 expands on the principles set out in the IT Services Acceptable Use Policy and is intended to provide guidance for anyone using IT provisioned systems and services to ensure accordance with it.
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 the IT Services Acceptable Use Policy
Published locations:	Public website (www.hull.ac.uk)
Document Communication and Implementation Plan:	Available upon request.

1 Introduction

1.1 This document expands on the principles set out in the **Acceptable Use Policy**. It provides many examples of the details and the specific situations and is intended to help you relate your everyday use of IT Services' systems to ensure accordance with it.

1.2 Where a list of examples is given, these are just some of the most common instances, and the list is not intended to be exhaustive.

1.3 Where terms similar to *Authority*, *Authorised*, *Approved,* or *Approval* appear, they refer to authority or approval originating from the person or body identified in section 3.1, or anyone with authority delegated to them by that person or body. The term 'Approval from the University' is used where procedures and policies require approval or authorisation outside of the **Acceptable Use Policy** or this guidance.

2 Scope

2.1 The IT Services Acceptable Use Policy applies to all University members, third parties, and visitors also referred to as "users." In addition to University staff and students it could include, for example:

- Visitors to the University website, and people accessing the University's online services from off campus.
- Members of Council and associated committees, honorary staff, visiting academics and other associate members of the University, including alumni.
- External partners, contractor and agents based onsite and using the University's network, or offsite and accessing the University's systems.
- University tenants using the University's desktop, servers, or network.
- Visitors using the University's guest wireless service.
- Students and staff from other institutions using Eduroam.

2.2 *Enterprise assets* are resources with the potential to process or store data. Examples are described in figure 1[1] below and can include:

- IT hardware that the University provides, such as desktop workstations, laptops, tablets, smartphones, and printers.
- Software that the University provides, such as operating systems, office application software, mobile apps, web browsers etc. It also includes software that the institution has arranged for you to have access to, for example exclusive deals for students on commercial application packages.
- Services that the University provides, such as social media, web applications, email and other services relating to domain names owned by the University.
- Data that the University provides or arranges access to. This might include online journals, data sets or citation databases.
- Online services arranged by the University, such as online information resources or Office 365.
- IT credentials, such as the use of your University user ID and password, or any other token (e.g., email address, OTP key) issued by the University to identify yourself when using IT Services' systems. For example, you may be able to use drop in facilities or wireless connectivity at other institutions using your usual user ID and password through Eduroam. While doing so, you are subject to University regulations, as well as the regulations at the institution you are visiting.

