UCISA TOOLKIT

Model IT Regulations

for the use of institutional IT facilities and systems

ucisa

Universities and Colleges Information Systems Association

Contents

Universities and Colleges
Information Systems Association

University of Oxford
13 Banbury Road
Oxford OX2 6NN

Tel: +44 (0)1865 283425
Fax: +44 (0)1865 283426
Email: admin@ucisa.ac.uk
www.ucisa.ac.uk

Executive summary

Most, if not all, universities and colleges have regulations or guidance about the use of IT facilities in their institution by students, staff and other users. These often form part of student regulations and staff terms and conditions of employment, and complement other organisations' regulations and policies, as well as wider legislation.

Institutional regulations provide something of a safeguard. A user of an institution's IT facilities, by signing or otherwise accepting them, is committing to behave appropriately when using the facilities. The institution, by linking such regulations to disciplinary procedures and by taking action on breaches, can demonstrate that they are seeking to ensure that the law is not breached and that their students and staff are aware of their responsibilities. The efficacy of such regulations was highlighted during the passage of the Digital Economy Bill through Parliament where, in the Committee stages of the Bill, the effectiveness of the processes in operation in the sector was recognised.

UCISA has sought to reduce the burden on individual institutions by producing Model Regulations for the use of IT facilities. This, the third edition, takes into account the increased use of personal devices to access institutional facilities and the growth of the use of social networks.

The Model Regulations are intended to be used, in whole or in part, as a template for institutions to tailor to their own requirements. The creation of these Model Regulations demonstrate UCISA's commitment to furthering good IT governance in the sector and, in turn, help universities and colleges to show that they have effective processes in place for managing their IT user base.

Introduction

This document is designed to provide a brief, easily comprehensible set of regulations for the use of IT facilities in UK HE institutions.

The regulations are presented at three levels:

1. A simplified code, suitable for login *splash* screens, listing just the essential points;
2. The core regulations, based around a set of 10 principles that we expect will remain stable as technology and legislation evolves;
3. A set of guidelines giving more information about and current examples of specific activities that would constitute a breach of the regulations.

It is suggested that the simplified code and the guidelines should remain outside your institution's formal approval process, so that they may be changed as required to draw the attention of new users to issues of the moment.

Finally, a gap analysis compares the content of the UCISA Model IT Regulations with directives drawn from sample institutional IT regulations; Janet and Eduserv requirements; requirements highlighted from the qualitative research and suggestions drawn from the *UCISA Information Security Toolkit*.

The regulations have been drafted to work with, rather than to reiterate, existing laws and institutional policies. So, for example, you will find references to general institutional regulations, information security policies and publication policies. It is assumed that the users are familiar with these other laws and regulations, and the IT regulations do not attempt to provide summaries of them.

Changes since 2007

The UCISA Model IT Regulations were last published in 2007, since then the context in which IT is used has changed considerably.

Significant research has been undertaken within the sector to determine how the Model IT Regulations should be revised. This has included a survey of UCISA IT Directors, discussions with key stakeholders and analysis of existing IT regulations from a large sample of institutions.

It seems unlikely that the context will remain static in the future, therefore, the regulations have been redrafted around a set of 10 core principles that should be relatively stable.

This means that while the 2014 regulations should enjoy some degree of longevity, it is not practicable to list the changes from the 2007 version – they have been rewritten from the ground up.

Some of the recent changes taken into account include:

- The growth in the use of social media by both users and institutions;
- The growth in the provision of wifi and the use of personally owned devices to access the network (Bring Your Own Device or BYOD);
- The growth in the use of cross institutional and transnational resources;
- The growth in the institutional adoption of cloud based services;
- The increased importance of cyber security.

Some of these changes have been reflected in explicit specific content within the revised regulations; others are implicit in the way the principles have been constructed.

There has been relatively little new specific IT legislation since 2007, the key items being the Equality Act 2010, the Defamation Act 2013 and the Electronic Communications (EC Directive) Regulations 2003 (as amended).

Tailoring

You will need to adapt the Model Regulations to suit your institution's local requirements.

As a minimum, you will need to:

- Insert the name of your institution;
- Nominate the ultimate authority for the regulations;
- Insert references to other institutional regulations and policies and
- Identify which domestic laws apply locally.

Parts of the regulations are likely to require tailoring and it is also quite possible that you may want to change the content of some of the regulations to suit local conditions.

