Guidance Notes in relation to the Policy on the Use of IT Facilities

Approved by	Executive Director (IT and Communication)		
Date approved	26/02/2015	**Status**	Approved
Policy owner	Andrew McCreath	**Impact assessed**	Yes
Version	Issue 1-0	**Date of next review**	June 2016

Guidance notes

This guidance expands on the principles set out in the IT Policy. It gives many examples of specific situations and is intended to help you relate your everyday use of the IT facilities to the Policy.

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

The IT Policy applies to **anyone** using RGU's IT facilities. This means more than students and staff. It could include, for example:

- People accessing the institution's online services from off campus;
- External partners, contractor and agents based onsite and using RGU's network, or offsite and accessing the institution's systems;
- Tenants of the institution using the University's computers, servers or network;
- Visitors, students and staff from other institutions using the institution's wifi;

1.2 IT facilities

The term IT facilities include:

- IT hardware that RGU 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.
- Data that RGU 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 includes, network connections in RGU halls of residence, on campus wifi, connectivity to the internet from University PCs;
- Online services arranged by the institution, such as Office 365 or any of the Library online resources;
- IT credentials, such as the use of your institutional login, or any other token (email address, smartcard, dongle) issued by RGU 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 the Policy for the use of IT Facilities, 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 but it is also subject to general laws and regulations such as RGU'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:

- **Copyright, Designs and Patents Act 1988**
- **Computer Misuse Act 1990**
- **Defamation Act 1996**
- **Human Rights Act 1998**
- **Data Protection Act 1998**
- **Regulation of Investigatory Powers Act 2000**
- **Freedom of Information (Scotland) Act 2002**
- **Privacy and Electronic Communications (EC Directive) Regulations 2003** (as amended)
- **Prevention of Terrorism Act 2005**
- **Terrorism Act 2006**

- **Equality Act 2010**

Links to the full text of each Act can be found at the end of this document.

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.

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 RGU's general regulations and policies.
These are available at http://www.rgu.ac.uk/about/planning-and-policy/policies.

2.4 Third party regulations

If you use RGU IT facilities to access third party service, software or resources you are bound by all the applicable licences, terms and conditions associated with that service or resource. (The association can be through something as simple as using your institutional username and password). As a user, if you access software and facilities provided to you by RGU, for the purposes for which it is provided, and comply with RGU policy and guidelines, then you are unlikely to infringe other licence terms.

When connecting to any site on the Internet you should be aware that you will be using Janet, a UK provided network infrastructure, and are 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**
- The Janet Eligibility Policy **https://community.ja.net/library/janet-policies/eligibility-policy**

The requirements of these policies have been incorporated into Policy for the use of IT Facilities, so if you abide by that policy you should not infringe the Janet policies.

2.5 Non-Academic and Third Party use

The licence terms of many software and online resources provided by RGU include restrictions which prevent non-academic use (e.g. commercial use), insist that copyright is respected, and prevent privileges granted under academic licences from being passed on to third parties.

If you wish to use RGU's IT facilities for non academic purposes, or if you wish to provide access to third parties (e.g. commercial clients or conference guests), this may breach license terms for software provided for academic use. You should contact the Head of IT Operations and Support prior to such use to ensure that all such access is properly licenced and, where appropriate, additional licence fees are paid.

3 Authority

This guidance is issued under the authority of the Executive Director (IT and Communication) who is also responsible for its 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 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 the IT Help Desk.

Attempting to use the IT facilities without the permission of the relevant authority is an offence under the Computer Misuse Act 1990.

4 Intended use

RGU's IT facilities, and the Janet network that connects institutions together and to the internet, are substantially 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 use the IT facilities for personal use provided that it does not breach the policy, 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, non Institutional use and personal gain

Use of IT facilities for non-institutional commercial purposes, or for personal gain is not permitted.

Use of IT Facilities for activities external to the University, but which are relevant to your role as a member of staff or student are permitted. Examples would be membership of professional bodies, or involvement with other external organisations whose activities are relevant to your role.

In all cases, however, you must ensure that you comply with the licences, terms and conditions of any IT software or services that you use.

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, 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. 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, as any security weaknesses in your personal accounts will put institutional IT facilities at risk. Do not share passwords with anyone else, even IT staff, no matter how convenient and harmless it may seem. It is good practice to change your passwords at regular intervals.

If you think someone else has found out what your password is, change it immediately and report the matter to the IT Help Desk.

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.

Don't 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 the IT Help Desk 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 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 institution's PCs. Unless you have been authorised, you must not add software to or remove software from PCs.

Do not move equipment without authority. You are likely to disrupt the operation or availability of equipment to others, and may be in breach of manual handling regulations if you have not been trained for this.

6.3 Network extension

You must not extend the wired or Wifi network without authorization. Such activities, which may involve the use of routers, repeaters, hubs or Wifi access points, can disrupt the network and are also likely to be in breach of the Janet Security Policy.

6.4 Setting up servers or other services

You must not set up any hardware or software (including access to externally hosted services) that would provide a service to others over the network without permission from IT Services. Examples would include externally hosted collaborative web sites, file sharing sites, external web sites.

