IT Code of Practice 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 IT facilities to the dos and don'ts in the IT Code of Practice.

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.

1 Scope

1.1 Users

These regulations apply to **anyone** using University of Sheffield IT facilities. This means more than students and staff. It could include, for example:

- Visitors to the University website, and people accessing the University's online services from off campus;
- External partners, contractor and agents based on site and using University network, or off-site and accessing the University's systems;
- Tenants of the University using the University's computers, servers or network;
- Visitors using the University's guest services;
- Students and staff from other institutions logging on using eduroam.

1.2 IT Facilities

The term IT Facilities include:

- IT Hardware that the University provides, such as PCs, laptops, tablets, smartphones and printers;
- Software that the University provides, such as operating systems, office application software, web browsers etc. It also includes software that the University has arranged for you to have access to, for example, special deals for students on commercial application packages;
- Data that the University 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, network connections in halls of residence, on-campus WiFi, connectivity to the internet from University PCs;
- Online services arranged by the University such as Google Apps, Turnitin;
- IT credentials, such as the use of your University login, or any other token (email address, smartcard, dongle) issued by the University to identify yourself when using IT facilities. For example, you may be able to use drop-in facilities or WiFi connectivity at other institutions using your usual username and password through the eduroam system. While doing so, you are subject to these regulations, as well as the regulations at the institution you are visiting.

2 Governance

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

Your use of IT is governed by IT-specific laws and regulations (such as these), but it is also subject to general laws and regulations such as the University's general policies.

2.1 Domestic Law

Your behaviour is subject to the laws of the land, even those that are not apparently 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
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- General Data Protection Regulation (GDPR)
- Regulation of Investigatory Powers Act 2000
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Counter Terrorism and Security Act 2015
- 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

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 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's general regulations and policies.
These are available at www.sheffield.ac.uk/calendar

2.4 Third Party Regulations

If you use University IT facilities to access third party services 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 username 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 IT network that connects all UK higher education and research institutions together and to the Internet

When connecting to any site outside the University 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. [If you modify this template, you must check that it still incorporates the Janet requirements]

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 https://www.chest.ac.uk/user-obligations/

There will be other instances where the University has provided you with a piece of software or a resource. Users shall only use software and other resources in compliance with all applicable licences, terms and conditions.

3 Authority

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

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

- The issue of a username 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 obviously open access setting, such as a University website; a self-service kiosk in a public area; or an open WiFi network on the campus.

If you have any doubt whether or not you have the authority to use an IT facility you should seek further advice from the CiCS Helpdesk.

Attempting to use the IT facilities without the permission of the relevant authority is an offence under the Computer Misuse Act.

4 Intended Use

University IT facilities, and the Janet network that connects institutions together and to the Internet, are funded by the tax-paying public. They have a right to know that the facilities are being used for the purposes for which they are intended.

4.1 Use for Purposes in Furtherance of the University's Mission

The IT 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 IT 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).

However, this is a concession and can be withdrawn at any time.

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

4.3 Commercial Use and Personal Gain

Use of IT facilities for non-University commercial purposes or for personal gains, such as running a club or society, requires the explicit approval of the Director of CiCS. The provider of the service may require a fee or a share of the income for this type of use. For more information, contact the CiCS Helpdesk.

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 IT 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 username and password, but other forms of *IT 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 *IT 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 IT 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 CiCS Helpdesk.

Do not use your username and password to login 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 smart card or other security hardware. Take care not to lose them, and if you do, report the matter to IT immediately.

5.2 Impersonation

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

6 Infrastructure

The IT infrastructure is all the underlying technology and processes that make IT 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 IT services.

You must not do anything to jeopardise the infrastructure.

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.

6.2 Reconfiguration

Do not attempt to change the setup of the infrastructure without authorisation, such as changing the network point that a PC is plugged in to, connecting devices to the network (except of course for WiFi or Ethernet networks specifically provided for this purpose) or altering the configuration of the University's PCs. Unless you have been authorised, you must not add software to or remove software from PCs.

Do not move equipment without authority.

