UNIVERSITY OF ROEHAMPTON

POLICY AND REGULATIONS FOR THE USE OF IT FACILITIES AND SYSTEMS (2016)

Originated by IT Services:	April 2014
Updated by Governance &Compliance Manager, IT, Library & Media Services:	March 2016
Endorsed by Senate:	27 April 2016
Approved by Council:	19 May 2016
Review Date:	March 2017

<div align="center">

UNIVERSITY OF ROEHAMPTON
POLICY AND REGULATIONS FOR THE USE OF IT
FACILITIES AND SYSTEMS (2016)

</div>

CONTENTS

Introduction

The aim of these regulations is to help ensure that the University of Roehampton's 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 in Appendix 1 attached**. This provides, not only more detailed information on the areas covered below, but also examples to aid further clarification.

Core Policy and Regulations

1.   Scope

These regulations apply to anyone using the IT facilities (hardware, software, data, network access, third party services, online services or *IT credentials*) provided or arranged by The University of Roehampton. IT Facilities are provided primarily to facilitate a person's essential work as an employee or student or other role within the University. The IT Facilities remain, at all times, the property of the University.

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 the University's general regulations when using the IT facilities, available at http://www.roehampton.ac.uk/Corporate-Information/Policies/.
- 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 the University of Roehampton 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 accompanying Guidance in Appendix 1 for more detail.*)
- 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 Senate and the Chief Information Officer who are 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 Senate and the Chief Information Officer 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, or you have any queries, these should be addressed to the University of Roehampton's Legal Officer.

4.   Intended Use

The IT facilities are provided for use in furtherance of the mission of the University of Roehampton, 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.
- You may only use the IT Facilities for commercial activities if you are an employee of the University and such use forms part of your duties of employment. You may not use the IT Facilities to advertise any trade, service or profession not endorsed by the University. You should raise any queries on whether a commercial activity using the IT Facilities is permitted with your line manager before commencing the relevant use of the IT Facilities.
- You must not use the IT facilities to plagiarise work authored by others. (Refer to the University's Academic Regulations for further details.)
- 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 accompanying Guidance in Appendix 1 for more detail.*)

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. No-one has the authority to ask you for your password, and you must not disclose it to anyone – refer to the [University of Roehampton Password Policy](#) for details.
- You will not be given administrative privileges on any IT facility unless you can provide sufficient justification to the CIO that your roles, or specific applications you use, require it. IT will investigate such justifications, and administrative rights will only be granted once the justification is validated. As a consequence you may need to agree to some additional conditions such following specific processes, or as best-endeavours support for the equipment. This does not apply to:

    a.   Users of laptops where remote IT support is not always possible whilst the user is away from campus for periods of time.

    b.   Users of applications which IT have investigated and reached the conclusion that there is no workaround to ensure the application works as required without administrative privileges.

- 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 from senior IT management:

- Damaging, reconfiguring or moving equipment;
- Loading software on University of Roehampton'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.

7.   Information

If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it and must observe the University of Roehampton's Data Protection and Information Security policies and guidance, available at http://www.roehampton.ac.uk/uploadedFiles/Pages_Assets/PDFs_and_Word_Docs/Policies/Data-Protection-Policy.pdf, 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 Vice-Chancellor, Deputy Vice-Chancellor or the Pro Vice-Chancellor.
- You must not, unless exempted through the University's ethics procedures, create, download, store or transmit unlawful material, or material that is indecent, offensive,

threatening or discriminatory or extremist. The University reserves the right to block or monitor access to such material.
- The University of Roehampton has procedures to approve and manage valid activities involving such material; these are available at http://www.roehampton.ac.uk/Research/Ethics/ and must be observed.
- Following such approval, the University of Roehampton has procedures to enable students to access and store downloaded research materials and data into a specially provisioned university secure safe storage area set up in line with the guidelines summarised in the report provided by Universities UK: Oversight of security-sensitive research material in UK universities: guidance.
- You must abide by The University of Roehampton's Intellectual Property Policy available at http://www.roehampton.ac.uk/Corporate-Information/Policies/ when using the IT facilities to publish information.

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

The University is committed to both protecting freedom of speech and academic freedom and to protecting and safeguarding its students and staff.