You may wish to *cherry pick* some of the regulations to incorporate into your existing set, and you are welcome to do so.

The regulations do not include a disclaimer (of the form *The Institution is not liable for any loss resulting from problems with the IT service*) as it was widely felt that firstly it was of dubious value and, secondly, it should be in a service agreement rather than in regulations, if anywhere. Please feel free to include one if you feel that it would be of value to your institution.

Whatever level of tailoring you apply, UCISA strongly recommends that you consult your institution's legal advisers before publishing the regulations.

Presentation

Each institution will have its own approach to presenting its IT regulations to the user community, and we would not wish to dictate how this should be done.

However, one theme that emerged strongly from the qualitative research leading up to the redrafting is worthy of note. If you want the regulations to go beyond laying out what is and is not acceptable, and actually influence the behaviour of users, then you should embed them in some form of educational process. Simply making them available and drawing users' attention to them (even by *click to accept*) is unlikely to make much difference in practice.

Simplified code

[This simplified code, listing essential points, is suitable for login splash screens]

The following is a very brief summary of the main points of the IT regulations. You are expected to be familiar with the full regulations, which are available at <insert institutional URL>.

- **Governance**

  Don't break the law, do abide by <institution's> regulations and policies, and do observe the regulations of any third parties whose facilities you access.

- **Identity**

  Don't allow anyone else to use your IT credentials, don't disguise your online identity and don't attempt to obtain or use anyone else's.

- **Infrastructure**

  Don't put the institution's IT facilities at risk by introducing malware, interfering with hardware or loading unauthorised software.

- **Information**

  Safeguard personal data, respect other people's information and don't abuse copyright material. Remember that mobile devices may not be a secure way to handle information.

- **Behaviour**

  Don't waste IT resources, interfere with others' legitimate use or behave towards others in a way that would not be acceptable in the physical world.

Core regulations

The aim of these regulations is to help ensure that <institution'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 document, available at <institution URL>. This gives more detailed information that we hope you will find useful.

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 <institution>.

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 <institution's> general regulations when using the IT facilities, available at <institutional URL>.

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 <institution> and the institution where you are accessing services.

Some software licences procured by <institution> will set out obligations for the user – these should be adhered to. If you use any software or resources covered by a Chest agreement, you are deemed to have accepted the Eduserv User Acknowledgement of Third Party Rights. (See accompanying guidance for more detail.)

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

3 Authority

These regulations are issued under the authority of <designated authority within institution> 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 <designated authority within institution>.

You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of these regulations. If you feel that any such instructions are unreasonable or are not in support of these regulations, you may appeal to <named department/person/authority within institution> or <link to complaints handling procedure>.

4 Intended use

The IT facilities are provided for use in furtherance of the mission of <institution>, 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 <add institutional contact>.

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 <institution'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 institution's> Data Protection and Information Security policies and guidance, available at <institutional URL>, 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 authority>.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory. <Institution> has procedures to approve and manage valid activities involving such material; these are available at <institutional ethics approval process URL> and must be observed.

You must abide by <institution's> publication policy available at <institutional URL> 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 should also adhere to <institution's> guidelines on social media.

You must not send spam (unsolicited bulk email).

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

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

9 Monitoring

<Institution> 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;
- <insert any other purposes covered by your institution's policies e.g. dealing with email in an employee's absence>.

<The institution> 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 <link to the institution's interception monitoring policy>.

10 Infringement

Infringing these regulations may result in sanctions under the institution's disciplinary processes <institutional URL>. Penalties may include withdrawal of services and/or fines. Offending material will be taken down.

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

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

You must inform <institutional named contact/department, with URL> 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 <institution's> IT facilities. This means more than students and staff. It could include, for example:

- Visitors to <institution's> website, and people accessing the institution's online services from off campus;
- External partners, contractor and agents based onsite and using <institution's> 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 wifi;
- Students and staff from other institutions logging on using Eduroam.

1.2 IT facilities

The term IT facilities include:

- IT hardware that <institution> 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 <institution> 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 wifi, connectivity to the internet from University PCs; [If your students make use of commercially provided halls of residence, you may wish to modify the above to suit the regulatory framework in place there]
- 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 <institution> 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 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**

Links to the full text of each Act can be found on page 24.

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 <institution's> general regulations and policies.

These are available at <institutional URL>.

2.4 Third party regulations

If you use <institution> 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 any site outside <institution> 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. [If you modify this template, you must check that it still incorporates the Janet requirements]

- **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 <institution> has provided you with a piece of software or a resource.

