

Regulations for the use of IT Facilities and Learning Resources

Issuing Authority: Howard Whiteley,
Chief Information Officer,
Information Systems and Technology

Signed: on master copy May 2015

Date Effective: May 2015

Review date: May 2017

Objective

To identify and promote the **Regulations for the use of the IT facilities and learning resources** to all staff, students and visitors.

Scope

The following regulations apply to all users of IT facilities and learning resources owned, leased or hired by Sheffield Hallam University (the University), all users of such facilities and resources on the University's premises and all such facilities and resources connected to the University's networks.

Staff and students should note the consequences of failing to comply with these regulations as set out in the Infringement section. In particular, disciplinary action against a user may be taken by the University for failure to comply with the Regulations and they may be charged for any costs arising out of such failure.

Definitions

Users - All staff and students of the University and others outside the Institution who have been given permission to use the University's IT facilities and learning resources.

Facilities - IT facilities located in the University, including networks, servers and personal computers, together with the software and data stored on them. Any IT use carried out on equipment connected to the institution network, whether or not this involves the use of a University based or University owned computer.

Learning Resources - All learning resources including (but not exclusively) text, video and audio which may be made available in hard copy or via the University IT facilities.

Designated Authority - The designated authority is the Sheffield Hallam University Director of IS&T. The Director of IS&T may delegate responsibility for particular areas to appropriate University staff.

Relevant Legislation

Users must comply with all UK legislation relating to the use of information, computers and networks. Applicable laws include:

- [Data Protection Act 1998](#) This act makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. More University information is available from: staff [policy](#) and [guidelines](#) and [guidance](#) for students.
- [Copyright, Designs & Patents Act 1988](#) Copyright material includes literary works (including computer software), artistic works (including photographs), sound recordings (including music), films (including video) and databases. More University help and advice on copyright is available for [Staff](#) and [Students](#)
- [Computer Misuse Act 1990](#) The Act provides safeguards for computer material against unauthorised access or modification. More University information on the Act can be found for staff [here](#) and for students [here](#).

- [Privacy and Electronic Communications \(EC Directive\) Regulations 2003](#). These regulations prohibit the sending of unsolicited marketing emails (or SMS/text messages) to individuals. In addition, the regulations control the use of 'cookies'. Further University provided guidance is available [here](#).
- [Fraud Act 2006](#). The Act prohibits 'phishing' whereby official-looking emails guide unsuspecting users to fake websites (e.g. fake bank websites) in order to steal their login details. Creating or possessing software to enable this activity is also an offence.

Registration

Authorisation - Use of IT facilities require prior registration and the granting of a user code and/or an individual password. The allocation of a user code and password will constitute authorisation for use of relevant facilities. Registration to use IT facilities constitutes acceptance of these regulations.

Identification - Users must not utilise another user's code, nor permit any password issued to them to become known to any other person. If having logged in, users must not leave IT facilities unattended and potentially exploitable by other persons. Users may not impersonate another person when sending electronic mail or making information available on-line in any other way. This includes attempts to obtain or change another user's password. System administrators of IT facilities should not give access to another user's code or password and should report any requests to do so to the designated authority.

Library resources - Users must not use another person's borrower number nor permit anyone else to borrow items using their number.

External Users - Use of IT facilities by persons other than staff or students must have the explicit prior permission of the designated authority and may be subject to charge.

Use of Facilities and Learning Resources

Personal Use - The University's IT facilities are provided for educational, administrative, research and personal development use by staff in the course of their employment and by students in the course of their education. Any other use of the University's resources puts an additional demand on those resources, which affects performance.

Limited personal use of certain facilities is permitted, during personal time. Any such use must neither interfere with the employee's own work or the student's study, nor prevent others from pursuing their legitimate work and use of the University's IT facilities. The University reserves the right to withdraw this benefit either individually or collectively at any time. In such circumstance the University will endeavour to give reasonable notice of its intention to withdraw such benefit.

Where the University becomes aware of a specific type of personal use which affects the efficient operation of its IT facilities, the University will take appropriate steps to withdraw, without notice, access to the relevant facility or resource. Non-exhaustive examples of this include barring access to certain technology or Internet resources such as web sites, news groups or other Internet resources. Users who have a legitimate requirement to access such withdrawn resources should discuss the matter with the designated authority or appointed representative.

If a user is able to access a particular technology, website or resource it does not necessarily imply that these may be accessed in accordance with the IT Regulations.

Commercial Use - Use of any of the University's IT facilities for commercial gain (including advertising) or for work on behalf of others (unconnected with a student's course of study at the University or a member of staff's legitimate activities) is prohibited, unless the user has explicit prior written permission of the designated authority and an appropriate charge (if applicable) for such use has been contractually agreed between the other party and the University.

Movement - University IT facilities should not be moved or disconnected without the prior agreement of the designated authority.

Connection (network access and power supply) - Users must not physically connect any device into the University's network or other IT facility without prior agreement from the designated authority.

Users may plug their laptop into a University mains socket whilst they are using it, but users should observe these [guidelines](#).

Compliance with external regulations - Users must not make use of University IT facilities to connect to any external IT facilities or commercial services without proper authority from the provider of those facilities. If the IT facilities of a third party are employed, users must comply with the regulations and codes governing that organisation.

Damage - Users must not cause any form of damage to the University's IT facilities, software, or to any of the rooms and their facilities and services which contain that equipment or software. The term 'damage' includes any unauthorised installation of hardware or software, which incurs time and/or cost in restoring the facilities to their original state.

