Regulations for the Use of the University of Reading's IT Facilities and Systems

The aim of these regulations is to help ensure that the University's IT facilities are used safely, securely, lawfully and equitably. They are derived largely from the Universities and Colleges Information Systems Association (UCISA) "Model IT Regulations for the use of IT facilities and systems". These regulations replace the earlier "Rules for the use of University Computers and Data Networks".

1 Scope

Users

These regulations apply to **anyone** using the University's IT Facilities and Systems. In addition to staff and students this may include, for example:

- Visitors to the University's website, and people accessing the University's online services from off campus;
- External partners, collaborators, contractor and agents based onsite and using the University's network, or offsite and accessing the University's systems;
- Tenants of the institution using the University's computers, servers or network;
- Visitors using the University's WiFi;
- Students undertaking placements or work experience;
- Students and staff from other institutions logging on using Eduroam.

IT Facilities and Systems

The term IT Facilities and Systems includes:

- IT hardware that the University provides, such as PCs, laptops, tablets, smart phones 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 covers, 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 Office 365, email, or any of the Jisc online resources;

- *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.

  These regulations do not form part of any employee's contract of employment and the University may amend them at any time.

2 Governance

When using the IT Facilities and Systems it is expected that your conduct will be lawful.

When accessing IT Facilities and Systems from another jurisdiction outside England, you must abide by all relevant local laws, as well as with English law .

You are bound by the University's general policies and regulations when using the IT Facilities and Systems.

You must abide by the regulations applicable to any other organisation whose services you access such as Janet, Eduserv and Jisc Collections.

When using services via Eduroam, you are subject to both the regulations and relevant policies of the University and the institution where you are accessing services.

See below for links to relevant policies.

Some software licences procured by the University will set out obligations for the user – these must be adhered to. If you use any software or resources covered by a Chest agreement, you are deemed to have accepted the Eduserv User Acknowledgement of Third Party Rights. (See below for more detail.)

Breach of any applicable law or third party regulation will be regarded as a breach of these IT regulations.

Your use of IT is governed by IT specific laws and regulations such as those listed below.

Domestic law

Your use of the University's IT Facilities will be subject to the laws of England and Wales, 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 Obscene Publications Act 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
- Protection from Harassment Act 1997
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Defamation Act 1996 and Defamation Act 2013
- Counter Terrorism and Security Act 2015

So, for example, unless otherwise permitted by the University in the course of your academic activities, you may not:

- Create or transmit, or cause the transmission, of any pornographic, 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 which is discriminatory, offensive, derogatory or with the intent to cause fear, alarm, annoyance, inconvenience or anxiety;
- Create or transmit material which encourages terrorism or extremism
- Create or transmit material with the intent to defraud;
- Create or transmit false or defamatory material;
- Create or transmit material such that this infringes the copyright of another person or organisation;
- Create or transmit material containing confidential information about the University, its employees or students unless in the proper course of the duties or studies;
- 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.

This list is illustrative and is not intended to be exhaustive.

There is an excellent set of overviews of law relating to IT use available at www.jisclegal.ac.uk/LegalAreas.

Foreign law

If you are using IT Facilities and Systems 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.

You should apply common sense, obey domestic laws and the regulations of the service you are using (which in most cases will refer to legal requirements for the host country).

Third party regulations

If you use the University's IT 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 institutional 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 of Reading 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, but you required to familiarise yourself with 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, with which you must comply and 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 has provided you with a piece of software or a resource and where you must comply with the terms relating to use.

- **Licence agreements**
  Users shall only use software and other resources in compliance with all applicable licences, terms and conditions. If in doubt about these please

consult the IT Department for clarification.

3 Personnel Responsible for the Regulations

3.1 University Executive Board (UEB) has overall responsibility for setting and approving these regulations.

3.2 The Director of IT has day-to-day operational responsibility for the Regulations. He or she will review these regulations from a legal and operational perspective once a year.

3.3 Managers have a specific responsibility to ensure the application of these regulations and all members of staff are responsible for supporting colleagues and students and ensuring its success.

You must not use the IT facilities without the permission of the Director of IT.

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 an Institutional website; a self-service kiosk in a public area; or an open WiFi network on a campus.

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

You must comply with any reasonable written or verbal instructions issued by the IT Department in support of these regulations.

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

4 Intended use

The IT facilities are provided for use in furtherance of the objects of the University of Reading, for example to support a course of study, research or in connection with your employment by the University.

Use of these facilities for personal activities, provided that such use does not infringe any of the regulations, does not interfere with others' valid use and is reasonable, is permitted, but this is a privilege that may be withdrawn by the University at any point. 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.

Use of IT facilities for non-institutional commercial purposes, or for personal gain, such as running a club or society, requires the explicit approval of the Chief Operating Officer.