- **Licence agreements**
  [Institutions to customise this section: add any other end user obligations required by licences they have procured, or if there are too many to list, state *Users shall only use software and other resources in compliance with all applicable licences, terms and conditions* and, if possible, explain how the user can find out what licence conditions apply].

3 Authority

These regulations are issued under the authority of <named institutional authority URL link> 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 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 [provide URL, or point to source of help].

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

4 Intended use

<Institution'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 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 <add institutional contact>. The provider of the service may require a fee or a share of the income for this type of use. For more information, contact <institutional contact>.

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, 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. 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.

If you think someone else has found out what your password is, change it immediately and report the matter to IT <insert institutional URL>.

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 IT 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.

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 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 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

<Institution> 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 <institutional URL for 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 <institution> ensures compliance with it is available at <institutional URL>.

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 at <institutional URL>.

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 at <institutional URL>.

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 <institutional URL>.

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 <institution> 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.

[Institutions may wish to tailor the above if you have undertaken an assessment of the security and privacy issues of BYOD and reached a less restrictive conclusion]

Advice on the use of personal devices to access institutional services is available at <institutional URL>.

[Institution may wish to tailor this section: if the institution provides cloud based tools, such as Google Apps, Office 365, Pebble Pad, it will have undertaken an assessment of the security and privacy implications, and you must comply with any guidance for their use].

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 (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 <institutional URL>. 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 <authority>.

Where information has been produced in the course of employment by <institution>, 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. [Institutions may wish to refer to the Jisc Legal template **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.

<Institution> 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 <institutional URL>.

[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 <institution> 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 <institution> without the approval of <insert institutional authority>.

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 <insert institutional authority>.

[If your institution has a publication policy, you should include a link to it here. If this prohibits publishing material that would bring the institution into disrepute, you might want to mention this as a further guideline]

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

<Institution'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.

[If your institution has a social media policy, you should include a link to it here. Jisc Legal has produced a Social Media for Staff Policy Template to help institutions make decisions on how social media might be used within institutions. **http://jiscleg.al/smediapolicy**].

8.2 Spam

You must not send unsolicited bulk emails or chain emails other than in specific circumstances. Advice on this is available from <institutional URL>.

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

<Institution> 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;
- <insert any other purposes covered by your institution's policies e.g. dealing with email in an employee's absence>.

<Institution> 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.

For more information, please refer to <link to Institution's interception and monitoring policy>.

9.2 Unauthorised monitoring

You must not attempt to monitor the use of the IT without the explicit permission of <institutional representative>.

This would include:

- 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 <institution's> disciplinary processes, defined at <institutional URL>.

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 <institution> 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.

UCISA Model Regulations – Gap Analysis

This document lists the requirements of Model IT Regulations that were identified in the research phases, and shows how they have been incorporated into the UCISA Model IT Regulations.

Key to incorporation:

Absent – this requirement is not reflected in this level of the regulations

Implicit – this requirement is covered in this level of the regulations by generic wording or generic reference to an external source

Referred – this requirement is covered in this level of the regulations by specific reference to an external source

Explicit – this requirement is laid out explicitly in this level of the regulations

Where appropriate, section and paragraph numbers (**P**) are quoted.

When reviewing the directives extracted from the UCISA Information Security Toolkit, it should be remembered that the Model IT Regulations are not intended to replace an institution's Information Security Policy, but should work in tandem with it.

