IT USER REGULATIONS

1. Purpose and Scope

This document sets out the responsibilities and required behaviours of all users of University of Reading provided IT facilities and systems.

1.1 This policy applies to all:
- University of Reading staff.
- University of Reading students.
- Third party users authorised by the University of Reading or any department thereof.

1.2 This policy applies to all IT facilities and systems owned, leased, hired or otherwise provided by the University of Reading, connected directly or remotely to University infrastructure or used on University premises, including (but not limited to):
- IT hardware such as PCs, laptops, tablets, mobile phones and printers.
- Software that the university provides, such as operating systems, office applications, 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, datasets or citation databases.
- Online services arranged by the University, such as Office 365, email etc.
- Access to the network provided or arranged by the University. This covers, for example, network connections in halls of residence, on-campus Wi-Fi and connectivity to the internet from University PCs.

2. Roles and Responsibility

2.1 It is the responsibility of all users of the University of Reading's IT facilities and systems to:
- Read, understand and comply with this and other related policies.
- Ensure that their behaviour and activities when using University of Reading IT facilities is in accordance with the requirements of this policy.

2.2 The Director of DTS has day-to-day operational responsibility for the regulations and will review these regulations from a legal and operational perspective on an annual basis.

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

3. Consequences of Non-Compliance

Failure to comply with this policy may result in:
- Revocation of access to University systems.
- The instigation of disciplinary procedures and, in certain circumstances, legal action may be taken.

- Action taken against members of staff (including third parties) up to and including dismissal/termination of the engagement.
- Where appropriate, breaches of the law may be reported to the authorities.

4. Policy

User Accounts/Identity

4.1 You must not use the IT facilities without the permission of the Director of DTS. 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 Wi-Fi network on a campus.

4.2 Those authorised to use University of Reading IT facilities are assigned an account for their individual use, under the following conditions:

- This account may not be used by anyone other than the individual to whom it has been issued.
- You must not attempt to usurp, borrow, corrupt or destroy someone else's IT credentials.
- The assigned account password must be changed immediately and not divulged to anyone, including DTS staff, for any reason.
- This password must not be used as the password for any other account.
- Will, if there is any indication that an account has been compromised, change their password immediately and report it as an incident to the IT Service Desk.
- Individual email addresses are for the sole use of the assignee, but remain University of Reading assets and their use is subject to University policy.
- You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.
- 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.

Equipment

The following statements define restrictions around the use of personal and University of Reading provided equipment when using University networks or information.

4.3 Equipment not provided and managed by the DTS department must not be connected to University of Reading internal networks (through network ports or staff only Wi-Fi) without the prior agreement of DTS.

4.4 Equipment on campus that is connected to the University of Reading network or otherwise managed by the DTS department may not be relocated without the prior agreement of the DTS department.

4.5 Staff and students are responsible for ensuring that all devices used in connection with university activity are password protected to safeguard any information held in the event of loss or theft.

4.6 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.

4.7 Staff must ensure that they have up-to-date Anti-Virus software installed plus a firewall running at all times on equipment connected to the University of Reading network, including equipment not owned by or supplied by the University.

4.8 Any device that is not compliant with the above criteria is liable to physical or logical disconnection from the network without notice.

4.9 Serious damage or the theft of electronic communications equipment should be reported to the relevant campus security office which will advise the University Insurance Officer and the DTS department.

4.10 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.

Information

4.11 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/.

4.12 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 DTS.

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:

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

4.14 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 Wi-Fi 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.

4.15 Do not move equipment without authority, including desktop equipment.

4.16 You must not extend the wired or Wi-Fi network without authorization. Such activities, which may involve the use of routers, repeaters, hubs or Wi-Fi access points, can disrupt the network.

4.17 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.

4.18 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.

4.19 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.

4.20 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.

Personal Use of University of Reading Facilities

4.21 The University of Reading provides IT facilities, including email addresses and computers, for academic and administrative purposes related to work or study. Reasonable personal use is however permitted under the following conditions:

- It is used in a manner which does not obstruct the work of other students or staff and which encourages a scholarly atmosphere to be maintained.
- It does not breach or undermine any University of Reading policies or codes of conduct.
- It is not excessive in its use of resources.

Use of Third Party IT Services

4.22 Wherever possible, users should always attempt to use only IT services provided or endorsed by the University of Reading for conducting University business. However, if a requirement arises that is not met by existing solutions, discuss this with the IT Service Desk in the first instance. An alternative solution may already be available or it may, subject to regulatory and procedural requirements, be possible to make use of services provided by third parties.

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

Unacceptable Use of University of Reading Facilities

4.24 Whilst not exhaustive, the following activities are considered to be unacceptable uses of University of Reading facilities:

- Any illegal activity or activity which knowingly breaches any University of Reading policy.
- Any attempt to knowingly gain unauthorised access to facilities or information.
- Any attempt to knowingly undermine the security or integrity of University of Reading facilities (including any unauthorised penetration testing or vulnerability scanning of any university systems).
- Providing access to facilities or information to those who are not entitled to access.
- Any irresponsible or reckless handling or unauthorised use or modification of University of Reading data.
- Any use of University of Reading facilities to bully, harass, intimidate or otherwise cause alarm or distress to others.
- Sending unsolicited and unauthorised bulk email (spam).
- Creating, storing, accessing or transmitting pornographic, offensive, defamatory, or obscene material.
- Create or transmit material:
    - Which encourages terrorism or extremism.
    - With the intent to defraud.

- Containing confidential information about the University, its employees or students unless in the proper course of your duties or studies.
- Which is discriminatory, offensive, derogatory, or with the intent to cause fear, alarm, annoyance, inconvenience or anxiety.

- Using University of Reading facilities for commercial gain without the explicit authorisation of the appropriate authority.
- Knowingly failing to report any breach or suspected breach of information security to the DTS department.
- Infringe copyright, trade marks, or any other third party-owned intellectual property rights, or break the terms of licences for software or other material.
- Deliberately or recklessly consume excessive IT resources such as processing power, bandwidth or consumables.

5. Compliance with Legislation

5.1 When using the IT facilities and systems it is expected that your conduct be lawful.

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

5.3 Your use of the University's IT facilities will be subject to the laws of England and Wales, including (but not limited to) the following legislation:

- Computer Misuse Act 1990
- EU General Data Protection Regulation (GDPR) 2018
- Copyright, Designs and Patents Act 1988
- Wireless Telegraphy Act 2006
- Protection from Harassment Act 1997
- Equality Act 2010

5.4 In addition to the above requirements, the University of Reading 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.

5.5 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.

6. Monitoring

Monitoring of individual usage of the electronic communications facilities will not be undertaken as a matter of course. However, this may be necessary when concerns arise about the level or nature of personal use of the systems. Disciplinary action may be considered appropriate in such circumstances.

7. Related Policies

This policy and other supporting policies can be found here:

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

8. Policies superseded by this policy

Regulations for the use of the University of Reading's IT facilities and systems v1.2

Document control

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
2.0	N/A	DTS	Biennially	University Policy Group	May 20	May 20	May 22