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

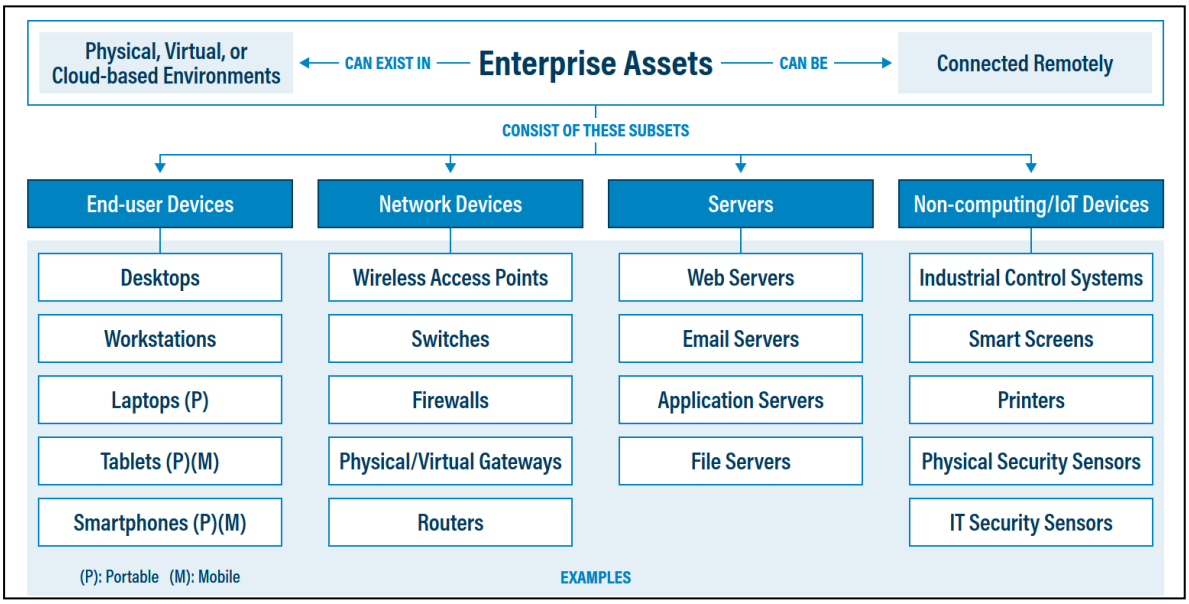

Figure 1:Enterprise Asset definition according to CIS Controls v8

2.3 During work or studies, staff, and students (particularly research students) may handle information that comes under the **Data Protection Act** or **General Data Protection Regulations (GDPR)** or is sensitive (e.g., Personal Identifiable Information, PII) or confidential in some other way. These types of data will be referred to as *protected information* throughout this policy.

2.4 Safeguarding the security of protected information is a complex issue, with organisational, technical, and human aspects. The University policies and guidelines on Data Protection and Information Assurance are available at www.hull.ac.uk/policies, and if your role is likely to involve handling protected information you must make yourself familiar with, and abide by, these policies and guidelines. Considerations include:

- When sending protected information electronically, you must use a method with appropriate security. Email is not inherently secure. Guidance on how to send protected information electronically should be sought from the Data Protection Officer.
- Automatic forwarding from a University email to a personal or non-partner organisation email account is not permitted, as this puts protected information at risk of breach.
- Information must not be stored on removable media (such as USB storage devices, removable hard drives, CDs, DVDs) or mobile devices (laptops, tablets, or smartphones) unless it is encrypted, and can be stored and transported securely.
- If you access protected information from off campus, you must make sure you are using an approved connection method that ensures that the information cannot be intercepted between the device you are using and the source of the secure service. You must also be careful to avoid working in public locations where your screen can be seen.
- When using an approved connection method, devices that are not managed by the University (personal devices) may be more likely to contain malicious software that could, for example, gather keyboard input and screen displays. You need to be aware of this risk if considering using such devices to access, transmit or store protected information.
- Do not store protected information in cloud-hosted services that are not provided or sanctioned by the University. A current list of approved cloud providers can be found on the support portal. You should also consider how access to any information could be granted in your absence, if required, for business continuity.

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 Authority to use the University's IT Services' systems are granted by a variety of means:

- The issue of a user ID and password or other IT credentials.
- The explicit granting of access rights to a specific system or resource.
- The provision of a facility in an open access setting, such as an institutional website, a self-service kiosk in a public area, or a guest wireless network on the campus.

3.4 If you have any doubt whether you have the authority to use an IT system, you should seek further advice from IT Services.

3.5 It is important to remember that using IT has consequences in the physical world. Your use of IT is governed by IT specific laws and regulations, but it is also subject to general laws and other University policies, regulations, and procedures. It is expected that your conduct is lawful. In the UK ignorance of the law is not a defence for unlawful conduct.

3.6 Your behaviour is subject to the domestic laws of the land, even those that are not explicitly related to IT such as the laws on fraud, theft, and harassment. There are many items of legislation that are particularly relevant to the use of IT, including:

- Obscene Publications Act 1959 and 1964.
- Protection of Children Act 1978.
- Police and Criminal Evidence Act 1984.
- Copyright, Designs and Patents Act 1988.
- Computer Misuse Act 1990.
- Defamation Act 1996 and 2013.
- Data Protection Act 1998 and 2018 (General Data Protection Regulation, GDPR).
- Human Rights Act 1998.
- Regulation of Investigatory Powers Act 2000.
- Freedom of Information Act 2000.
- Freedom of Information (Scotland) Act 2002.
- Privacy and Electronic Communications (EC Directive) Regulations 2003.
- Prevention of Terrorism Act 2005.
- Terrorism Act 2006.
- Police and Justice Act 2006.
- Criminal Justice and Immigration Act 2008.
- Equality Act 2010.
- Counter-Terrorism and Security Act 2015.

3.7 If you are using services that are hosted in a different part of the world you may also be subject to foreign law. It can be difficult to know where a service is hosted from and what the applicable laws are

in that locality. In general, if you apply common sense, obey domestic laws and the regulations of the service you are using, you are unlikely to go astray.