6.3 Network Extension

You must not extend the wired or WiFi network without authorization. Such activities, which may involve the use of routers, repeaters, hubs or WiFi 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 abide by the University's Code of Connection when connecting devices to the University network.

You must not set up any hardware or software that would provide a service to others over the network without following the appropriate processes. 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 anti-virus 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 has taken measures to safeguard the security of its IT infrastructure, including things such as anti-virus 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 General Data Protection Regulation (GDPR), 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 has policies on Data Protection and Information Security www.sheffield.ac.uk/cics/information-security, and if your role is likely to involve handling protected information, you must make yourself familiar with and abide by these policies.

Additional guidance on the provisions of the General Data Protection Regulation (GDPR) and how the University ensures compliance with it is available at www.sheffield.ac.uk/govern/data-protection.

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 at www.sheffield.ac.uk/cics/information-security

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 smartphones) 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 at www.sheffield.ac.uk/cics/remote/information.

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.

Advice on working remotely with protected information is available at www.sheffield.ac.uk/cics/remote

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 University cannot be guaranteed to be free of malicious software that could, for example, gather keyboard input and screen displays.

Do not store or process protected information on personal or public devices without careful assessment of the risks. The same level of security must be applied as would be used on University devices; www.sheffield.ac.uk/cics/security

Do not store or process protected information in personal cloud services such as Office 365, iCloud, Google Apps (with a non-University account) or Dropbox unless securely encrypted first.

Note: University provided Google Apps services are covered by a contractual agreement and can be used to process some types of protected information, for further information see www.sheffield.ac.uk/cics/google/security

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 training and guidance are available at www.sheffield.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 have approval from the Director of CiCS and relevant Director/Head of Department.

Where information has been produced in the course of employment by the University, and the person who created or manages it is unavailable, the responsible Head of Department may give permission for it to be retrieved for work purposes. In doing so, care must be taken not to retrieve any private information in the account, nor to compromise the security of the account concerned.

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 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 from being drawn into terrorism. The University reserves the right to block or monitor access to such material.

The University has procedures to approve and manage valid activities involving *such* material for valid research purposes where legal with the appropriate ethical approval. For more information, please refer to www.sheffield.ac.uk/rs/ethicsandintegrity/ethicspolicy/policy-notes.

There is also an exemption covering authorised IT staff involved in the preservation of evidence for the purposes of investigating breaches of the 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 generally encourages publication you should be mindful of University policy and procedure. www.sheffield.ac.uk/corporate-communications

7.5.1 Representing the University

You must not make statements that purport to represent University without the approval of the relevant authority. www.sheffield.ac.uk/corporate-communications

7.5.2 Publishing for Others

You must not publish information on behalf of third parties using the University's IT facilities without the approval of the relevant authority. www.sheffield.ac.uk/corporate-communications

8 Behaviour

The way you behave when using IT 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

University policies concerning staff and students also apply to the use of social media. These include human resource policies, codes of conduct, acceptable use of IT and disciplinary procedures.

8.2 Spam

You must not send unsolicited bulk emails or chain emails other than in specific circumstances. Advice on this is available from www.sheffield.ac.uk/cics/email.

8.3 Denying Others Access

If you are using shared IT 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 to work without undue disturbance. Keep noise down (turn mobile devices 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. Do not waste paper by printing more than is needed, or by printing single sided when double-sided would do. Don't waste electricity by leaving equipment needlessly switched on.

9 Monitoring

9.1 University Monitoring

The University monitors and logs the use of its IT 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.
- 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.

For more information, please refer to www.sheffield.ac.uk/cics/information-security

9.2 Unauthorised Monitoring

You must not attempt to monitor the use of the IT without the explicit permission of the Director of CiCS

This would include:

- Monitoring of network traffic;
- Network and/or device discovery;
- WiFi 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 IT is itself the subject of study or research, special arrangements will have been made, and you should 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's disciplinary processes, the principles of which are set out at www.sheffield.ac.uk/calendar

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 IT 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 may 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 relevant authorities. www.sheffield.ac.uk/cics/policies/securityincident