University of Essex

IT Acceptable Use Policy

Guidance

Authors:	Digital Innovation and Technology Services
Publication date:	May 2024
Amended:	March 2024
Review date:	March 2025

Table of Contents

IT Acceptable Use Policy: guidance

These notes are to clarify points in the University of Essex IT Acceptable Use Policy and give examples of activities that would and would not be advised.

This is not meant to be an exhaustive list of what is and isn't authorised so if you have any doubts, please email heldpesk@essex.ac.uk to ask for clarification.

Scope

Users

This policy applies 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:

- external partners, contractors and agents based on site and using the University of Essex's network, or offsite and accessing the University systems
- tenants of the institution using the University's computers, servers or network
- students and staff from other institutions logging on using eduroam
- members of organisations linked with the University

IT facilities

The following list is not exhaustive – if you are unsure if a particular thing constitutes an IT facility it probably is, clarification can be asked from helpdesk@essex.ac.uk.

- IT hardware that the University of Essex provides, such as computers, laptops, tablets, printers, smart and soft phones.
- software that the institution provides, such as operating systems and apps.
- 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, eduroam or accessing the internet from University computers.
- 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.
- using your Essex account at other institutions – e.g. Eduroam.

Governance

It is helpful to remember that using IT has consequences in the real world as well as the digital one.

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.

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 although this list is not exhaustive, to do any of the below would be unlawful:

- create or transmit, or cause the transmission, of any images, data or other material that would be legally obscene or indecent
- 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 defraud or would violate common law on confidentiality or privacy
- 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:

Computer Misuse Act 1990

Copyright, Designs and Patents Act 1988

Data Protection Act 2018

Obscene Publications Act 1959 and 1964

Police and Criminal Evidence Act 1984

Counter-Terrorism and Security Act 2015

Criminal Justice and Immigration Act 2008

Data Retention and Investigatory Powers Act 2014

Human Rights Act 1998

Regulation of Investigatory Powers Act 2000

Terrorism Act 2006

Police and Justice Act 2006

Protection from Harassment Act 1997

Protection of Children Act 1978

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

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.

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 when using IT facilities as well as more generally.

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. Very often, these regulations will be presented to you the first time you use the service, but in some cases you may hardly be aware. If you break their rules using our IT Facilities, we may legally be asked and obliged to provide evidence.

Authority

These guidelines are issued under the authority of the Chief Information Officer 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 such as a University web site; a self-service kiosk in a public areas

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.

Intended use

The University of Essex's IT facilities are provided to support the mission and goals of the University of Essex - excellence in education and research, for the benefit of individuals, communities and society

Personal use

You may currently use the IT facilities for reasonable personal use, provided that such use does not breach these, or any other University guidelines, and that it does not prevent or interfere with other people using the facilities for their purposes.

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.

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 University of Essex Students Union), requires the explicit approval of the Chief Information Officer. For more information contact the IT Helpdesk.

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 them 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 reported to spamreport@essex.ac.uk.

Protect identity

You must take all reasonable precautions to safeguard your IT credentials. These are the keys to your online identity and if someone else has them it could have negative consequences for you and for the University.

You must change passwords when first issued and when asked. 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.

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.

Impersonation

Never use someone else’s IT credentials or attempt to disguise or hide your real identity when using the institution’s IT facilities.

Attempt to compromise others’ identities

Do not interfere with other people’s identities.

Infrastructure

The IT infrastructure is all the underlying stuff (equipment, cables, software) that makes IT work. 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.

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.

IT configuration

Only authorised changes to IT infrastructure can be made. You must not alter wired network connections, remove software or add unapproved software, and you must not move static IT equipment.

Network extension

You must not extend the University's wired or Wi-Fi network without authorisation, which may involve the use of routers, repeaters, hubs or Wi-Fi access points.

Setting up servers

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

Introducing malware

You must take all reasonable steps to avoid introducing malware to the infrastructure The term malware covers many things such as viruses and Trojans, and covers any software used to disrupt IT facilities. Ensure your software, operating system, apps and anti-virus software is up to date on all your devices.

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.

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, access, download, store or transmit unlawful material, for example material that is legally indecent, obscene, harassing or extremist material that risks drawing people into terrorism.

Where you may need to access such materials for properly constituted educational or research purposes, you must obtain authorisation from the Chief Information Officer in advance, and where required, have secured the appropriate 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.

Behaviour

The way you behave when using IT should be no different to how you would behave under other circumstances. Abusive 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 legally indecent, obscene or otherwise unlawful.

Denying others access

If you are using shared IT facilities for reasonable 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.

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.

Monitoring

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; for monitoring the effective function of the facilities; and for
- 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.

Unauthorised monitoring

You must not attempt to monitor the use of the University’s IT facilities without the explicit permission of the Chief Information Officer. 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
- attempting to capture or clone details of RFID cards, or any other form of wireless access control

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.

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 upsetting, or morally or ethically offensive to you. Should you require support in relation to any materials linked to use of the internet, you may contact the IT Helpdesk or Student Support.

Infringement

Disciplinary process and sanctions

Breaches of these regulations will be handled under the University of Essex's disciplinary processes. This could have a bearing on your future studies or employment with the institution. Sanctions may be imposed if the disciplinary process finds that you have breached the regulations. If you are not a member of the University, the matter will be raised with the person or organisation that requested access to University IT Facilities for you.

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.

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.

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

Document Control Panel

Field	Description
Title	**IT Acceptable Use Policy: guidance**
Policy Classification	Guidelines,
Security Classification	Restricted to Staff and Students
Security Rationale	Guidance only relevant to members of staff and students
Policy Manager Role	Chief Information Officer
Nominated Contact	helpdesk@essex.ac.uk
Responsible UoE Section	Digital Innovation and Technology Services
Approval Body	USG
Signed Off Date	23 April 2024
Publication Status	Published
Published Date	May 2024
Last Review Date	April 2024
Minimum Review Frequency	Annually
Review Date	23 April 2025
UoE Identifier	0177

If you require this document in an alternative format, such as braille, please contact the nominated contact at helpdesk@essex.ac.uk