3.8 You should already be familiar with the University of Hull general regulations and policies, available at www.hull.ac.uk/policies.

3.9 If you use IT systems to access a third-party service or resources, you are bound by the policies associated with that service or resource (the association can be through something as simple as using your University user ID and password). Very often, these policies will be presented to you the first time you use the service, but in some cases the service is so pervasive that you will not even know that you are using it. Examples of this include:

- When connecting to any site outside the University, Janet will be used, and therefore subject to the Janet Acceptable Use Policy[2], the Janet Security Policy[3], and the Janet Eligibility Policy[4]. The requirements of these policies have been incorporated into the acceptable use policy, so if you abide by these then you should not infringe Janet policies.
- When procuring digital content for University use, these are subject to the terms of Jisc Collections[5].
- CHEST is an organisation that has negotiated many deals for software and online resources on behalf of the UK higher education community, under the common banner of CHEST agreements[6]. These agreements have certain restrictions, for instance non-academic use is not permitted.
- Use of any Office 365 services provided by Microsoft[7].

3.10 There will be other instances where the University has provided you with a software package, service, or resource. These are bound by licence agreements which vary from supplier to supplier. You must only use software, services, and other resources in accordance with all applicable licences, terms, and conditions.

3.11 The use of IT systems is provided for use in furtherance of University's mission. Such use might be for:

- Learning.
- Teaching.
- Research.
- Knowledge transfer.
- Public outreach.
- Commercial activities of the University.
- Or the administration necessary to support all the above.

3.12 Many IT systems provided or arranged by the University require you to identify yourself so that the system knows that you are entitled to use it. This is commonly done by providing you with a user ID and password, but other forms of IT credentials may be used, such as an email address, a smart card, multifactor authentication (via a smartphone app or SMS), or some other form of security device. When doing so:

- You must take all reasonable precautions to protect this identity and safeguard any IT credentials issued to you.

[2] https://community.ja.net/library/acceptable-use-policy
[3] https://community.ja.net/library/janet-policies/security-policy
[4] https://community.ja.net/library/janet-policies/eligibility-policy
[5] https://www.jisc.ac.uk/jisc-collections
[6] https://www.chest.ac.uk/agreements
[7] https://www.microsoft.com/en-gb/servicesagreement/

- You must change passwords when first issued and as instructed.
    - Do not use obvious passwords.
    - Do not record passwords where there is any likelihood of someone else finding them.
    - Do not use the same password as you do for personal (i.e., non-University) accounts.
    - Do not share passwords with anyone else, even IT staff, no matter how convenient and harmless it may seem.
    - Password guidance can be found at support.hull.ac.uk.
- If you think someone else has found out what your password is, change it immediately and report the matter to IT Services.

3.13 Almost all published works are protected by copyright. If you are going to use material (images, text, music, software), the onus is on you to ensure that you use it within copyright law. This is a complex area, and further guidance is available at libguides.hull.ac.uk/copyright. The key point to remember is that because you can see something on the web, download it or otherwise access it, it does not mean that you can do what you want with it.

3.14 University policies and regulations apply to appropriate conduct in the use of IT systems and extend to online activity including social media. These are available at www.hull.ac.uk/policies, and include, but are not limited to:

- Bullying and Harassment Policy.
- Disciplinary Policy and Procedure.
- Diversity and Inclusion Policy.
- Anti-Fraud and Bribery Policy.
- Code of Practice on Freedom of Speech.
- Library Regulations.
- Code of Student Conduct.

3.15 When using shared spaces, remember that others have a right to work without undue disturbance. Keep noise down (turn phones to silent if you are in a silent study area), do not obstruct passageways, and be sensitive to what others around you might find offensive.

3.16 If you have been issued with any University enterprise assets, throughout the course of your employment, research, or study, you must return these assets upon completion of your contractual employment, research project, degree, or upon contract termination.

3.17 When stepping away from your work area, you must ensure that:

- Your computer screen has been locked.
- No protected information is on display on your work area.
- No login information is on display.

3.18 Where IT is itself the subject of study or research, special arrangements must be made with the approval of the Executive Director of Infrastructure Services by the school or faculty.

4 Prohibited Use

4.1 Attempting to use or access IT systems which the University has not authorised you to use, or access, may be an offence under the **Computer Misuse Act**.

