Policy cover sheet

Policy title:	**ICT Regulations: guidance notes**
Scope:	These regulations apply to anyone using the ICT facilities (hardware, software, data, network access, third party services, online services or ICT credentials) provided or sanctioned by the University.
With effect from:	27 November 2015
Other related policies	ICT Regulations: core regulations ICT Regulations: simplified code
Contact for further information:	Registrar's office
Approved by	Exec
Policy approved date	3 November 2015
Next due for review	November 2016
Relevant legal framework:	See *Section 2: Compliance*
Equality analysis	The implementation of this policy is not considered to have a negative impact on protected characteristics.
Freedom of Information	This document will be publicly available through the University's Publication Scheme under the Freedom of Information Act 2000
Version	1.5
Status	Approved.

Change control

Version	Changes
1.0	Initial version, based on UCISA model regulations
1.1	Formatting and tailoring to the University of Hull. Changes reflecting *Prevent* guidance from UK government.
1.2	Changes after review by Director of ICT and Deputy Secretary
1.3	Changed references to *IT* to *ICT* and other minor edits
1.4	Changes after legal review by University Solicitor and feedback from IT Operations Group
1.5	Changes after review by Executive

ICT Regulations – Guidance notes

This guidance expands on the principles set out in the core regulations. It gives many examples of specific situations and is intended to help you relate your everyday use of the ICT (Information and Communication Technology) facilities to the *Do's and Don'ts* in the core regulations.

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.

Where the 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*,* Authority*,* 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 ICT core regulations or guidance.

1) Scope

1.1 Users

The ICT regulations apply to anyone using the University of Hull's ICT facilities. 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 computers, servers or network;
- Visitors using the University's wireless service;
- Students and staff from other institutions logging on using Eduroam.

1.2 ICT facilities

ICT facilities include:

- ICT hardware that the University of Hull provides, such as PCs, laptops, tablets, smart phones 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, special 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 of Hull provides, or arranges access to. This might include online journals, data sets or citation databases;
- Access to the network provided or arranged by the University. This would cover, for example, connectivity to the internet from University PCs, on campus wi-fi and network connections in University managed student residences.
- Online services arranged by the University, such as online information resources, Box or Office 365.
- ICT credentials, such as the use of your University user ID and password, or any other token (email address, smartcard, dongle) issued by the University of Hull to identify yourself when using ICT facilities. For example, you may be able to use drop in facilities or wi-fi connectivity at other institutions using your usual user ID and password through the Eduroam system. While doing so, you are subject to University regulations, as well as the regulations at the institution you are visiting.

2) Compliance

It is helpful to remember that using ICT has consequences in the physical world.

Your use of ICT is governed by ICT specific laws and regulations, but it is also subject to general laws and other University regulations, policies and procedures.

2.1 Domestic law

Your behaviour is subject to the laws of the land, even those that are not apparently related to ICT such as the laws on fraud, theft and harassment.

There are many items of legislation that are particularly relevant to the use of ICT,

including:

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

So, for example, you may 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 or 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.

2.2 Foreign law

If you are using services that are hosted in a different part of the world, you may also be subject to their laws. It can be difficult to know where any particular 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.

2.3 General University regulations

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

2.4 Third party regulations or terms and conditions of use

If you use the University of Hull's ICT facilities to access third party service or resources you are bound by the regulations 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 regulations 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.

Two examples of this would be:

- *Using Janet, the network that connects all UK higher education and research institutions together and to the internet*
  When connecting to any site outside the University of Hull you will be using Janet, and subject to the Janet Acceptable Use Policy, https://community.ja.net/library/acceptable-use-policy the Janet Security Policy, https://community.ja.net/library/janet-policies/security-policy and the Janet Eligibility Policy https://community.ja.net/library/janet-policies/eligibility-policy.
  The requirements of these policies have been incorporated into these regulations, so if you abide by these regulations you should not infringe the Janet policies.

- *Using Chest agreements*
  Eduserv 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*. These agreements have

certain restrictions, that may be summarised as: non-academic use is not permitted; copyright must be respected; privileges granted under *Chest agreements* must not be passed on to third parties; and users must accept the User Acknowledgement of Third Party Rights, available at www.eduserv.org.uk/services/Chest-Agreements/about-our-licences/user-obligations

There will be other instances where the University of Hull has provided you with a piece of software or a resource.

- **Licence agreements**
  You must only use software and other resources in compliance with all applicable licences, terms and conditions. If you need further advice on compliance please consult the ICT Service Desk in the first instance.

3) Authority

The regulations are issued under the authority of the Executive. The Director of ICT is responsible for their interpretation and enforcement, and may also delegate such authority to other people.

Authority to use the University's ICT facilities is granted by a variety of means:

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

If you have any doubt whether or not you have the authority to use an ICT facility you should seek further advice from the ICT Service Desk.