The University of Roehampton reserves the right to monitor and record 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;
- To protect the IT Facilities against viruses and hackers;
- To assist in the investigation of breaches of these Conditions of Use,
- To prevent or detect suspected or possible misconduct or crime or other unauthorised use of the IT Facilities;
- Where such access or monitoring is necessary, to pursue the University's other legitimate interests, for example the detection of plagiarism, or by accessing files and reviewing the emails of employees who are absent, or to enable the office functions to be undertaken/shared by appropriate members of staff.

The University acts in accordance with applicable legislation and the Information Commissioner's Employment Practices Data Protection Code, notably in relation to the monitoring of use of the IT Facilities.

The University of Roehampton 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 by the Vice-Chancellor, the Deputy Vice-Chancellor or the Pro Vice-Chancellor.

10. Infringement

Infringing these regulations may result in sanctions under the institution's disciplinary processes. See [Student Disciplinary Regulations and Staff Disciplinary Procedures](#).

If a complaint or allegation is received, your account may be immediately suspended for investigation. Penalties for breach of these Conditions of Use may include temporary or long term suspension of your access to the IT Facilities, and/or other disciplinary penalties up to and including expulsion from University in the case of a student, dismissal from the University in the case of staff, or a permanent suspension of access to facilities in the case of a conference attendee or other visitor. The University will cooperate fully with any police investigations in relation to the use of IT facilities.

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

University of Roehampton
IT Department
March 2016

POLICY AND REGULATIONS FOR THE USE OF
THE UNIVERSITY OF ROEHAMPTON IT FACILITIES AND SYSTEMS

APPENDIX 1 – 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 S*ection 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 the University's IT facilities. This means more than students and staff. It could include, for example:

- Visitors to the University's website, and people accessing the institution's online services from off campus;
- External partners, contractor and agents based on site and using the University's network, or offsite and accessing the institution's systems;
- Tenants of the University using the University's computers, servers or network;
- Visitors using the University's Wi-Fi;
- Students and staff from other institutions logging on using eduroam.

1.2 IT Facilities

The term IT Facilities includes:

- IT Hardware that the University of Roehampton provides, such as PCs, laptops, tablets, smart phones and printers;
- Software that the The University of Roehampton provides, such as operating systems, office application software, web browsers etc. It also includes software that the The University of Roehampton has arranged for you to have access to, for example special deals for students on commercial application packages;
- Data that the University of Roehampton 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 of Roehampton. This would cover, for example, network connections in halls of residence, on-campus WiFi, connectivity to the internet from University PCs;
- Online services arranged by the The University of Roehampton such as Office 365 and Google Apps, JSTOR, or any of the Jisc online resources;

- *IT credentials*, such as the use of your The University of Roehampton login, or any other token (email address, smartcard, dongle) issued by The University of Roehampton 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.

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 the University of Roehampton'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 Acts 1959 and 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
- Counter-Terrorism and Security Act 2015
- 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 Acts 1996 and 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;
- material with the intent to cause annoyance, inconvenience or needless anxiety;
- material with the intent to defraud;
- defamatory material;
- material such that this infringes the copyright of another person or organisation;
- 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; or
- Deliberately (and without authorisation) access networked facilities or services.

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

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 the University's general regulations and policies. These are available at http://www.roehampton.ac.uk/Corporate-Information/Governance/

2.4 Third Party Regulations

If you use the University's IT facilities to access third party services 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 University of Roehampton 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 Roehampton you will be using Janet, and subject to:

  - Janet Acceptable Use Policy: https://community.ja.net/library/acceptable-use-policy
  - Janet Security Policy: https://community.ja.net/library/janet-policies/security-policy; and
  - 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 Roehampton has provided you with a piece of software or a resource.

- Users shall only use software and other resources in compliance with all applicable licences, terms and conditions - if unsure please check with the IT Helpdesk.

3.   Authority

These regulations are issued under the authority of the University Senate via the Chief Information Officer who is also responsible for their interpretation and enforcement, and who may also delegate such authority to other people. http://www.roehampton.ac.uk/Corporate-Information/Governance/

Authority to use the University of Roehampton'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 a The University of Roehampton website; a self-service kiosk in a public area; or an open WiFi 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 ithelpdesk@roehampton.ac.uk

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

4.   Intended Use

The University's IT facilities, and the Janet network that connects institutions together and to the Internet, are 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 the University of Roehampton's Mission

The IT facilities are provided for use in furtherance of the The University of Roehampton's mission. Such use might be for learning, teaching, research, knowledge transfer, public outreach, the commercial activities of the University, 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 Senate via the Chief Information Officer.

