# Rules for the use of Richmond University Computers and Data Networks

The aim of these regulations is to help ensure that Richmond University 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.

## 1 Scope

These rules are derived from the Universities and Colleges Information Systems Association (UCISA) Model Regulations. They apply to anyone using the IT facilities (hardware, software, data, network access, third party services, online services or *IT credentials*) provided or arranged by Richmond, the American International University in London (hereafter called "Richmond University").

Users are responsible for ensuring that they are familiar with these rules and any specific rules that apply to particular systems.

## 2 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 are bound by Richmond University general regulations when using the IT facilities. These regulations can be found at the following locations but require authentication:

- Employees: details are in the Employment Handbook: https://my.richmond.ac.uk/hrservices/Documents/Employment%20Handbook,%20June%202015.pdf.
- Students: details are in the Student Code of Conduct: https://my.richmond.ac.uk/studentlife/Shared%20Documents/Forms/AllItems.aspx

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

Some software licences procured by Richmond 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.

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

## 3  Authority

These regulations are issued under the authority of the Chair of the Data and Information Policy Committee (DIPC) who is also responsible for their interpretation and enforcement, and who may also delegate such authority to other people.

You must not use the IT facilities without the permission of the Head of IT Services.

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, students may appeal using the institutional complaints and appeals policy, section 4; employees should address matters to their line manager, or in accordance with the Employment Handbook.

## 4  Intended use

The IT facilities are provided for use in furtherance of the mission of Richmond 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, requires the explicit approval of a member of the University's Executive team.

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.

## 5  Identity

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.

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.

## 6  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 Richmond University 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.


## 7   Information

If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it.

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 Chair of the Data and Information Policy Committee (DIPC).

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory.


## 8   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 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

Richmond 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;

- Other matters deemed appropriate by the Chair of the Data and Information Policy Committee (DIPC), provided this has the agreement of the president and/or the vice president for human resources and administration;

Richmond 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 of the Head of IT or a member of the University's Executive team.

**Infringement**

Infringing these regulations may result in sanctions under the institution's disciplinary processes. For Students these can be found in the Student Code of Conduct: https://my.richmond.ac.uk/studentlife/Shared%20Documents/Forms/AllItems.aspx; for employees these are available in the Employment Handbook https://my.richmond.ac.uk/hrservices/Documents/Employment%20Handbook,%20June%20 2015.pdf

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

Richmond University reserves the right to recover from you any costs incurred as a result of your infringement, in accordance with the procedures provided in the employment handbook or the student code of conduct.

A student must inform either Student Affairs or the Academic Registry if you become aware of any infringement of these regulations.

A member of staff and faculty must inform their line manager if you become aware of any infringement of these regulations.

**Guidance notes**

This guidance expands on the principles set out in the core regulations. It gives many examples of specific situations and is intended to help you relate your everyday use of the IT facilities to the *do's and don'ts* in the core regulations.

Where a list of examples is given, these are just some of the most common instances, and the list is not intended to be exhaustive.

Where the terms similar to Authority, Authorised, Approved or Approval appear, they refer to authority or approval originating from the person or body identified in section 3*, Authority,* or anyone with authority delegated to them by that person or body.

## 1   Scope

### 1.1   Users

These regulations apply to **anyone** using Richmond University IT facilities. This means more than students and staff. It could include, for example:

- Visitors to Richmond University website, and people accessing the institution's online services from off campus;

- External partners, contractors and agents based onsite and using Richmond University network, or offsite and accessing the institution's systems;

- Tenants of the institution using the University's computers, servers or network;

- Visitors using the institution's Wi-Fi;

- Students and staff from other institutions logging on using Eduroam.

### 1.2   IT facilities

The term IT facilities include:

- IT hardware that Richmond University provides, such as PCs, laptops, tablets, smart phones and printers;

- Software that the institution provides, such as operating systems, office application software, web browsers etc. It also includes software that the institution has arranged for you to have access to, for example, special deals for students on commercial application packages;

- Data that Richmond 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 institution. This would cover, for example, network connections in halls of residence, on campus Wi-Fi, connectivity to the internet from University PCs;

- Online services arranged by the institution, such as Office 365 and Google Apps, JSTOR, or any of the Jisc online resources;

- *IT credentials*, such as the use of your institutional login, or any other token

(email address, smartcard, dongle) issued by Richmond University to identify yourself when using IT facilities. For example, you may be able to use drop-in facilities (Guest) or Wi-Fi 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.