Attempting to use or access ICT facilities which the University has not authorised you to use or access may be an offence under the Computer Misuse Act.

4) Intended use

4.1 Use for purposes in furtherance of University's mission

The ICT facilities are provided for use in furtherance of the University's mission. Such use might be for learning, teaching, research, knowledge transfer, public outreach, the commercial activities of the University, or the administration necessary to support all of the above.

4.2 Personal use

You may currently use the ICT facilities for personal use provided that it does not breach the regulations, and that it does not prevent or interfere with other people using the facilities for valid purposes (for example, using a PC to update your Facebook page when others are waiting to complete their assignments is a breach of the regulations).

Personal use of ICT facilities is a concession and can be withdrawn at any time.

Employees using the ICT facilities for non-work purposes during working hours are subject to the same management policies as for any other type of non-work activity.

Use of your University email account for personal use is discouraged, including 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. Additionally, as the University may need to authorise access to your email by other colleagues to ensure business continuity, using a non-University email account for personal correspondence and activities will minimise any privacy risks.

4.3 Commercial use and personal gain

Use of ICT facilities 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 the ICT Service Desk 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.

5) Identity

Many of the ICT services provided or arranged by the University require you to identify yourself so that the service knows that you are entitled to use it.

This is most commonly done by providing you with a user ID and password, but other forms of ICT credentials may be used, such as an email address, a smart card or some other form of security device.

5.1 Protect identity

You must take all reasonable precautions to safeguard any ICT credentials issued to you.

You must change passwords when first issued and at regular intervals as instructed. Do not use obvious passwords, and do not record them 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 ICT staff, no matter how convenient and harmless it may seem.

If you think someone else has found out what your password is, change it immediately and report the matter to the ICT Service Desk.

Do not use your user ID and password to log in to websites or services you do not recognise, and do not log in to websites that are not showing the padlock symbol.

Do not leave logged in computers unattended, and log out properly when you are finished.

Don't 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 the ICT Service Desk immediately.

5.2 Impersonation

Never use someone else's ICT credentials, or attempt to disguise or hide your real identity when using the University's ICT facilities.

However, it is acceptable not to reveal your identity if the system or service clearly allows anonymous use (such as a public facing website).

5.3 Attempt to compromise others' identities

You must not attempt to usurp, borrow, corrupt or destroy someone else's ICT credentials.

6) Infrastructure

The ICT infrastructure is all the underlying hardware and software that makes ICT function. It includes servers, the network, PCs, printers, operating systems, databases and a whole host of other hardware and software that has to be set up correctly to ensure the reliable, efficient and secure delivery of ICT services.

You must not do anything to jeopardise the infrastructure. This includes attempting to impair the operation of any ICT facility, whether at the University or belonging to another organisation.

6.1 Physical damage or risk of damage

Do not damage, or do anything to risk physically damaging the infrastructure, such as being careless with food or drink at a PC. Use of University ICT equipment off campus, including limited personal use, must be approved by your department,

faculty or service area and comply with Insurance Office guidance (see www.hull.ac.uk/insurance for details).

6.2 Reconfiguration

Do not attempt to change the setup of the 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 wi-fi or ethernet networks specifically provided for this purpose) or altering the configuration of University devices. Unless you have been authorised, you must not add software to or remove software from University devices.

Do not move equipment without authority.

6.3 Network extension

You must not extend the wired or wireless network, or disrupt the configuration without authorization. Such activities, which may involve the use of routers, repeaters, hubs or wireless access points, can disrupt the network and are likely to be in breach of the Janet Security Policy.

6.4 Setting up servers

You must not set up any hardware or software that would provide a service to others over the network without permission. Examples would include games servers, file sharing services, IRC servers or websites.

6.5 Introducing malware

You must take all reasonable steps to avoid introducing malware to the infrastructure.

The term malware covers many things such as viruses, worms and Trojans, but is basically 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 have been created on compromised computers.

If you avoid these types of behaviour, keep your antivirus software up to date and switched on, and run scans of your computer on a regular basis, you should not fall foul of this problem.

6.6 Subverting security measures

The University of Hull has taken measures to safeguard the security of its ICT infrastructure, including things such as antivirus software, firewalls, spam filters and so on.

You must not attempt to subvert or circumvent these measures in any way.

7) Information

7.1 Personal, sensitive and confidential information

During the course of their work or studies, staff and students (particularly research students) may handle information that comes under the Data Protection Act 1998, or is sensitive or confidential in some other way. For the rest of this section, these will be grouped together as protected information.

Safeguarding the security of protected information is a highly complex issue, with organisational, technical and human aspects. The University of Hull has policies and guidelines on Data Protection and Information Assurance 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.