IT Security - Users should conform to all relevant University IT policies issued by the designated authority, as contained within the [Electronic Information Security Framework \(EISF\)](#). In particular, users must not deliberately introduce any virus, worm, Trojan horse or other harmful or nuisance program or file into any IT facility, nor take deliberate action to circumvent any precautions taken or prescribed by the University to prevent this. Users must not attempt to penetrate the security and/or privacy of other users' files.

Spam and Mass-circulation - Spam is usually defined as unsolicited electronic messages (using email, SMS, Instant Messaging or other means) sent in bulk. Users may not use University IT facilities to send spam.

Sending unsolicited electronic messages for the purposes of marketing is prohibited under the [Privacy and Electronic Communications \(EC Directive\) Regulations 2003](#)

Illegal and/or Offensive Material - Users must not use the University IT facilities to access, produce, obtain, download, store, view, share, or distribute material (including images, video, text or sound files) which are either illegal under UK law (e.g. in breach of copyright law) and/ or can reasonably be judged to be offensive, obscene, indecent, abusive or likely to incite racial hatred.

The only exceptions would be where such material is essential for research or teaching purposes and is permitted by law, and prior written permission has been granted by the designated authority or permission has been granted by the copyright holder.

Discrimination - Users must not use the University's IT facilities to place, disseminate or receive material which discriminates or encourages discrimination on, for example, the grounds of gender, sexual orientation, disability, age, religious belief, race or ethnic origin. The University has harassment policies and procedures for [students](#) and [staff](#).

Defamation - Users must not use the University's IT facilities to publish any information which

- they know or believe to be untrue
- is defamatory and could not be defended on the grounds that it is true/factual or that it is fair comment on a matter of public interest (e.g. works of literature, art, music, television and radio or the activities of public figures)

A defamatory statement is one that would "tend to lower the [person] in the estimation of right-thinking members of society generally". (Lord Atkin, *Sim-v-Stretch*, 1936)

Behaviour

Users must respect the rights of others and should conduct themselves accordingly when using IT facilities and learning centres to create a conducive environment for all. Staff should have regard

for the University's [Code of Behaviour](#). Students should have regard for the University [Behaviour Policy and Disciplinary Procedures](#).

- Users must not interfere with or disrupt the availability and use of the IT facilities by others.
- Users must take every precaution to avoid damage to equipment and learning resources caused by the presence of food and drink in its vicinity.
- Users must also comply with any further specific instructions or regulations displayed alongside IT facilities or on computer screens.

A guide to good practice can be found here for [staff](#) and [students](#).

Borrowing Library Resources

Users have a responsibility for items on loan to them and may incur fines for late return, or charges for non-return, of learning resources borrowed on their library card.

Copyright and Licence Agreements

Users must adhere to the terms and conditions of all licence agreements relating to IT facilities and learning resources which they use including software, services documentation and other goods.

Users must not copy or modify any copyright material (third party material) nor incorporate any part of the third party material into their own work unless such acts are either permitted under the [Copyright Designs & Patents Act 1988](#), by a licence agreement, or with the permission of the copyright holder.

Users must not install, make, store, or transfer unlicensed copies of any copyright or trademark work including, but not limited to software, videos or music, unless permitted under legislation or with the permission of the copyright holder.

Infringement

Withdrawal of facilities - If a user is in breach of any of these regulations, the designated authority may withdraw or restrict the user's access to IT facilities and learning resources, following consultation with the user's Head of Directorate or PVC/Executive Dean of Faculty.

Removal of Material - The University reserves the right to remove material from its IT facilities without notice where such material is in breach of these regulations.

Disciplinary action - Any breach of the regulations may be dealt with under the University's formal disciplinary procedure for [students](#) and the Problem Resolution Framework for [staff](#) and in certain circumstances may result in expulsion or dismissal. The user may be charged for any costs that have arisen as the result of misuse or abuse of facilities and/or resources.

Breaches of the law - Where appropriate, suspected breaches of the law may be reported to the police. Where the breach has occurred in a jurisdiction outside of the UK, the breach may be reported to the relevant authorities within that jurisdiction.

Monitoring of IT Facilities

In order to protect the security and working of the University's IT facilities, it may be necessary to monitor collective or individual use of the IT facilities and systems. This may occur where there are indications of abuse of systems, or that individuals may be using systems in excess of their authority. Information including, but not limited to, files, messages and user account information may be intercepted, monitored, recorded, copied, audited, and inspected. This information may also be disclosed to authorised University staff and to the police where deemed necessary.

Such investigations will only be carried out with the agreement of the designated authority and in accordance with the [University Monitoring Policy](#). This policy sets out the principles and good practice guidelines to which the University adheres. Further good practice recommendations are contained in the [Employment Practices Code, Part 3](#).

Any intentional unauthorised monitoring will be regarded as an invasion of privacy and may result in disciplinary action.

Investigation of Misuse of Copyright third-party materials

Investigations will be undertaken where there is reasonable belief of misuse. Should this relate to items made available via the University IT facilities they will be immediately removed pending an investigation.

Disclaimer

Subject to the [Terms and Conditions for Students](#), Clause 11 (Liability), where applicable, the University accepts no responsibility and expressly excludes liability to the fullest extent permissible by law, for:

- the malfunctioning of any IT facility or part thereof, whether hardware, software or other.
- the loss of any data or software or the failure of any security or privacy mechanism.

Enquiries

All enquiries relating to this Regulation should be addressed to:

- [ITHelp](#), extension 3333
- Director IS&T, extension 4079