## 2 Governance

It is helpful to remember that using IT has consequences in the physical world.

Your use of IT is governed by IT specific laws and regulations (such as these), but it is also subject to general laws and regulations such as your institution's general policies.

### 2.1 Domestic law

Your behaviour is subject to the laws of the land, 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
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Defamation Act 1996 and Defamation Act 2013

So, for example, you may not:

- Create or transmit, or cause the transmission, of any 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 with the intent to cause annoyance, inconvenience or needless anxiety;

- Create or transmit material with the intent to defraud;

- Create or transmit defamatory material;

- Create or transmit material such that this infringes the copyright of another person or organisation;

- 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.

## 2.2 Foreign law

If you are using services 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.

In general, if you apply common sense, obey domestic laws and the regulations of the service you are using, you are unlikely to go astray.

## 2.3 General institutional regulations

You should already be familiar with Richmond University general regulations and policies.

These are available at:
https://my.richmond.ac.uk/Uniorg/policies_and_procedures/default.aspx

## 2.4 Third party regulations

If you use Richmond University 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 many UK Higher Education services site outside Richmond University 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, so if you abide by these regulations you should not infringe 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, 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 Richmond University has provided you with a piece of software or a resource.

- **Licence agreements**

  Users shall only use software and other resources in compliance with all applicable licences, terms and conditions.

  If you are unsure of the specific licence terms for a particular software package then please log a call with the IT helpline.

## 3   Authority

These regulations are issued under the authority of the Head of IT who is also responsible for their interpretation and enforcement, and who may also delegate such authority to other people.

Authority to use the institution'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 the campus.

If you have any doubt whether or not you have the authority to use an IT facility you should seek further advice from the IT & AV services department.

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

## 4   Intended use

Richmond University IT facilities are part- funded by the tax paying public. They have a right

to know that the facilities are being used for the purposes for which they are intended.

### 4.1 Use for purposes in furtherance of institution's mission

The IT facilities are provided for use in furtherance of the institution's mission. Such use might be for learning, teaching, research, knowledge transfer, public outreach, the commercial activities of the institution, or the administration necessary to support all of the above.

### 4.2 Personal use

You may currently use the IT facilities for personal use provided that it does not breach the regulations, and that it does not prevent or interfere with other people using the facilities for valid purposes (for example, using a PC to update your Facebook page when others are waiting to complete their assignments).

However, this is a concession and can be withdrawn at any time.

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.

### 4.3 Commercial use and personal gain

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 a member of Executive. The provider of the service may require a fee or a share of the income for this type of use. For more information, contact your line manager or a member of the Student Affairs team if you are a student.

Even with such approval, the use of licences under the Chest agreements for anything other than teaching, studying or research, administration or management purposes is prohibited, and you must ensure that licences allowing commercial use are in place.

## 5  Identity

Many of the IT services provided or arranged by the institution require you to identify yourself so that the service *knows* that you are entitled to use it.

This is most commonly done by providing you with a username and password, but other forms of *IT credentials* may be used, such as an email address, ID card or some other form of security device.

### 5.1 Protect identity

You must take all reasonable precautions to safeguard any *IT credentials* issued to you.

You must change passwords when first issued and at regular intervals or as instructed. Do not use obvious passwords, and do not record them where there is any likelihood of someone else finding them. Do not use the same password as you do for personal (i.e. non-institutional) accounts. Do not share passwords with anyone else, even IT staff, no matter how convenient and harmless it may seem.

Advice on how to construct a strong password can be found on the Portal *(IT & AV Services -> Information Security -> General Password Guidelines)*

If you think someone else has found out what your password is, change it immediately and report the matter to the IT department in person or via the IT Helpline.

Do not use your username and password to log in to websites or services you do not recognise, and do not log in to websites that are not showing the padlock symbol.

Do not leave logged in computers unattended, and log out properly when you are finished or "Lock" the screen using the combination CTRL-ALT-DELETE -> Lock this screen.

Don't allow anyone else to use your ID card or other security hardware. Take care not to lose them, and if you do, report the matter to IT and Security immediately.