Requests for the Introduction of any new IT based facilities to be used by staff or students should be submitted to the Executive Director (IT and Communication) for approval and may require approval by the University's Major Projects Group.

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.

6.6 Subverting security measures

RGU 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 constitutes personal data 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 and guidance on Data Protection and Information Management (https://you.rgu.ac.uk/org/ig/SitePages/Home.aspx) and if your role is likely to involve handling protected information, you must make yourself familiar with, and abide by these policies.

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 at http://www.rgu.ac.uk/current-students/library/library-home/library-policies/policy-on-copyright/. 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.

Where information has been produced in the course of employment by RGU, 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. RGU has procedures and safeguards for accessing information in these circumstances, and the Head of IT Operations and Support should be contacted if such access is required.

Private information may only be accessed by someone other than the owner under very specific circumstances governed by institutional and/or legal processes. Any such access must be approved on a case by case basis, by a member of RGU's Strategic Planning and Resources Group, and under advice from the University's Legal Adviser.

7.4 Inappropriate material

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

RGU has procedures to approve and manage valid activities involving such material for valid research purposes where this is legal and ethical. Any requests for such access should be passed to the IT Help Desk.

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 RGU generally encourages publication, there are some general guidelines you should adhere to:

7.5.1 Representing the institution

You must not make statements online that purport to represent RGU without the approval of The Director of Marketing, Communications and Student Recruitment. Further information is available from the social media toolkit web page at http://www.rgu.ac.uk/staff/rightclick-reloaded .

7.5.2 Publishing for others

You must not publish information as a service on behalf of third parties using the institution's IT facilities without the approval of the Executive Director (IT and Communication).

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

RGU'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, disciplinary procedures and Academic Regulations.

See also the Social Media Toolit at http://www.rgu.ac.uk/staff/rightclick-reloaded .

8.2 Spam

You must not send unsolicited bulk emails or chain emails unless this is clearly an integral part of a recognised organisational function (e.g. to communicate official news bulletins to all staff).

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, including any images or other material clearly visible on computer screens.

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.

9 Monitoring

9.1 Institutional monitoring

Users should be aware that RGU monitors and records the overall 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 the Policy for the use of IT Facilities;
- Investigation of alleged misconduct;

Monitoring of individual use, and accessing data in individual user accounts, will only be undertaken by specific members of staff as a recognised part of their normal duties. Any such activity will be:

- Approved by the Executive Director of IT & Communication, or another member of RGU's Strategic Planning and Resources Group
- For legitimate business reasons
- Justifiable
- Fair
- Proportionate
- Not unnecessarily intrusive
- Compliant with all applicable UK legislation such as the Data Protection, and Human Rights Acts.

RGU 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 yourself to monitor the use of RGU's IT facilities as such monitoring may in itself create security risks or interfere with the performance of the facilities. If you require information in relation to the use of RGU's IT facilities, you should contact the Executive Director (IT and Communication).
This includes any of the following monitoring activities:

- 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 the Policy for the use of IT Facilities will be handled by the RGU's disciplinary processes. For staff, this is the Disciplinary Policy and Procedure. For students, this is the Academic Regulations in particular A3, Section 2 (Student Misconduct Procedure). Links to these procedures can be found at http://www.rgu.ac.uk/about/planning-and-policy/policies.

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 breached the policy - 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 RGU as a result of the breach.

If you are a visitor to RGU, you may be denied further access to RGU's IT Facilities if you have breached the Policy for the use of IT Facilities.

For commercial and academic partners using RGU's IT facilities, breaches of the Policy for the use of IT Facilities may result in sanctions as defined in any contract or partnership agreement.

10.2 Reporting to other authorities

If RGU 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 RGU 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 the policy, you must inform your line manager (for staff) or your course tutor (for students). If you are uncertain who to contact, you should ask the IT Help Desk. For serious infringements or you should inform the Executive Director (IT and Communication).

Links to the full text of Acts listed in the Governance section of the Guidance notes

- **Copyright, Designs and Patents Act 1988**
  www.legislation.gov.uk/ukpga/1988/48/contents
- **Computer Misuse Act 1990**
  www.legislation.gov.uk/ukpga/1990/18/contents
- **Defamation Act 1996** **www.legislation.gov.uk/ukpga/1996/31/contents**
- **Human Rights Act 1998**
  www.legislation.gov.uk/ukpga/1998/42/contents
- **Data Protection Act 1998**
  www.legislation.gov.uk/ukpga/1998/29/contents
- **Regulation of Investigatory Powers Act 2000**
  www.legislation.gov.uk/ukpga/2000/23/contents
- **Freedom of Information (Scotland) Act 2002**
  www.legislation.gov.uk/asp/2002/13/contents
- **Privacy and Electronic Communications (EC Directive) Regulations 2003** (as amended)
  www.legislation.gov.uk/uksi/2003/2426/contents/made
- **Prevention of Terrorism Act 2005**
  www.legislation.gov.uk/ukpga/2005/2/contents
- **Terrorism Act 2006** **www.legislation.gov.uk/ukpga/2006/11/contents**
- **Equality Act 2010** **www.legislation.gov.uk/ukpga/2010/15/contents**

Acknowledgements

These guidance notes are based on the UCISA Model Regulations published at: http://www.ucisa.ac.uk/modelregs.