
# IT Acceptable Use Policy

## Office of the CIO

## Version 2.0

REGENT'S
UNIVERSITY LONDON

**Document Revision History**

| Version | Date | Author | Description of Change |
|---|---|---|---|
| 1.00 | 12/09/2012 | JN CIO | Edit and Revision |
| 1.1 | 25/08/2013 | JN CIO | Edit and annual revision |
| 2.0 | 30/10/2015 | DT CIO | Adoption of UCISA Template version |

REGENT'S
UNIVERSITY LONDON

**Contents**

## Core Regulations

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

The issues covered by these regulations are complex and you are strongly urged to read the accompanying guidance document (Appendix A).

## Scope

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

## 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 Janet, Eduserv and Jisc Collections.

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

Some software licences procured by RUL 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 accompanying guidance for more detail.)

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

## Authority

These regulations are issued under the authority of the Office of the CIO (OCIO) who is also responsible for their interpretation and enforcement, and who may also delegate such authority to other people.

You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of these regulations. If you feel that any

such instructions are unreasonable or are not in support of these regulations, you may appeal to the Chief Information Officer.

## Intended use

The IT facilities are provided for use in furtherance of the mission of RUL, 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 Chief Information Officer.

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. See the accompanying guidance for further details.

## Identity

You must take all reasonable precautions to safeguard your identifty (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 RUL'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.

## Information

If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it and must observe RUL's Data Protection and Information Security policies particularly with regard to removable media, mobile and privately owned devices.

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 Chief Information Officer.

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

## Behaviour

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

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

You should also adhere to RUL'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

RUL 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

RUL 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 Electronic Communications and Monitoring Policy.

### Infringement

Infringing these regulations may result in sanctions under the institution's disciplinary procedure. 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.

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

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

REGENT'S
UNIVERSITY LONDON

## Appendix A

### *General Guidelines*

1. ITS services, administered by Regent's University London (the University), may be used only by students and staff of the University and other persons authorised in writing. The authorisation needs to be by the CIO, Deputy CIO or the Manager of the ITS Department.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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 authorized by the ITS Department.

7. 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 licence 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.

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 CIO or the Head of the Department 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 licence 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 1998, 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 Computer Systems*

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

Once a workstation 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 U: drive and not to your desktop. There is a risk of losing your data by doing so, as the desktop is not backed up. If you have important work to save, it is best to keep copies in more than one place, such as on your U: drive, and also on portable media such as a

USB device (memory stick, CD-RW, portable hard drive etc), or in an online repository (such as an email account or a cloud-based service).
You must have up-to-date anti-virus software on your own computer if you are using the RUL network.

### *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. If you are sending confidential information by email this should be sent using password protected attachments.

Campus news and emails from your faculty 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 particular 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 RUL Facilities for conducting personal activities such as setting up a website, conducting private advertising or publicity campaigns via e-mail.