The aim of these regulations is to help ensure that the University's IT facilities are used safely, securely, lawfully and equitably. They are derived largely from the Universities and Colleges

Data that the 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 University. This covers, for example, network connections in halls of residence, on campus WiFi, connectivity to the internet from University PCs.

Online services arranged by the University, such as Office 365, email, or any of the Jisc online resources;

, such as the use of your University login, or any other token (email address, smartcard, dongle) issued by the University to identify yourself when using IT facilities. For example, you may be able to use drop in facilities or WiFi connectivity at otheT/F2t

those that are not apparently related to IT such as the laws on fraud, theft and harassment.

There are many items of

Create or transmit material which encourages terrorism or extremism

Create or transmit material with the intent to defraud;

Create or transmit false or defamatory material;

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

Create or transmit material containing confidential information about the University, its employees or students unless in the proper course of the duties or studies;

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.

This list is illustrative and is not intended to be exhaustive.

There is an excellent set of over views of law relating to IT use available at

.

If you are using IT Facilities and Systems 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.

You should apply common sense, obey domestic laws and the regulations of the service you are using (which in most cases will refer to legal requirements for the host country).

If you use the University's 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:

Janet Eligibility Policy

You must comply with any reasonable written or verbal instructions issued by the IT Department in support of these regulations.

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

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

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

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 the Chief Operating Officer.

Even with such approval, the 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). .

at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, electronic documents may be read by third parties, for example, passengers on public transport.

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. However, it is acceptable not to reveal your identity if the system or service clearly allows anonymous use (such as a public facing website).

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

The IT

software used to disrupt computer operation or subvert security.

University. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Real world standards of behaviour apply online and on social networking platforms, such as Facebook, Blogger and Twitter. In using the IT facilities you must act in accordance with the University's Values for Working Together and Professional Behaviours. Additionally:

You must not cause fear, alarm or distress to others.

You must not unlawfully discriminate against, harass, defame or bully others.

You must adhere to University guidelines on social media.

You must not send spam (unsolicited bulk email).

You must not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth or consumables.

You must not use the IT facilities in a way that interferes with others' valid use of them.

You must not attempt to monitor the use of the IT facilities without the explicit authority of the Director of IT . This would include:

Monitoring of network traffic; of

Network and/or device discovery;

Version	Keeper	Reviewed	Approved by	Approval date
1.0	ITS	Annually	UEB	December 2015
1.1	ITS	Annually		September 2016
1.2	ITS	Annually		September 2017