### 5.2 Impersonation

Never use someone else's *IT credentials*, or attempt to disguise or hide your real identity when using the institution's 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).

### 5.3 Attempt to compromise others' identities

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

## 6  Infrastructure

The IT infrastructure is all the underlying *stuff* that makes IT function. It includes servers, the network, PCs, printers, operating systems, databases and a whole 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.

### 6.1 Physical damage or risk of damage

Do not damage, or do anything to risk physically damaging the infrastructure, such as being careless with food or drink at a PC or Apple Mac.

Do not move IT kit yourself without prior agreement from the IT department.

### 6.2 Reconfiguration

Do not attempt to change the setup of the infrastructure without authorisation, such as changing the network point that a PC / Apple Mac is plugged in to, connecting devices to the network (except of course for Wi-Fi or Ethernet networks specifically provided for this purpose) or altering the configuration of the institution's PCs. Unless you have been authorised, you must not add software to or remove software from PCs or Apple Macs.

Do not move equipment without authority.

### 6.3 Network extension

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.

6.4 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.

6.5 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 is basically 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 from people you do not know or inserting media that have been created on compromised computers.

If you avoid these types of behaviour, keep your antivirus software up to date and switched on, and run scans of your computer on a regular basis, you should not fall foul of this problem.

6.6 Subverting security measures

Richmond 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.


**7  Information**

7.1 Personal, sensitive and confidential information

During the course of their work or studies, staff and students (particularly research students) may handle information that comes under the Data Protection Act 1998, or is sensitive or confidential in some other way. For the rest of this section, these will be grouped together as protected information.

Safeguarding the security of protected information is a highly complex issue, with organisational, technical and human aspects. The institution has policies on Data Protection and Information Management and how we use data.

Further details for students along with the University student privacy statement can be found at http://www.richmond.ac.uk/wp-content/uploads/2014/12/NEW-Richmond-FPN-May-2014.pdf

For employees, the Staff Handbook provides more details and is found under the HR section of the Portal (https://my.richmond.ac.uk/hrservices/default.aspx). If your role is likely to involve handling protected information, you must make yourself familiar with and abide by these policies.

### 7.1.1   Transmission of protected information

When sending protected or personally sensitive information electronically, you must use a method with appropriate security. Email is not inherently secure. For advice about how to send protected information electronically please contact IT & AV Services.

### 7.1.2   Removable media and mobile devices

Protected information must not be stored on removable media (such as USB storage devices, removable hard drives, CDs, DVDs) or mobile devices (laptops, tablet or smart phones) unless it is encrypted, and the key kept securely.

If protected information is sent using removable media, you must use a secure, tracked service so that you know it has arrived safely. Advice on the use of removable media and mobile devices for protected information is available from the Portal -> IT & AV Services.

### 7.1.3   Remote working

If you access protected information from off campus, you must make sure you are using an approved connection method that ensures that the information cannot be intercepted between the device you are using and the source of the secure service.

You must also be careful to avoid working in public locations where your screen can be seen.

The University uses a Remote Desktop Service to connect safely and securely to corporate information systems when off campus.

Advice on working remotely with protected information is available from the portal: Portal -> IT & AV Services -> Useful Info.

### 7.1.4   Personal or public devices and cloud services

Even if you are using approved connection methods, devices that are not fully managed by Richmond University cannot be guaranteed to be free of malicious software that could, for example, gather keyboard input and screen displays. You

should not therefore use such devices to access, transmit or store protected information unless you have discussed it with the IT department prior to use.

Advice on the use of personal devices and how to encrypt them can be found under the Portal -> IT & AV Services -> Information Security.

### 7.2 Copyright information

Almost all published works are protected by copyright. If you are going to use material (images, text, music, software), the onus is on you to ensure that you use it within copyright law. This is a complex area, and training and guidance are available from Library staff. For further advice and guidance please refer to https://my.richmond.ac.uk/library/scancopy/advice/default.aspx  or contact library staff directly on librarian@richmond.ac.uk or in person at either Richmond or Kensington Library. The key point to remember is that the fact that you can see something on the web, download it or otherwise access it does not mean that you can do what you want with it.

### 7.3 **Others' information**

You must not attempt to access, delete, modify or disclose restricted information belonging to other people without their permission, unless it is obvious that they intend others to do this, or you have approval from the Chair of the Data and Information Policy Committee (DIPC).

