IT Acceptable Use Policy: Explanatory Notes

Version 2.4, last updated September 2017

These explanatory notes expand on the principles set out in the University's formal IT Acceptable Use Policy. They give examples of specific situations and are intended to help you relate your everyday use of the IT facilities to the dos and don'ts in the formal policy..

Where a list of examples is given, these are just some of the most common instances, and the list is not intended to be exhaustive.

Where the terms similar to Authority, Authorised, Approved or Approval appear, they refer to authority or approval originating from the person or body identified in section 3, Authority or anyone with authority delegated to them by that person or body.

1. Scope

1.1 Users

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

- contributors to the University of Essex's web presence, and people accessing the institution's online services from off campus
- external partners, contractor and agents based on site and using the University of Essex'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 Wi-Fi services
- students and staff from other institutions logging on using eduroam

1.2 IT facilities

The term IT facilities include:

- IT hardware that the University of Essex provides, such as computers, 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 Essex 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 Wi-Fi, connectivity to the internet from University computers
- 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 the University of Essex to identify yourself when using IT facilities. For example, you may be able to use drop-in facilities or Wi-Fi 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 the University's IT Acceptable Use Policy), 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, and to do any of the below would be unlawful:

- 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
- distribute or circulate a terrorist publication or other material that might be a direct or indirect encouragement or inducement to others to the commission, preparation or instigation of acts of terrorism
- 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

Below are some of the laws that explain this:

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Counter-Terrorism and Security Act 2015
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Data Retention and Investigatory Powers Act 2014
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- 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

Further information about the legal aspects of the use of IT is provided by the Jisc, see: https://www.jisc.ac.uk/guides?f[0]=field_project_topics%3A490

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 rules and regulations

The University has formally constituted codes and rules (known as Ordinances) and specific regulations relating to academic and other matters. You are expected to understand and abide by these, and other University polices.

Relevant University policies include:

- Equality and Diversity Policy (http://www.essex.ac.uk/equality/strategy.aspx)
- Fitness to Practise (https://www.essex.ac.uk/hhs/current_students/fitness-to-practise.aspx)
- Freedom of Speech (https://www.essex.ac.uk/about/governance/documents/policies/cop-freedom-of-speech.pdf)
- Guidelines for Dealing with Harassment and Bullying (http://www.essex.ac.uk/equality/harassment/guidelines.aspx)
- Guideline for the Professional Conduct of Staff (http://www.essex.ac.uk/hr/policies/professional-conduct-of-staff.aspx)
- Information Security Policy
- Safeguarding policy (http://www.essex.ac.uk/staff/student_support/safeguarding/default.aspx)
- Whistleblowing policy (http://www.essex.ac.uk/about/governance/documents/policies/policy-whistleblowing.pdf)

2.4 Third party regulations

If you use the University of Essex's IT facilities to access third party services or resources you are bound by the regulations associated with that service or resource (the association can be through something as simple as using your 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 Essex you will be using Janet, and subject to the Janet Acceptable Use Policy, https://community.jisc.ac.uk/library/acceptable-

use-policy the Janet Security Policy, https://community.jisc.ac.uk/library/janet-policies/security-policy and the Janet Eligibility Policy https://community.jisc.ac.uk/library/janet-policies/eligibility-policy. The requirements of these policies have been incorporated into these regulations, so if you abide by these regulations you should not infringe the Janet policies.

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

3. Authority

These guidelines are issued under the authority of the Director of IT Services 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 a University web site; a self-service kiosk in a public area; or an open Wi-Fi 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 Helpdesk.

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

4. Intended use

The University of Essex'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 and resources 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 these.

4.2 Personal use

You may currently use the IT facilities for personal use provided that it does not breach these, or any other University guidelines, and that it does not prevent or interfere with other people using the facilities for valid purposes (for example using a computer 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 and resources for non-institutional commercial purposes or for personal gain, such as running a club or society (other than through the Students Union Societies Guild), requires the explicit approval of the Director of IT Services. For more information contact the IT Helpdesk. Even with such approval, the use of licences under the Chest and other 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 and some personalise the information provided.