4.2 You must not use IT systems without due authority. This is usually granted through the issuance of a user ID and password or other IT credentials.

4.3 You must not:

- Create or transmit, or cause the transmission, of any offensive, obscene, or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Create or transmit material with the intent to cause annoyance, inconvenience, or needless anxiety.
- Create or transmit material with the intent to defraud.
- Create or transmit defamatory material.
- Create or transmit material that is discriminatory on the grounds of race, age, sex, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, religion, belief, or sexual orientation.
- Create or transmit material likely to incite hatred or terrorism.
- Create or transmit material such that this infringes the copyright of another person or organisation.
- Create or transmit unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their user organisation has chosen to subscribe.
- Deliberately and without authorisation access networked facilities or services.

4.4 Do not use your University user ID and password (credentials) to log in to websites or services you do not recognise, and do not log in to websites that are not secured.

4.5 Do not use your university credentials to sign up for websites you access in your personal time. For example, social media, shopping, or banking websites.

4.6 Do not allow anyone else to use your smartcard or other security hardware. Take care not to lose them, and if you do, report the matter to IT Services immediately.

4.7 Never use someone else's IT credentials or attempt to disguise or hide your real identity when using the University's IT systems. It is, however, acceptable not to reveal your identity if the system or service clearly allows anonymous use (such as a public facing website).

4.8 You must not attempt to disrupt, borrow, corrupt, or destroy someone else's IT credentials, or otherwise compromise their identity.

4.9 You must not do anything to jeopardise the University's IT Infrastructure. This includes attempting to impair the operation of any IT system, whether at the University or belonging to another organisation. Examples of this include:

- Damaging, or doing anything to risk physically damaging the infrastructure, such as being careless with food or drink at a workstation. Use of University IT equipment off campus, including limited personal use, must be approved by your department, faculty, or service area.
- Attempting to reconfigure the setup of IT infrastructure without authorisation, such as changing the network point that a device is plugged in to, connecting devices to the network (except of course for wireless or wired networks specifically provided for this purpose) or altering the configuration of University 'managed' devices. Unless you have been authorised, you must not add software to or remove software from University devices.
- Moving equipment without authority.
- You must not extend or disrupt the configuration of the wired or wireless network without authorisation. Such activities, which may involve the use of switches, repeaters, hubs, or wireless access points, can disrupt the network and are likely to be in breach of the Janet Security Policy.

- You must not set up any hardware or software, such as a server, that would provide a service to others over the network without permission. Examples would include games servers, file sharing services, bit-coin mining servers, or websites.
- You must take all reasonable steps to avoid introducing malware to the infrastructure. The term malware covers many things such as ransomware, viruses, worms, trojans, and spyware, but is, essentially, any software used to disrupt computer operation or subvert security. 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.
- IT Services has taken measures to safeguard the security of its infrastructure, including the provision of anti-malware, firewalls, intrusion monitoring and detection, and spam filters. You must not attempt to subvert or circumvent these measures in any way.

4.10 You must not attempt to access, delete, modify, or disclose restricted information belonging to other people without their permission, unless it is obvious that they intend others to do this, or you are specifically authorised to do so having obtained approval from the University.

4.11 Where information has been produced in the course of employment or study at the University, and the person who created or manages it is unavailable, authorisation may be granted to retrieve the information for work purposes. Those acting on such authorisation must take care not to retrieve any personal information in the account, nor to compromise the security of the account concerned. Contact the Data Protection Officer for further guidance;

4.12 Personal information may only be accessed by someone other than the owner under extremely specific circumstances governed by University and/or legal processes.

4.13 You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory, or extremist. The University reserves the right to block or monitor access to such material.

4.14 The University has procedures to approve and manage valid activities involving such material for valid research purposes, where legal, and with the appropriate ethical approval. For more information, please refer to your faculty ethics officer. Universities UK has also produced guidance on handling sensitive research materials[8];

4.15 The University has a statutory duty, under the **Counter Terrorism and Security Act**, and termed "Prevent," to aid the process of preventing people being drawn into terrorism.

4.16 There is a limited exemption to this policy covering authorised IT Services staff involved in the preservation of evidence for the purposes of investigating breaches of University regulations or the law.