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 University of Roehampton 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, a smart 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 as instructed. Do not:

- Use obvious passwords, and do not record them where there is any likelihood of someone else finding them.
- Use the same password as you do for personal (i.e. non-Roehampton) accounts.
- Share passwords with anyone else, even IT staff, no matter how convenient and harmless it may seem.
- Use your username and password to log in to websites or services you do not recognise, and do not log in to web sites that are not showing the padlock symbol.
- Leave logged in computers unattended, and log out properly when you are finished.
- Allow anyone else to use your smartcard or other security hardware. Take care not to lose them and, if you do, report the matter to IT immediately.

If you think someone else has found out what your password is, change it immediately and report the matter to IT via the IT Helpdesk. - ithelpdesk@toehampton.ac.uk

5.2   Impersonation

Never use someone else's *IT credentials*, or attempt to disguise or hide your real identity when using the University'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 playing football in a drop-in facility.

6.2 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 of course for WiFi or Ethernet networks specifically provided for this purpose) or altering the configuration of the University's PCs. Unless you have been authorised, you must not add software to or remove software from PCs.

Do not move equipment without authority.

6.3 Network Extension

You must not extend the wired or Wi-Fi network without authorisation. 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.

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 web sites.

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 anti-virus 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

Roehampton has taken measures to safeguard the security of its IT infrastructure, including things such as anti-virus 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 University has policies on Data Protection and Information Management - http://www.roehampton.ac.uk/corporate-information/Policies/ - and if your role is likely to involve handling protected information, you must make yourself familiar with and abide by these policies.

Additional guidance on the provisions of the Data Protection Act 1998 and how the University of Roehampton ensures compliance with it is available at https://portal.roehampton.ac.uk/information/it/Pages/Remote-Access.aspx

7.1.1 Transmission of Protected Information

When sending protected information electronically, you must use a method with appropriate security. Email is not inherently secure. Advice about how to send protected information electronically is available from the IT Helpdesk.

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.

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.

Advice on working remotely with protected information is available at https://portal.roehampton.ac.uk/information/it/Pages/Remote-Access.aspx

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 the IT Department at the University of Roehampton 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.

Do not store protected information in personal cloud services such as Dropbox unless securely encrypted first.

7.2 Copyright Information

Almost all published works are protected by copyright. If you are going to use material *(text, images, music, software*), the onus is on you to ensure that you use it within copyright law. The key point to remember is: just because you can see something on the web, download or otherwise access it, does not mean that you can do what you want with it. This is a complex area - see online training and guidance: http://www.roehampton.ac.uk/Library/Copyright.aspx

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 a Pro Vice-Chancellor.

Where information has been produced in the course of employment by the University of Roehampton, 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 the University of Roehampton and/or legal processes. For reference see http://jiscleg.al/AccessITAccounts

7.4   Inappropriate Material

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

Roehampton has procedures to approve and manage valid activities involving such material for valid research purposes where legal with the appropriate ethical approval.

[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 the University generally encourages publication, the general guideline to follow is that you must not make statements that purport to represent the University without the approval of the University Senate via the Chief Information Officer.

7.6   Publishing for Others

You must not publish information on behalf of third parties using the University of Roehampton's IT facilities without the approval of Senate via the Chief Information Officer.

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

The University's 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 the IT Helpdesk: ithelpdesk@roehampton.ac.uk

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 to 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. Do not:

- consume excessive bandwidth by uploading or downloading more material (*particularly video*) than is necessary;
- waste paper by printing more than is needed, or by printing single sided when double sided would do; or
- Waste electricity by leaving equipment needlessly switched on.

9.   Monitoring

9.1   Institutional Monitoring

Roehampton 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;
- To comply with the University's Prevent Duty
- The 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 IT without the explicit permission of the Chief Information Officer. This includes:

- 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

10.1 Disciplinary Process and Sanctions

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

This could have a bearing on your future studies or employment with the University of Roehampton 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 the University of Roehampton as a result of the breach.

10.2 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.

10.3 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.

10.4 Reporting Infringements

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

IT Department
April 2016