Directive	Simplified code	Core regulations	Guidance
Most frequent directives from sample regulations			
Respect copyright material and software licence conditions	Explicit	Explicit 7 **P** 2	Explicit 7.2
Do not download or create obscene or offensive material	Implicit	Explicit 7 **P** 4	Explicit 7.4
Do not allow others to use your login, or reveal your password to anyone	Explicit	Explicit 5	Explicit 5.1
Comply with English/Scottish Law	Explicit	Explicit 2	Explicit 2.1
Statement on use of facilities for commercial gain	Absent	Explicit 4 **P** 3	Explicit 4.3
Do not send spam/chain email	Implicit	Explicit 8 **P** 4	Explicit 8.4
Definition of who the regulations apply to	Absent	Explicit 1	Explicit 1.1
Definition of what facilities the regulations cover	Absent	Explicit 1	Explicit 1.2
Do not publish defamatory material/emails	Implicit	Implicit 7 **P** 4	Explicit 7.4
Statement on use of facilities for personal, non-university purposes	Absent	Explicit 4 **P** 2	Explicit 4.2
You must comply with third party regulations (e.g. Janet AUP)	Explicit	Explicit 2 **P** 5	Explicit 2.4
Notice of institutional monitoring and its purposes	Absent	Explicit 9 **P** 1	Explicit 9.1
Do not attempt to circumvent security measures	Absent	Explicit 6	Explicit 6.6
Infringement can lead to disciplinary proceedings	Absent	Explicit 10 **P** 1	Explicit 10.1
Do not attempt to access other people's information	Explicit	Explicit 7 **P** 3	Explicit 7.3
Do not interfere with others' legitimate use of the facilities	Explicit	Explicit 8 **P** 3	Explicit 8.1, 8.2
Do not introduce malware	Explicit	Explicit 6	Explicit 6.5
Restrictions on connecting equipment to the wired network	Implicit	Explicit 6	Explicit 6.2, 6.3
Do not cause offence, concern, annoyance etc., to other users	Implicit	Explicit 8	Explicit 8
Infringement may lead to suspension of service	Absent	Explicit 10 **P** 1	Explicit 10.1
Do not attempt to use someone else's identity	Explicit	Explicit 5 **P** 2	Explicit 5.2
Do not damage equipment	Implicit	Explicit 6	Explicit 6.1
Do not attempt to access facilities you are not authorised for	Absent	Explicit 3 **P** 2	Explicit 3 **P** 4
Special measures to be taken when handling personal data	Explicit	Explicit 7 **P** 1	Explicit 7.1
Do not publish or download discriminatory material	Implicit	Explicit 7 **P** 4	Explicit 7.4
Do not bring the University into disrepute	Implicit	Implicit 2 **P** 4	Explicit 7.5
Do not interfere with the configuration of university computers	Explicit	Explicit 6	Explicit 6.2
Restrictions on food, drink and/or smoking	Implicit	Implicit 6	Implicit 6.1
Infringement may be reported to law enforcement	Absent	Explicit 10 **P** 2	Explicit 10.2
Disclaimer for loss of service	Absent	Absent	Absent
Do not move equipment	Implicit	Explicit 6	Explicit 6.2
Special measures to be taken when handing confidential data	Absent	Explicit 7 **P** 1	Explicit 7.1
Do not interfere with the configuration of university network equipment	Explicit	Explicit 6	Explicit 6.2
Do not send emails with a false sender	Explicit	Explicit 5 **P** 3	Explicit 5.2
University may charge for costs incurred as a result of infringement	Absent	Explicit 10 **P** 3	Explicit 10.1