Even with such approval, the use of certain licences is only permitted for academic use and where applicable to the code of conduct published by the Combined Higher Education Software Team (CHEST). http://www.eduserv.ac.uk/services/Chest-Agreements.

4 Identity

You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone other than in accordance with these regulations.

You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended and ensure it is switched off on leaving the office, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access the University network should only be allowed to use terminals under supervision.

You must take all reasonable precautions to safeguard any *IT credentials* (for example, a username and password, email address, smart card or other identity hardware) issued to you.

You must not allow anyone else to use your IT credentials. Nobody has the authority to ask you for your password and you must not disclose it to anyone. Do not share passwords with anyone else, even IT staff, no matter how convenient and harmless it may seem.

You must not use your University email account or *IT credentials* to demonstrate or infer that you are acting on University approved business when you are acting in a personal capacity.

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

If you have been issued with a laptop, or mobile phone, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, electronic documents may be read by third parties, for example, passengers on public transport.

You must not attempt to obtain or use anyone else's credentials.

You must not impersonate someone else or otherwise disguise your identity when using the 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).

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

6 Infrastructure

The IT infrastructure includes servers, the network, PCs, printers, operating systems, databases and a 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, including the following:

Physical damage or risk of damage

> Do not damage, or do anything to risk physically damaging the infrastructure, such as attempting to change or move network access points.

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 for Wifi or ethernet networks specifically provided for this purpose)

or altering the configuration of the University's PCs and other provided equipment. Unless you have been authorised, you must not add software to or remove software from PCs and laptops.

Do not move equipment without authority, including desktop equipment.

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.

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.

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 includes 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/links in emails from people you do not know, or inserting media that have been created on compromised computers.

Subverting security measures

The University has taken measures to safeguard the security of its IT 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.

You should exercise particular caution when opening unsolicited e-mails from unknown sources or an e-mail which appears suspicious (for example, if it contains a link to a web address, or contains an attachment). Inform the IT Service Desk immediately if you suspect your computer may have a virus. The University reserves the right to delete or block access to e-mails or attachments in the interests of security. It also reserves the right not to transmit any e-mail message.

7 Information

If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it and must observe the University's Information Security policies and guidance, available at:

http://www.reading.ac.uk/internal/imps/policiesdocs/imps-policies.aspx

You must not infringe copyright, trade marks, or any other third party-owned intellectual property rights, or break the terms of licences for software or other material.

You must not publish defamatory material.

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

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 being drawn into terrorism.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening, discriminatory or extremist or which may cause others to be 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; these are available at:

http://www.reading.ac.uk/internal/res/ResearchEthics/reas-REethicshomepage.aspx

and must be observed.

You must abide by the University's Content Management guidelines when using the IT facilities to publish information.

Any emails sent by a member of staff or a student of the University may be disclosed under the Freedom of Information Act 2000 or in legal proceedings brought by or against the University. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

8 Behaviour

Real world standards of behaviour apply online and on social networking platforms, such as Facebook, Blogger and Twitter. In using the IT facilities you must act in accordance with the University's Values for Working Together and Professional Behaviours. Additionally:

You must not cause fear, alarm or distress to others.

You must not unlawfully discriminate against, harass, defame or bully others.

You must adhere to University guidelines on social media.

You must not send spam (unsolicited bulk email).

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

You must not use the IT facilities in a way that interferes with others' valid use of them.

9 Monitoring

The University monitors and records the use of its IT facilities, including any permitted personal use, for the purposes of:

- The effective and efficient planning and operation of the IT facilities;
- Detection and prevention of infringement of these regulations;
- Investigation of alleged misconduct, including ensuring compliance with University policies;
- To find lost data or to retrieve data lost due to computer failure;
- Detection of potential security threats; and
- Complying with any legal obligations.

Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for the purposes set out above.

The University will comply with lawful requests for information from government and law enforcement agencies.

You must not attempt to monitor the use of the IT facilities without the explicit authority of the Director of IT . 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

Breaches of these regulations by staff will be handled in accordance with the University's Disciplinary Policy and, in serious cases may be treated as gross misconduct leading to summary dismissal. Breaches by Students will be reviewed by the IT Department and following such review Students may have their access to the IT Facilities and Systems removed. Further, such breaches may be dealt with under the relevant Student Disciplinary processes.

This could have a bearing on your future studies or employment with University and beyond.

All other users may have their access to the IT Facilities and Systems revoked by the IT Department.

Sanctions may be imposed if the relevant process finds that you have breached the regulations. This could include but is not limited to the imposition of restrictions on your use of IT Facilities and Systems; removal of services; withdrawal of offending material; fines, and recovery of any costs incurred by the University as a result of the breach.

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.

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.

Report infringements

If you become aware of an infringement of these regulations, you must report the matter in the first instance to your line manager and thence to the Director of IT.