REGENT'S
UNIVERSITY LONDON

IT Acceptable Use Policy

Owner: *Asad Rehman, IT Director*

Review date: *July 2021*

Next review due date: *April 2024*

Version: *2.3*

If you require this document in an alternative format please contact the Disability Officer on 020 7487 7863 or email disability@regents.ac.uk

Contents

Core Regulations **3**

Scope **3**

Governance **3**

Intended use **4**

Identity **4**

Infrastructure **4**

Phishing **5**

Information **5**

Prevent **5**

Behaviour **6**

Monitoring **6**

Infringement **6**

Appendix A **7**

Core Regulations

The aim of these regulations is to help ensure that Regent's University London (the University) IT facilities can be used safely, lawfully and equitably.

There are a number of related policies that should be read in conjunction with this Policy. These include, but are not limited to:

- Data Protection Policy
- Social Media Policy
- Telephone and Portable Devices Policy
- Information Systems Security Policy
- Prevent Guidelines
- Electronic Communications and Monitoring Policy
- Disciplinary Policy

The issues covered by these regulations are complex and you are strongly urged to read the accompanying guidance document (Appendix A). This Policy is based on the UCISA Model Regulations for the use of institutional IT facilities and systems, originally created in April 2014, subsequently internally updated in 2015, 2016, and 2019. See www.ucisa.ac.uk for further details.

Scope

These regulations apply to anyone using the IT facilities (hardware, software, data, network, including wi-fi access, third party services, online services) provided or arranged by the University.

Governance

When using IT, you remain subject to the same laws and regulations as in the physical world.

It is expected that your conduct is lawful. Furthermore, ignorance of the law is not considered to be an adequate defence for unlawful conduct.

When accessing services from another jurisdiction, you must abide by all relevant local laws, as well as those applicable to the location of the service.

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

When using services via Eduroam, you are subject to both the regulations of the University and the institution where you are accessing services.
Some software licences procured by the University will set out obligations for the user – these should 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 the chest website for further details (www.chest.ac.uk).

Breach of any applicable law or third-party regulation will be regarded as a breach

of these IT regulations.

Intended use

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

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

Use of these IT facilities for non-institutional commercial purposes, or for personal gain is not permitted unless expressly given approval by the IT Director.

Identity

You must take all reasonable precautions to safeguard your identify (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. 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.

Infrastructure

You must not do anything to jeopardise the integrity of the IT infrastructure by, for example, doing any of the following without approval:

- Damaging, reconfiguring or moving equipment;
- Loading software on the University's equipment other than in approved circumstances;
- Reconfiguring or connecting equipment to the network other than by approved methods;
- Setting up servers or services on the network;
- Deliberately or recklessly introducing malware;
- Attempting to disrupt or circumvent IT security measures.

Phishing

Phishing is the practice of attempting, in an electronic communication, to acquire personal data from people such as usernames, passwords, and credit card details by disguising the request as originating from a trustworthy entity. The threat of phishing attempts is real. Individuals and organisations, including universities have suffered loss as a result of staff mistakenly divulging their login and password details, resulting in fraudsters gaining access to personal data, and in some cases using this information to fraudulently attempt to receive funds from students or staff.

All staff and students receive mandatory phishing training during their induction to the University. A range of training materials are available to all users on the intranet, which contains examples of real phishing emails, which, in some cases are difficult to distinguish from genuine emails.

If you believe that you have received a phishing email, do not click on any links. Contact the IT Service Desk for advice (itsservicedesk@regents.ac.uk).

Information

If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it and must observe the University's **Data Protection Policy** in relation to the **General Data Protection Regulations (2018**) and the **Data Protection Act (2018).**

You must not infringe copyright or break the terms of licences for software or other material.

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

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory. the University has procedures to approve and manage valid activities involving such material.

Prevent

The University has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "**Prevent**". According to the UK government's Prevent Strategy, radicalisation refers to "the process by which a person comes to support terrorism and forms for extremism leading to terrorism". The University subscribes to a filter service which categories websites that have been flagged by the Home Office as containing material which is linked to extremism and terrorism. Users will be presented with a warning message prior to the site loading and advised that, should they decide to access the site, their activity will be monitored and investigated by the University. The investigation may lead to disciplinary action and involvement with the authorities if the access is not in connection with legitimate

academic research.