Directive	Simplified code	Core regulations	Guidance
Disclaimer for loss of data	Absent	Absent	Absent
Do not set up servers (games, file sharing, IRC etc.)	Absent	Explicit 6	Explicit 6.4
Do not monitor the network without authority	Absent	Explicit 9 **P** 2	Explicit 9.2
Restrictions/policy on publishing on the web	Absent	Referred 7 **P** 5	Referred 7.5
Do not attempt to obtain someone else's credentials	Explicit	Explicit 5 **P** 2	Explicit 5.2
Reserves the right to take down infringing material	Absent	Explicit 10 **P** 1	Explicit 10.1 **P** 3
Information on termination of service at end of study/ employment	Absent	Absent	Absent
You must change your password regularly	Absent	Implicit 5 **P** 1	Explicit 5.1 **P** 2
You must change your password if you believe it has been compromised	Absent	Implicit 5 **P** 1	Explicit 5.1 **P** 3
Personal/confidential information must be encrypted on removable media	Implicit	Referred 7 **P** 1	Referred 7.1.2
Only use approved connection methods when working remotely	Absent	Referred 7 **P** 1	Explicit 7.1.3
Switch off mobile in labs/drop ins	Implicit	Implicit 8	Explicit 8.2
You must report any observed infringement to IT staff	Absent	Explicit 10 **P** 4	Explicit 10.4
You must comply with the instructions of IT staff	Absent	Explicit 3 **P** 3	Absent
Guidance on ownership of information after end of study/employment	Absent	Absent	Absent
You must carry ID at all times	Absent	Absent	Absent
Restrictions on systems storing payment card details	Absent	Referred 7 **P** 1	Referred 7.1
You must not download or publish terrorist material	Implicit	Implicit 2 **P** 2, 7 **P** 4	Explicit 2.1
You must not use the facilities for fraudulent purposes	Implicit	Implicit 2 **P** 2	Explicit 2.1
You must comply with written notices in IT areas	Absent	Explicit 3 **P** 3	Absent
Media containing sensitive information must be sent by tracked means	Implicit	Referred 7 **P** 1	Referred 7.1 Explicit 7.1.2
Restriction on using public devices when remote working	Absent	Implicit 7 **P** 1	Referred 7.1.3 Explicit 7.1.3
Restriction on using public location when remote working	Absent	Implicit 7 **P** 1	Referred 7.1.3 Explicit 7.1.3
Restriction on using unsecured Wifi when remote working	Absent	Implicit 7 **P** 1	Referred 7.1.3 Explicit 7.1.3
You must vacate accessible facilities if they are required by a user who needs them	Implicit	Implicit 8 **P** 3	Explicit 8.1
Infringement may be reported to third parties whose regulations have been breached	Absent	Explicit 10 **P** 2	Explicit 10.3
Directives from Janet			
Janet AUP – don't do unlawful things	Explicit	Explicit 2 **P** 1	Explicit 2.1
Janet AUP – don't do things that jeopardise the infrastructure	Explicit	Explicit 6	Explicit 6
Janet AUP – don't do things not in furtherance of the missions of the user organisation	Absent	Explicit 4	Explicit 4
Janet Eligibility Policy – don't grant anyone else access to Janet	Absent	Explicit 5 **P** 1, Explicit 6 **P**	Explicit 5.1, Explicit 6
Janet Security Policy – don't share issued identity	Explicit	Explicit 5 **P** 1	Explicit 5.1
Janet Security Policy – do obey instructions of local IT staff	Absent	Explicit 3 **P** 3	Absent

Directive	Simplified code	Core regulations	Guidance
Directives from Eduserv			
Only use Chest licensed material for teaching, studying or research, administration or management	Implicit	Explicit 4 **P** 4	Explicit 4.3
Users are bound by End User Acknowledgement of Third Party Rights	Implicit	Explicit 2 **P** 5	Explicit 2.4
Other issues raised in research			
BYOD	Implicit	Referred 7 **P** 1	Referred 7.1.4 Explicit 7.1.4
Wifi	Absent	Implicit 1,6,7,9	Explicit 1,6,7,9
Social media	Absent	Implicit 2,4,5,7,8	Implicit 2,4.2,5,7.4,8.1
Cloud services	Absent	Referred 7 **P** 1 Implicit 7 **P** 1	Referred 7.1.4 Explicit 7.1.4
Suggestions from UCISA Security Toolkit			
C i – A nominated person is responsible for ensuring that all staff and students are fully aware of, and agree to comply with, their legal responsibilities with respect to their use of computer based information systems and data. Such responsibilities are to be included within key staff and student documentation, such as Terms and Conditions of Employment and the Organisation Code of Conduct. Users to be deterred from using information processing facilities for unauthorised purposes.	Explicit	Explicit 2 **P** 2, 3 **P** 2	Explicit 2.1, 2.2, 3 **P** 4
C iii – A nominated person is responsible for preparing guidelines to ensure that all staff and students are aware of the key aspects of the law of copyright, in so far as these requirements impact on their duties or studies.	Explicit	Explicit 7 **P** 2	Explicit 7.2
C viii – Information regarding the organisation's applicants, students, suppliers or other people dealing with the organisation is to be kept confidential and must be protected and safeguarded from unauthorised access and disclosure.	Explicit	Explicit 7 **P** 1	Explicit 7.1
C ix – Persons responsible for Human Resources management are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organisation and to external parties.	Explicit	Explicit 7 **P** 1	Explicit 7.1
C x – A nominated person is responsible for preparing guidelines to ensure that all staff and students are aware of the key aspects of computer misuse legislation (or its equivalent), in so far as these requirements impact on their duties.	Implicit	Implicit 2 **P** 1	Explicit 2.1
C xi – Staff and students are prohibited from writing derogatory remarks about other persons or organisations.	Implicit	Explicit 7 **P** 4	Explicit 7.4
C xiii – All staff and students are required to comply fully with the organisation's information security policies. The monitoring of such compliance is the responsibility of management.	Implicit	Explicit 7 **P** 1	Explicit 7.1