4.17 Publishing means the act of making information available to the public, this includes through websites, social networks, and news feeds. Whilst the University encourages publication, there are some general guidelines you should adhere to:

- You must not make statements that declare to represent the University without approval. If in any doubt, you must consult the Registrar's office for advice.
- You must not publish information on behalf of third parties using the University's systems and services without approval.

[8] https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/security-sensitive-research-material-UK-universities-guidance.aspx

- You must not publish any material that would bring the University into disrepute.
- You must not publish any information which the University is contractually obliged to keep confidential, or which would breach any law. Guidance can be sought from the Marketing and Communication Directorate for further advice on publishing information.

4.18 You must not send unsolicited ('spam') bulk emails or chain emails other than in specific circumstances. Advice on this is available from IT Services.

4.19 If you are using shared IT systems, for personal or social purposes, you should make them available to others with work to do. Similarly, you should not occupy specialist facilities unnecessarily if someone else needs them.

4.20 Do not consume excessive bandwidth by uploading or downloading more material (particularly video) than is necessary.

4.21 Do not waste paper by printing more than is needed, or by printing single sided if double sided would suffice.

4.22 Do not waste electricity by leaving equipment needlessly switched on.

4.23 You must not attempt to monitor the use of IT Services' systems without explicit approval from the Executive Director of Infrastructure Services. This includes:

- Monitoring of network traffic.
- Network and/or device discovery – such as 'port scanning;'
- Wireless traffic capture.
- Installation of key logging or screen grabbing software that may affect users other than yourself.
- Penetration testing.
- Attempting to access system logs, servers, or network equipment.

5 Personal Use

5.1 You may currently use IT systems for limited personal use providing it does not breach the **Acceptable Use Policy and** does not prevent or interfere with other people using the facilities for valid purposes. It should be noted that:

- Personal use of IT systems is a concession and can be withdrawn at any time.
- Employees using IT systems for non-work purposes during working hours are subject to the same management policies as for any other type of non-work activity.
- Note that personal data may be wiped if the managed device is deemed compromised in any way.
- Use of University equipment for any personal means must be approved by your department, faculty, or service area. Allowing a family member to use a university owned device in a way that may expose information would constitute a breach.

5.2 Use of your University email account for personal use is forbidden. This includes using your University email address when registering for websites that are not related to work.

- This increases the risk to the University from 'phishing' emails including those containing malware.

- The University may need to authorise access to your email by other colleagues to ensure business continuity; using a non-University (personal) email account for personal correspondence and activities will minimise any privacy risks.

5.3 Use of IT Services' systems for non-University commercial purposes, or for personal gain or interest, such as private consulting, running a private club or society, requires explicit approval. The provider of the service may require a fee or a share of the income for this type of use. For more information, please consult IT Services in the first instance. Even with such approval, the use of licences under the CHEST agreements for anything other than teaching, studying or research, administration or management purposes is prohibited, and you must ensure that licences allowing commercial use are in place.

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 by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by law.

6.2 The University monitors and logs the use of IT systems for the purposes of:

- Detecting, investigating, or preventing misuse of the systems and services, or for breaches of University regulations.
- Detecting, investigating, or preventing cyber security risks.
- Monitoring the effective function of the systems and services and the University.
- Investigation of alleged misconduct.
- The University will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating, or preventing crime, and ensuring national security.

7 Infringement

7.1 Breaches of these policies will be handled by the University's disciplinary processes, available at www.hull.ac.uk/policies. This could have a bearing on your future studies or employment with the University and beyond. Sanctions may be imposed if the disciplinary process finds that you have indeed breached the policies, for example:

- Imposition of restrictions or removal of your use of IT systems and enterprise assets.
- Withdrawal of offending material.
- Fines and recovery of any costs incurred by the University because of the breach.

7.2 If the University believes that unlawful activity has taken place, it will refer the matter to the police or other enforcement agency.

7.3 If the University believes that a breach of a third party's regulations has taken place, it may report the matter to that organisation.

7.4 If you become aware of an infringement of these policies, you must report the matter to IT Services or to the Executive Director of Infrastructure Services.

8 Version History

Version	Date	Reviewed By
2.0	20 July 2021	Steph Jones, Stewart Doyle
3.0	19 September 2023	Hollie Huxstep, Carl McCabe, Nigel Kavanagh