Behaviour

Real world standards of behaviour apply online and on social networking platforms, such as Facebook, Twitter, Instagram, and other platforms.

You must not cause needless offence, concern or annoyance to others.

You should also adhere to the University's 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.

Monitoring

Under the Electronic Communications and Monitoring Policy**,** the University monitors and records the use of its IT facilities 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;
- Dealing with email in an employee's absence

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 explicit authority.

Infringement

Infringing these regulations may result in sanctions under the institution's **Disciplinary Policy**. Penalties may include withdrawal of services and/or fines. Offending material will be taken down.

Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.

The University reserves the right to recover from you any costs incurred as a result of your infringement.

You must inform the IT Service if you become aware of any infringement of these

regulations.

REGENT'S
UNIVERSITY LONDON

Appendix A

General Guidelines

1. ITS facilities available for use within the University may be used only for:

    2.1. Learning and Teaching.
    2.2. Research.
    2.3. Personal educational development.
    2.4. Administration and management of University business.
    2.5. Development work and communication associated with the above.
    2.6. Consultancy work contracted to the University.

2. The ITS systems are used on the understanding that the University will not accept any liability whatsoever for loss, damage, or expense which may result from the ITS facilities. The exception is to the extent that such loss, damage, injury or expense are attributed to negligence, fraudulent misrepresentations or breach of statutory duty on the part of the University or any of its servants or agents acting in their capacity as such.

3. The University reserves the right to monitor all communications and other use of ITS systems in order to ensure compliance with these rules. Monitoring will only be undertaken to such extent as is necessary in the circumstances.

4. Access gained through permitted use of the University's ITS to other computing centres and facilities linked to those at this University is governed by these rules, in addition to any rules in force from time to time for use of the ITS facilities at a remote site.

5. Usernames and other allocated resources shall be used only by the registered holder (user). Users shall maintain a secure password to control access to their usernames and accounts. Users shall ensure that passwords are not stored in locations that can easily be accessed by anyone other than the authorised password holder. Use shall not be made of computing resources allocated to another person unless such use has been specifically authorised by the ITS Department.

6. No person shall by any wilful or deliberate act or omission or by failure to act with due and reasonable care jeopardise the integrity of the ITS equipment, its operating systems, systems programs or other stored information, or the work of other users, whether within the University or in other computing locations to which the facilities at the University allow connection. Such acts include (but not limited to):

    7.1. The creation of network traffic high enough to degrade significantly network performance for other users.
    7.2. The use of tools to alter the behaviour of network devices.
    7.3. The scanning of ports on external computers.
    7.4. Circumvention of Network Access Control.

7.5. Monitoring or interception of network traffic.
7.6. Associating any device to network access points, including wireless, to which the user is not authorised.
7.7. The copying, downloading, distribution or storage of music, video, film or other material, for which you do not hold a valid license or other valid permission from the copyright holder.
7.8. The distribution, copying or storage by any means of pirated or unlicensed software or music.
7.9. The passing on of electronic chain mail.
7.10. The use of University mailing lists for non-academic purposes but including the Staff Social list.
7.11. The use of University mailing lists for non-academic purposes but including the Staff Social list.
7.12. The unauthorised use of programs on central servers, which consume such resources as to reduce significantly the server's performance for other users.

8. ITS shall not be used to access, store or create material of an offensive nature. This includes (but not limited to) material containing:

8.1. Racist or sexual terminology;
8.2. Offensive references to disability, religion or sexual orientation;
8.3. Pornographic images or other content.
8.4. Extremist content

9. ITS shall not be used for unauthorised access to computer material (i.e. a program or data) and unauthorised modification of computer material which are forbidden by law (Computer Misuse Act 1990) and by these rules, which endorse the Guidance on the Computer Misuse Act published by the Universities and Colleges Information Systems Association.

10. Reasonable use of ITS facilities for personal correspondence, where not connected with any commercial activity, is at present regarded as acceptable.

11. Prior permission from the IT Director or the 'Head of' administering the relevant computer facility, as appropriate, must be obtained in writing if use could possibly fall outside of the terms defined above.