Directive	Simplified code	Core regulations	Guidance
D i – All third parties who are given access to the organisation's information systems, whether as suppliers, customers or otherwise, must agree to follow the information security policies of the organisation. An appropriate summary of the information security policies and the third party's role in ensuring compliance must be formally delivered to any such third party, prior to their being granted access.	Absent	Implicit 1	Implicit 1
E i – All employees must comply with the information security policies of the organisation. Any information security incidents resulting from non-compliance should result in appropriate disciplinary action.	Implicit	Explicit 7 **P** 1	Explicit 7.1
F iv – Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the organisation's business operations and information processing systems. Mechanisms shall be in place to monitor and learn from those incidents.	Absent	Absent	Absent
F v – Procedures will be established for the reporting of software malfunctions and faults in the organisation's information processing systems. Faults and malfunctions shall be logged and monitored and timely corrective action taken.	Absent	Absent	Absent
G vi – This organisation advocates a clear desk and screen policy particularly when employees are absent from their normal desk and outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.	Absent	Referred 7 **P** 1	Referred 7.1
G vii – Removal off site of the organisation's sensitive information assets, either printed or held on computer storage media, should be properly authorised by management. Prior to authorisation a risk assessment based on the criticality of the information asset should be carried out.	Implicit	Referred 7 **P** 1	Referred 7.1
G xiii – All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary should be applied by management and determined by the classification of the information in question.	Implicit	Referred 7 **P** 1	Referred 7.1
G xx – Unsolicited mail should not receive serious attention until and unless the sender's identity and authenticity of the mail have been verified.	Absent	Absent	Absent
G xxiii – Prior to sending sensitive information or documents to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party, must be seen to continue to assure the confidentiality and integrity of the information.	Implicit	Referred 7 **P** 1	Referred 7.1

Directive	Simplified code	Core regulations	Guidance
G xxiv – Sensitive data or information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured throughout the transfer.	Implicit	Referred 7 **P** 1	Referred 7.1
G xxxiv – Email should only be used for business purposes in a way which is consistent with other forms of business communication. The attachment of data files to an email is only permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code.	Implicit	Referred 7 **P** 1	Referred 7.1
G xxxv – Information received via email must be treated with care due to its inherent information security risks. File attachments should be scanned for possible viruses or other malicious code.	Implicit	Referred 7 **P** 1	Referred 7.1
H vi and I i – All users shall have a unique identifier (user ID) for their personal and sole use for access to all computing services. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason.	Explicit	Explicit 5	Explicit 5.1
I ii – The selection of passwords, their use and management must adhere to best practice guidelines.	Implicit	Implicit 5	Implicit 5.1
I iii – Equipment must be safeguarded appropriately – especially when left unattended.	Absent	Implicit 5	Explicit 5.1
I iv and K xii – Files downloaded from the internet, including mobile code and files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.	Absent	Implicit 6	Explicit 6.5
I v – Electronic mail must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed and that the recipients are authorised to receive it.	Implicit	Implicit 7 **P** 1	Explicit 7.1.1
I vi – Any essential information stored on a laptop or on a PC's local disk must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.	Absent	Absent	Absent
I vii – Sensitive or confidential data should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.	Implicit	Referred 7 **P** 1	Referred 7.1 Explicit 7.1.3
I viii – Utmost care must be used when transporting files on removable media (e.g. disks, CD-ROMs and USB flash drives) to ensure that valid files are not overwritten or incorrect or out of date information is not imported.	Absent	Absent	Absent
I ix – Employees are not permitted to load unapproved software onto the organisation's PCs, laptops and workstations.	Explicit	Explicit 6	Explicit 6.2
K ix – All access to IT services is to be logged and monitored to identify potential misuse of systems or information.	Absent	Explicit 9	Explicit 9.1

Directive	Simplified code	Core regulations	Guidance
L vi – Moves, changes and other reconfigurations of users' network access points will only be carried out by suitably trained and authorised staff and a full record of all changes will be maintained.	Implicit	Explicit 6	Explicit 6.2, 6.3
L ix – Access to the resources on the network must be strictly controlled to prevent unauthorised access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.	Absent	Explicit 3 **P** 2	Explicit 3
N i – Persons accessing information systems remotely to support business activities must be authorised to do so by an appropriate authority within the organisation. A risk assessment based on the criticality of the information asset being used must be carried out.	Absent	Referred 7 **P** 1	Referred 7.1
P ii – Confidential information shall only be taken for use away from the organisation in an encrypted form unless its confidentiality can otherwise be assured.	Implicit	Referred 7 **P** 1	Referred 7.1 Explicit 7.1.2
P iv – The confidentiality of information being transferred on portable media or across networks, must be protected by use of appropriate encryption techniques.	Implicit	Referred 7 **P** 1	Referred 7.1 Explicit 7.1.3
P vii – Important business information being communicated electronically shall be authenticated by the use of digital signatures; information received without a digital signature shall not be relied upon.	Absent	Referred 7 **P** 1	Referred 7.1