7.1.1 Transmission of protected information

When sending protected information electronically, you must use a method with appropriate security. Email is not inherently secure. Advice about how to send protected information electronically is available from the ICT Service Desk.

7.1.2 Removable media and mobile devices

Protected information must not be stored on removable media (such as USB storage devices, removable hard drives, CDs, DVDs) or mobile devices (laptops, tablet or smart phones) unless it is encrypted, and the key kept securely.

If protected information is sent using removable media, you must use a secure, tracked service so that you know it has arrived safely. Advice on the use of removable media and mobile devices for protected information is available from the ICT Service Desk and on the ICT website at www.hull.ac.uk/ict.

7.1.3 Remote working

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.

Use of University equipment off campus, including limited personal use, must be approved by your department, faculty or service area. It must also comply with Insurance Office guidance (see www.hull.ac.uk/insurance for details) and

must not significantly increase the risk to any information held on the equipment. For example, allowing family members to use a University-owned laptop would be a breach of this latter requirement.

Advice on working remotely with protected information is available from the ICT Service Desk and on the ICT website at www.hull.ac.uk/ict.

7.1.4 Personal or public devices and cloud services

Even if you are using approved connection methods, devices that are not fully managed by the University of Hull 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 services that are not provided or sanctioned by the University unless securely encrypted first. You should also consider how access to any information could be granted in your absence, if required for business continuity.

7.2 Copyright information

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 http://libguides.hull.ac.uk/copyright. The key point to remember is that the fact that you can see something on the web, download it or otherwise access it does not mean that you can do what you want with it.

7.3 Others' information

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.

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 private information in the account, nor to compromise the security of the account concerned. Contact the ICT Service Desk for details on the authorisation process.

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

7.4 Inappropriate material

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.

The University of Hull 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 the Deputy Secretary via your Faculty ethics officer. Universities UK has also produced guidance on handling sensitive research materials. The University of Hull also has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "Prevent". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

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

7.5 Publishing information

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

7.5.1 Representing the University

You must not make statements that purport to represent the University of Hull without the approval of the University. If in any doubt, you must consult the Registrar's office for advice.

7.5.2 Publishing for others

You must not publish information on behalf of third parties using the University's ICT facilities without the approval of the University.

7.5.3 Bringing the University into disrepute

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. Please contact the Marketing and Communication Directorate for further advice on publishing information.

8) Behaviour

The way you behave when using ICT should be no different to how you would behave under other circumstances. Abusive, inconsiderate or discriminatory behaviour is unacceptable.

8.1 Conduct online and on social media

The University of Hull's policies concerning staff and student behaviour also apply to the use of social media. These include human resource policies, codes of conduct, the ICT regulations and disciplinary procedures. Specific examples include policies on bullying and harassment, and the Anti-Fraud and Bribery Policy.

8.2 Spam

You must not send unsolicited bulk emails or chain emails other than in specific circumstances. Advice on this is available from the ICT Service Desk.

8.3 Denying others access

If you are using shared ICT facilities for personal or social purposes, you should vacate them if they are needed by others with work to do. Similarly, do not occupy specialist facilities unnecessarily if someone else needs them.

8.4 Disturbing others

When using shared spaces, remember that others have a right 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.

8.5 Excessive consumption of bandwidth/resources

Use resources wisely. Don't consume excessive bandwidth by uploading or downloading more material (particularly video) than is necessary. Don't waste paper by printing more than is needed, or by printing single sided if double sided would do. Don't waste electricity by leaving equipment needlessly switched on.

9) Monitoring

9.1 University Monitoring

The University of Hull monitors and logs the use of its ICT facilities for the purposes of:

- Detecting, investigating or preventing misuse of the facilities or breaches of the University's regulations;
- Monitoring the effective function of the facilities and the University;
- Investigation of alleged misconduct;

The University of Hull 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.

9.2 Unauthorised monitoring

You must not attempt to monitor the use of ICT facilities without explicit approval from the University.

This would include:

- Monitoring of network traffic;
- Network and/or device discovery;
- Wi-fi traffic capture;
- Installation of key logging or screen grabbing software that may affect users other than yourself;
- Attempting to access system logs or servers or network equipment.

Where ICT is itself the subject of study or research, special arrangements will have been made. Contact your course leader/research supervisor for more information.

10) Infringement

10.1 Disciplinary process and sanctions

Breaches of these regulations will be handled by the University of Hull's disciplinary processes, described 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 regulations, for example, imposition of restrictions on your use of ICT facilities; removal of services; withdrawal of offending material; fines and recovery of any costs incurred by the University as a result of the breach.

10.2 Reporting to other authorities

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

10.3 Reporting to other organisations

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

10.4 Report infringements

If you become aware of an infringement of these regulations, you must report the matter to the Director of ICT, either directly or via the ICT Service Desk.