12. No person shall use, copy or transmit any software from University ITS equipment unless a license from the copyright holder permitting such act is in force. Copies of the list of software licensed for use within the University are available from ITS.

13. Any restrictions placed from time to time on the use of ITS administered by the University or amendments to these rules from time to time must be observed.

14. No person or persons shall use the University's information systems to hold or process personal data except in accordance with the provisions of the Data Protection Act 2018, GDPR (2018), the University's Data Protection Policy and the University's HR Data Protection Policy. Any person wishing to use the facilities to hold or process personal data shall be required to:

14.1. Comply with any restrictions the University may impose concerning the

manner in which the data may be held or the processing carried out and inform the University's Data Protection Officer.

15. All use of the facilities shall be honest and decent and shall have regard to the rights and sensitivities of other people. All users are bound to adhere to English law in their use of computing facilities.

16. Breaches of this Policy are offences under the rules of the University and will be dealt with under the University's disciplinary codes for students and staff. If after investigation it appears that a member of the University, whether staff or student, may have acted in breach of these rules, he or she may be denied access to all ITS facilities pending the conclusion of disciplinary proceedings against him or her. The University reserves the right, in appropriate circumstances, to treat breaches of this Policy as offences of gross misconduct. In addition, breaches of these rules which are also breaches of English law may leave the person in question open to legal action from external bodies and/or the University.

Use of IT Systems

Ensure that you log out from any University laptop/workstations once you have finished using them, both to keep your account secure, and to allow others to use the laptop/workstation.

Once a workstation/laptop has been left unattended for more than 15 minutes, an automatic logoff process will be activated, giving you 5 minutes to cancel it. If this process is not cancelled, your account will be logged off and any unsaved data will be lost. This facility has been put into place to prevent workstations being locked for prolonged periods of time and to ensure their availability to other users.

You should ensure that you save all of your files regularly to your OneDrive account and not to your desktop, as the desktop is not backed up. Your OneDrive account can be accessed from anywhere with Internet access, which facilitates off- site working and collaboration.

You must have up-to-date anti-virus software on your personal computer if you are using the University network. ITS provides free antivirus software – see the Intranet for details.

Email

Email is not a secure medium of communication - it can be intercepted and read. Do not use it to say anything you would not wish to be made public, and restrict the use of sending confidential, personal, or sensitive data via email, and only when it is encrypted via a password accessible to authorised recipients. Where possible, a link to a password-protected file which is stored on a OneDrive secure area should be sent rather than the actual file to reduce the chance of unauthorised access to data.

University-wide news and emails from your faculty/department will be sent to your University email account, so you should check it frequently. Regular "housekeeping"

(in particular, the deletion of unnecessary emails) should be carried out in order to control mailbox size and keep your access speed high.

The sending of 'All Staff' or 'All Students' emails is not allowed, except by certain authorised email account holders. All Staff and All Student emails are used only to convey crucial messages when an unplanned event or a news item of significance occurs, such as the notification of an IT system outage, flood etc.

Please note: The University states that all formal communication between staff and students should be conducted via your Regent's University London email account. Email forwarding is available for students should they wish to forward their Regent's University London email to personal email accounts. **Regent's University London Students and Staff must conduct email communications with Regent's University London Staff and Students via their Regent's University London Email account.**

Contracts

You are expressly forbidden from using the University Facilities for conducting personal activities such as setting up a website, conducting private advertising or publicity campaigns via e-mail.

REGENT'S
UNIVERSITY LONDON

Policy version tracking

Version Number	Date	Revision Description	Editor	Status
1.0	12/09/2012	Edit and Revision	JN CIO	<updated, approved, published>
1.1	25/08/2013	Edit and Revision	JN CIO	<updated, approved, published>
2.0	30/10/2015	Adoption of UCISA Template version	DT CIO	<updated, approved, published>
2.1	09/12/2016	Edit and Revision Prevent	DT CIO	<updated, approved, published>
2.2	05/08/2019	Minor edit to include explicit phishing reference and link to updated DP policy	DT CIO	<updated, approved, published>
2.3	20/07/21	Minor edit	AR IT Director	<updated, approved, published>