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

- Obscene Publications Act 1959 **www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents** and Obscene Publications Act 1964 **www.legislation.gov.uk/ukpga/1964/74**
- Protection of Children Act 1978 **www.legislation.gov.uk/ukpga/1978/37/contents**
- Police and Criminal Evidence Act 1984 **www.legislation.gov.uk/ukpga/1984/60/contents**
- Copyright, Designs and Patents Act 1988 **www.legislation.gov.uk/ukpga/1988/48/contents**
- Criminal Justice and Immigration Act 2008 **www.legislation.gov.uk/ukpga/2008/4/contents**
- Computer Misuse Act 1990 **www.legislation.gov.uk/ukpga/1990/18/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**
- Prevention of Terrorism Act 2005 **www.legislation.gov.uk/ukpga/2005/2/contents**
- Terrorism Act 2006 **www.legislation.gov.uk/ukpga/2006/11/contents**
- Police and Justice Act 2006 **www.legislation.gov.uk/ukpga/2006/48/contents**
- Freedom of Information Act 2000 **www.legislation.gov.uk/ukpga/2000/36/contents**
- Freedom of Information (Scotland) Act 2002 **www.legislation.gov.uk/asp/2002/13/contents**
- Equality Act 2010 **www.legislation.gov.uk/ukpga/2010/15/contents**
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) **www.legislation.gov.uk/uksi/2003/2426/contents/made**
- Defamation Act 1996 **www.legislation.gov.uk/ukpga/1996/31/contents** and Defamation Act 2013 **www.legislation.gov.uk/ukpga/2013/26/contents**

Acknowledgements

The UCISA Model Regulations steering group was led by Richard Murphy, Director, Information Systems Services at the University of Essex (Co-opted Member of the UCISA Executive Committee) in conjunction with Heidi Fraser-Krauss, Head of IT Services at the University of York (UCISA Vice Chair) and Anna Mathews, UCISA Head of Policy and Projects.

We are very grateful for the help received from colleagues across the sector.

Thirty three participants completed a survey on the Model Regulations that UCISA produced in 2007, and on IT regulation more generally. Many survey respondents also kindly provided a copy of their institution's current regulations for Jerry Niman, the project consultant to use in his background research.

In particular, we would like to thank the following individuals who were interviewed as part of the research process and/or who reviewed drafts of the revised Model Regulations before their publication.

Chris Bayliss, IT Security Services Manager, University of Birmingham

Frank Briggs, Head of Service Delivery, Information Services, Royal Holloway, University of London

Stephen Butcher, CEO, Eduserv

Chris Cobb, Chief Operating Officer and University Secretary, University of London and Co-opted Member of the Executive Board of AHUA (the Association of Heads of University Administration)

Andrew Cormack, Chief Regulatory Adviser, Janet

Basem El-Haddadeh, Director, Information, Media and Technology Services, Leeds Metropolitan University

Phil George, Service and Architecture Manager, Sheffield Hallam University

Brian Gilmore, Director, IT Infrastructure, University of Edinburgh

Nikki Green, Business Development Manager, Eduserv

Aline Hayes, Director, Information Systems and Technology, Sheffield Hallam University

Paul Lambert, IT Director, Teesside University

Sara Marsh, Director of Learner Support Services, University of Bradford and Chair of SCONUL (the Society of College, National and University Libraries)

Jason Miles-Campbell, Manager, Jisc Legal

Kay Mills-Hicks, Information Policy Consultant, University of York

Emily- Ann Nash, Student Experience Manager, University of Brighton

Janusz Naks, Information Security Manager, University of Greenwich

Mike Roch, Director, Information Services, Heriot-Watt University

Stephen Town, Director of Information, University of York

Chris Willis, Information Security Manager, University of Sheffield

We would also like to thank the UCISA Executive Committee for their comments and suggestions.