This is most commonly done by providing you with a username and password, but occasionally other forms of IT credentials may be used, such as an email address, a smart card or some other form of security device.

It is important that you do not share your IT credentials with anyone. IT credentials provide easy access for identity theft and fraud.

IT Services will never ask you for your password and any email inviting or directing you to divulge your password should be treated as spam and deleted.

5.1 Protect identity

You must take all reasonable precautions to safeguard any IT credentials issued to you. Your IT credentials are your online identity and if someone else has them it could cause you loss of reputation, money and have a significant impact on your future.

You must change passwords when first issued and at regular intervals as instructed. Do not record passwords 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 Helpdesk.

Do not use your username and password to log in to web sites or services you do not recognise, and do not log in to web sites that are not showing the padlock symbol in the address bar.

Do not leave logged in computers unattended, and log out properly when you are finished.

Don’t allow anyone else to use your campus/ registration card. Take care not to lose it, and if you do, report it as soon as possible and obtain a replacement.

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.

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 (equipment, cables, software) that makes IT function. It includes servers, the network, computers, 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 IT infrastructure.

6.1 Physical damage or risk of damage

Do not damage, or do anything to risk physically damaging the IT infrastructure, such as being careless with food or drink at a computer, or playing football in a drop-in facility.

6.2 Reconfiguration

Do not attempt to change the setup of the IT infrastructure without authorisation, such as changing the network point that a computer is plugged in to, connecting devices to the network (except of course for Wi-Fi or Ethernet networks specifically provided for this purpose) or altering the configuration of the University's computers. Unless you have been authorised, you must not add software to or remove software from computers.

Do not move IT equipment without authority.

6.3 Network extension

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

6.4 Setting up servers

You must not set up any hardware or software that would provide a service to others over the network without permission. Examples would include games servers, file sharing services, IRC servers or web sites.

6.5 Introducing malware

You must take all reasonable steps to avoid introducing malware to the infrastructure.

The term malware covers many things such as viruses, worms and Trojans, but is basically any software used to disrupt computer operation or subvert security. It is usually spread by visiting websites of a dubious nature, downloading files from untrusted sources, opening email attachments from people you do not know or inserting media that have been created on compromised computers. If you avoid these types of behaviour, keep your anti-virus software up to date and switched on, and run scans of your computer on a regular basis, you should not fall foul of this problem.

6.6 Subverting security measures

The University of Essex has taken measures to safeguard the security of its IT infrastructure, including things such as anti-virus software, firewalls, spam filters and so on. You must not attempt to subvert or circumvent these measures in any way.

7. Information

7.1 Personal, sensitive and confidential information

During the course of their work or studies, staff and students (particularly research students) may handle information that comes under the Data Protection Act 1998, or is sensitive or confidential in some other way. For the rest of this section, these will be grouped together as protected information. Safeguarding the security of protected information is a highly complex issue, with organisational, technical and human aspects. The institution has policies on Data Protection http://www.essex.ac.uk/records_management/policies/data_protection_policy.aspx, and Information Security and if your role is likely to involve handling protected information, you must make yourself familiar with and abide by these policies.

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 can be requested from the IT Helpdesk.

7.1.2 Removable media and mobile devices

Protected information must not be stored on removable media (such as USB storage devices, removable hard drives, CDs, DVDs) or mobile devices (laptops, tablet or smart phones) unless it is encrypted, and the encryption key kept securely.

If protected information is sent using removable media, you must use a secure, tracked service so that you know it has arrived safely.

7.1.3 Remote working

If you access protected information from off campus, you must make sure you are using an approved connection method that ensures that the information cannot be intercepted between the device you are using and the source of the secure service.

You must also be careful to avoid working in public locations where your screen can be seen.

7.1.4 Personal or public devices and cloud services

Even if you are using approved connection methods, devices that are not fully managed by the University of Essex cannot be guaranteed to be free of malicious software that could, for example, gather keyboard input and screen displays. You should not use such devices to access, transmit or store protected information.

