

Guidance Notes on the Regulations for the use of Information Technology

1 Introduction

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 Information Technology [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 4 - Authority, or anyone with authority delegated to them by that person or body.

2 Scope

2.1 Users

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

-) Visitors to the University of Sussex's website, and people accessing the institution's online services from off campus;
-) External partners, contractor and agents based onsite and using the University of Sussex'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.

2.2 IT facilities

The term IT facilities include:

-) IT hardware that the University of Sussex 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 the University of Sussex 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;
-) Online services arranged by the institution, such as Office 365 and Google Apps, JSTOR, or any of the Jisc online resources;
-) Web-based services, email (including role based accounts) and online access to University systems.
-) *IT credentials*, such as the use of your institutional login, or any other token (email address, smartcard, dongle) issued by the University of Sussex 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.

3 Governance

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

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

3.1 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 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](#)
- [Counter Terrorism & Security Act 2015 \(covering PREVENT\)](#)
- [Human Rights Act 1998](#)
- [General Data Protection Regulation](#)
- [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 [2013](#)

The online version of this document has Links to the full text of each Act.

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 <http://www.jisclegal.ac.uk/LegalAreas> .

3.2 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.

3.3 General institutional regulations

You should already be familiar with the University of Sussex's general regulations and policies.

These are available at <http://www.sussex.ac.uk/ogs> .

3.4 Third party regulations

If you use the University of Sussex'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:

) **Using Janet, the IT network that connects all UK higher education and research institutions together and to the internet**

When connecting to any site outside the University of Sussex you will be using Janet, and subject to the Janet Acceptable Use Policy, <https://community.ja.net/library/acceptable-use-policy> the Janet Security Policy, <https://community.ja.net/library/janet-policies/security-policy> and the Janet Eligibility Policy <https://community.ja.net/library/janet-policies/eligibility-policy>

The requirements of these policies have been incorporated into these regulations, so if you abide by these regulations you should not infringe the Janet policies.

) **Using Chest agreements**

Eduserv is an organisation that has negotiated many deals for software and online resources on behalf of the UK higher education community, under the common banner of *Chest agreements*. These agreements have certain restrictions, that may be summarised as: non-academic use is not permitted; copyright must be respected; privileges granted under *Chest agreements* must not be passed on to third parties; and users must accept the User Acknowledgement of Third Party Rights, available at <http://www.eduserv.org.uk/services/Chest-Agreements/about-our-licences/user-obligations>

There will be other instances where the University of Sussex has provided you with a piece of software or a resource. You must only use software and other resources in compliance with all applicable licences, terms and conditions. More information is available on the [IT Services website](#) .

4 Authority

These regulations are issued under the authority of the Information Services Committee, which has delegated responsibility for their interpretation and enforcement to the Director of IT Services, 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 Service Desk](#) .

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

5 Intended use

The University of Sussex'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.

5.1 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.

5.2 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.

5.3 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 the Director of IT Services. The provider of the service may require a fee or a share of the income for this type of use. For more information, contact the [IT Service Desk](#) .

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.

6 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.

6.1 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 the [IT Service 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 / registration card or other security hardware. Take care not to lose them, and if you do, report the matter to the Security Office immediately.

6.2 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).

6.3 Attempt to compromise others' identities

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

7 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.

7.1 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.

7.2 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.

7.3 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.

7.4 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 and network sharing services, or websites.

7.5 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.

7.6 Subverting security measures

The University of Sussex 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.

8 Information

8.1 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 2018 (GDPR) 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 <http://www.sussex.ac.uk/infosec/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 General Data Protection Regulation and how the University of Sussex ensures compliance with it is available at <http://www.sussex.ac.uk/oqs/policies/information/dpa>.

8.1.1 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 <http://www.sussex.ac.uk/infosec/policies>.

8.1.2 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 <http://www.sussex.ac.uk/infosec/policies>.

8.1.3 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 <http://www.sussex.ac.uk/infosec/policies>.

8.1.4 Personal or public devices and cloud services

Even if you are using approved connection methods, devices that are not fully managed by the University of Sussex cannot be guaranteed to be free of malicious software that could, for example, gather keyboard input and screen displays. You should refer to the BYOD policy, available at <http://www.sussex.ac.uk/infosec/documents/BYOD-policy.pdf>

Advice on the use of personal devices to access institutional services is available at <http://www.sussex.ac.uk/its/help/guide?id=60>

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

8.2 *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://guides.lib.sussex.ac.uk/teaching>. 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.

8.3 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 Director of IT Services or the Chief Operating Officer.

Where information has been produced in the course of employment by the University of Sussex, 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. Please see the [Policy for Institutional Access to information within University IT Accounts, Equipment and Networks](#) for more information.

8.4 Inappropriate material

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

The University of Sussex 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

<http://www.sussex.ac.uk/staff/research/spg/research-policy>

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.

8.5 Publishing information

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

8.5.1 Representing the institution

You should follow the University of Sussex's publication guidelines available at <http://www.sussex.ac.uk/publications/> when using the IT facilities to publish information on behalf of the University

8.5.2 Publishing for others

You must not publish information on behalf of third parties using the institution's IT facilities without the approval of the Director of IT Services.

9 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.

9.1 *Conduct online and on social media*

The University of Sussex'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.

9.2 *Spam*

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

<http://www.sussex.ac.uk/pressandcomms/communications/channels/email/bestpractice> .

9.3 *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.

9.4 *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.

9.5 *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.

10 Monitoring

10.1 *Institutional monitoring*

The University of Sussex 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;
-) For certain other prescribed reasons laid out the University's Institutional Access Policy, available at <https://www.sussex.ac.uk/webteam/gateway/file.php?name=institutional-access.pdf&site=370>

The University of Sussex 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

<https://www.sussex.ac.uk/webteam/gateway/file.php?name=institutional-access.pdf&site=370> .

10.2 *Unauthorised monitoring*

You must not attempt to monitor the use of the IT without the explicit permission of The Director of IT Services.

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.

11 Infringement

11.1 *Disciplinary process and sanctions*

Breaches of these regulations will be handled by the University of Sussex's disciplinary processes, defined at

<http://www.sussex.ac.uk/ogs/policies/studentguidance/studentdiscipline> and

<http://www.sussex.ac.uk/humanresources/documents/disciplinaryprocedure.pdf>

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 the University of Sussex as a result of the breach.

11.2 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.

11.3 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.

11.4 Report infringements

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

Ownership:

Owner	Department/Team
Director ITS	ITS

Authors:

Author(s)	Department/Team
Jerry Niman	Consultant

Contributors and Reviewers:

Contributor/Reviewer	Department/Team
Matthew Trump	Information Service Assurance Manager

Revision History:

Version Number	Status D/R/A/I ¹	Date Issued	Reason for Issue	Issued by
0.1	R		Review by ISC	PD
1.0	I	3 March 2015	Approved by ISC	PD
1.1	I	4 April 2016	Inclusion of reference to Counter Terrorism and Security Act 2015 for PREVENT	PD
1.2	I	20 June 2017	Minor amendments	MT
1.2	I	12 Sept 2017	Change Registrar to COO	MT

¹ D = Draft; R= Ready for approval; A = Approved for issue; I = Issued