Where information has been produced in the course of employment by Richmond University and the person who created or manages it is unavailable, the responsible line manager may give permission for it to be retrieved for work purposes. In doing so, care must be taken not to retrieve any private information in the account, nor to compromise the security of the account concerned.

Private information may only be accessed by someone other than the owner under very specific circumstances governed by institutional and/or legal processes.

### 7.4 Inappropriate material

Richmond 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, defamatory, threatening, discriminatory or extremist. The University reserves the right to block or monitor access to such material.

Richmond University has procedures to approve and manage valid activities involving such material for valid research purposes where legal with the appropriate ethical approval. For more information, please refer to the Chair of the Data and Information Policy Committee (DIPC).

Universities UK has produced guidance on handling sensitive research materials, available at
http://www.universitiesuk.ac.uk/highereducation/Pages/OversightOfSecuritySensitiveResearchMaterial.aspx

There is also an exemption covering authorised IT staff involved in the preservation of evidence for the purposes of investigating breaches of the regulations or the law.

### 7.5 Publishing information

Publishing means the act of making information available to the general public, this includes through websites, social networks and news feeds. Whilst Richmond University generally encourages publication, there are some general guidelines you should adhere to:

7.5.1    Representing the institution

You must not make statements that purport to represent Richmond University without the approval of the Chair of the Data and Information Policy Committee (DIPC).

7.5.2    Publishing for others

You must not publish information on behalf of third parties using the institution's IT facilities without the approval of the Chair of the Data and Information Policy Committee (DIPC).

## 8   Behaviour

The way you behave when using IT should be no different to how you would behave under other circumstances. Abusive, inconsiderate or discriminatory behaviour is unacceptable.

8.1 Conduct online and on social media

Richmond University policies concerning staff and students also apply to the use of social media. These include human resource policies, codes of conduct, acceptable use of IT and disciplinary procedures.

8.2 Spam

You must not send unsolicited bulk emails or chain emails other than in specific circumstances. Advice on this is available from IT & AV services.

8.3 Denying others access

If you are using shared IT facilities for personal or social purposes, you should vacate them if they are needed by others with work to do. Similarly, do not occupy specialist facilities unnecessarily if someone else needs them.

8.4 Disturbing others

When using shared spaces, remember that others have a right work without undue disturbance. Keep noise down (turn phones to silent if you are in a silent study area), do not obstruct passageways and be sensitive to what others around you might find offensive.

8.5 Excessive consumption of bandwidth/resources

Use resources wisely. Don't consume excessive bandwidth by uploading or downloading more material (particularly video) than is necessary. Do not waste paper by printing more than is needed, or by printing single sided when double sided would do. Don't waste electricity by leaving equipment needlessly switched on.

## 9 Monitoring

9.1 Institutional monitoring

Richmond University monitors and logs the use of its IT facilities for the purposes of:

- Detecting, investigating or preventing misuse of the facilities or breaches of the University's regulations;
- Monitoring the effective function of the facilities;
- Investigation of alleged misconduct;

Richmond University will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime, and ensuring national security.

9.2 Unauthorised monitoring

You must not attempt to monitor the use of the IT without the explicit permission of the Head of IT or a member of the University Executive team.

This would include:

- Monitoring of network traffic;
- Network and/or device discovery;
- Wi-Fi 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

10.1 Disciplinary process and sanctions

Breaches of these regulations will be handled by the Richmond University disciplinary processes.

For staff these are defined at:

- https://my.richmond.ac.uk/hrservices/default.aspx

For students (Student Code of Conduct):

- https://my.richmond.ac.uk/studentlife/Shared%20Documents/Forms/AllItems.aspx

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

Sanctions may be imposed if the disciplinary process finds that you have indeed breached the regulations, for example, imposition of restrictions on your use of IT facilities; removal of services; withdrawal of offending material; fines and recovery of any costs incurred by Richmond University as a result of the breach.

10.2 Reporting to other authorities

If the institution believes that unlawful activity has taken place, it will refer the matter to the police or other enforcement agency.

10.3 Reporting to other organisations

If the institution believes that a breach of a third party's regulations has taken place, it may report the matter to that organisation.

10.4 Report infringements

If you become aware of an infringement of these regulations, you must report the matter to the relevant authorities.

**Updated: 26/10/2017**