Do not store protected information in personal cloud services such as Dropbox. Use University provided storage, for example OneDrive.

7.2 Copyright information

Most 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. 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 clearly belonging to other people without their permission, unless it is obvious that they intend others to do this, for example, by releasing material under Creative Commons licences

https://creativecommons.org/licenses/. It is important to be able to distinguish between information that is deliberately and accidently or illicitly made available.

Where information has been produced in the course of employment by the University of Essex, 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. The lack of availability should be unforeseen and ongoing. Permission is unlikely to be granted to cover planned absence such as annual leave or short term absence. 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.

7.4 Inappropriate material

The University of Essex encourages independent thinkers who have the confidence to challenge, and to ask difficult questions. It is fully committed to promoting an environment in which intense inquiry and informed argument generate lasting ideas and where members of its community have a responsibility both to challenge and listen fully.

However, the rights to academic freedom and freedom of speech are not absolute. You must not create, download, store or transmit unlawful material, or material that is grossly offensive, that is indecent, obscene or of a menacing nature, or extremist material that risks drawing people into terrorism.

Where you may need to do so for properly constituted educational or research purposes, you must obtain authorisation from the Director of IT Services in advance, and where required ethical approval.

Advice is available about accessing and storing sensitive materials.

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 web sites, social networks and news feeds. Whilst the University of Essex generally encourages publication, you must not make statements that purport to represent the University of Essex unless you are authorised to do so by your role, a work assignment, or given explicit approval.

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, as is any extremist behaviour that risks drawing people into terrorism. You should not use IT for items that are grossly offensive, or that are indecent, obscene or of a menacing nature.

8.1 Conduct online and on social media

The University of Essex's policies concerning staff and students also apply to the use of social media. These include human resource policies, codes of conduct, acceptable use of IT and disciplinary procedures.

8.2 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 academic work to do. Similarly, do not occupy specialist facilities unnecessarily if someone else needs them.

8.3 Disturbing others

If you cause disturbance, you should expect to be asked to stop. When using shared spaces, remember that others have a right to work without undue disturbance. Keep noise down (turn phones to silent if you are in a silent study area), do not obstruct passageways and be sensitive to what others around you might find offensive.

If you notice someone accessing material that causes you concern, either for their safety and wellbeing, or for that of others, contact the IT Helpdesk or Student Support.

8.4 Excessive consumption of resources

Use resources wisely. Don't consume excessive network bandwidth by uploading or downloading more material (particularly video) than is necessary. Do not waste paper and energy by printing more than is needed. Don't waste electricity by leaving equipment needlessly switched on.

9. Monitoring

9.1 Institutional monitoring

The University of Essex 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

The University of Essex will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime, and ensuring national security.

9.2 Unauthorised monitoring

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

- monitoring of network traffic
- network and/or device discovery
- Wi-Fi 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 must be made, and you should contact your course leader / research supervisor for more information.

10. Concern about use

The internet reflects the diversity of the world. Some of the materials you may access through University IT facilities you may consider to be illegal, upsetting, or morally or ethically offensive. Accepting the rights to academic freedom and to free speech, if you are concerned about the safety and wellbeing of yourself or others, linked to use of the internet, you may contact the IT Helpdesk or Student Support.

11. Infringement

11.1 Disciplinary process and sanctions

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

This could have a bearing on your future studies or employment with the institution and beyond.

Sanctions may be imposed if the disciplinary process finds that you have breached the regulations.

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 law 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.

Contact details for the IT Helpdesk

- Open Monday to Thursday 8.30am-6.00pm, Friday 8.30am-5.45pm
- Email: it.helpdesk@essex.ac.uk
- Telephone: +44 (0)1206 87 2345
- Location: ground floor of the Silberrad Student Centre, Colchester Campus

About this document

The IT Acceptable Use Policy and the explanatory notes have been prepared by the Director of IT Services and the Information Assurance Manager, endorsed by the ICT Steering Group, and approved by the Registrar and Secretary.

Last updated September 2017