IT Regulations overview

Who needs to read and adhere to these regulations

They apply to you whenever you use a University of Kent IT service or facility. They are therefore relevant to anyone with a Kent IT Account, plus anyone using an IT facility provided or arranged by the University of Kent.

What we expect from you

Follow these principles and you should never be in breach of the full IT Regulations:

Know the rules

- Abide by all University of Kent regulations and policies.
- Observe the regulations of any third parties whose facilities you access.
- Don’t break the law.

Be yourself

- Always keep your Kent IT Account to yourself, never reveal your password.
- Use your own identity online, don’t pretend to be someone else.
- Always use your own account, never anyone else’s.

Use facilities appropriately

- Don’t do anything that would put IT facilities at risk of malware.
- Don’t interfere with hardware or load unauthorised software on University machines.

Use information responsibly

- Safeguard your personal data.
- Respect other people’s information.
- Don’t abuse copyright material.
- Mobile devices may not be a secure way to handle information.

Behave respectfully

- Don’t waste IT resources or interfere with others’ legitimate use.

- Don’t behave towards others in a way that isn’t acceptable in the physical world.

Full IT Regulations

1. The regulations apply to all users of the University of Kent’s IT facilities

Users could be students staff or visitors who may or may not have a Kent IT Account, plus anyone using any IT facility provided or arranged by the University.

Facilities include:

- hardware such as PCs, smartphones, printers, etc
- software
- data
- network access including Wi-Fi
- email including alumni email
- our website
- online services arranged by the University (for example Office 365 or Library online resources such as JSTOR)
- third party services, etc

2. The law

Your behaviour is subject to the UK law and, if you are accessing service from outside the UK, the law of the land you are in. This includes laws on fraud, theft and harassment.

Ignorance of the law is not an adequate defence. Breach of the law or a relevant third party regulation is also a breach of these IT regulations.

For example, you may not:

- view, 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;

    - material with the intent to defraud;
    - defamatory material;
    - material such that this infringes the copyright of another person or organisation;
    - unsolicited bulk or marketing material to users of networked facilities or services, unless it is part of a service that the user or their organisation has subscribed to;
- deliberately access networked facilities or services that you don't have permission to use (ie, without authorisation).

You are bound by all other University of Kent regulations, policies and procedures when using the IT facilities, including but not limited to:

- University Regulations
- Information Security Policy (pdf)
- Use of the Kent Network (pdf)
- Use of your own computer/mobile device (pdf)
- Use of a University mobile device (pdf)
- IT Security Policy (pdf)
- Privileged user charter (pdf)
- Staff access to key corporate applications policy (pdf)
- Security procedures for system administrators (pdf)
- Blogs conditions of use

If you use our IT facilities and/or your Kent IT Account details to access third party services or resources you are bound the third party's regulations too. Sometimes you may not realise that you are using a third party service.

JANET are the organisation that provide the eduroam service (our Wi-Fi network) and our wired internet. The requirements of these policies have been incorporated into our IT regulations, so if you abide by these regulations you should not infringe the Janet Acceptable Use Policy, Janet Security Policy or the Janet Eligibility Policy.

Software and online resources:

- 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.

Laws that are particularly relevant to the use of IT include:

- 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
- Human Rights Act 1998
- Data Protection Act 2018
- General Data Protection Regulation 2018
- 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 University of Kent has a statutory duty, under the Counter Terrorism and Security Act 2015, termed “PREVENT”. The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

When using services hosted outside the UK you may also be subject to the law in the host country.

JISC, who provide IT services to the education sector, have excellent legal guides to IT usage in education.

3. Authority

These regulations are issued by the Director of Information Services, who is responsible for their interpretation and enforcement, and who may delegate responsibilities to others.

You are using IT facilities with permission if you:

- have a Kent IT Account with appropriate access to relevant systems and services
- have been given access rights to a specific system or resource
- use open access facilities in an obviously open access setting, such as:
    - a University of Kent website;
    - a self-service kiosk in a public area;
    - or an open WiFi network on campus.

If you are not sure whether you have the authority to use an IT facility, contact us for advice.

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

You must comply with any reasonable request (written or verbal) issued by staff with the relevant authority. If you feel that any requests are unreasonable or are not in support of these regulations, please refer to the computer misuse/abuse procedures.

4. How you should use IT facilities

University facilities are funded by students and the tax-paying public. They have a right to know that the facilities are being used for the purposes for which they are intended.

IT facilities are there to further the University's mission, for example to support a course of study, research or to help staff do their jobs. 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.

You can use facilities for personal use, as long as you don't infringe any of the regulations, and don't interfere with anyone else's valid use. This privilege can be withdrawn. Staff using IT facilities for non-work purposes during working hours are subject to the same management policies as for any non-work activity.

If you make personal use of the IT facilities please note that in certain circumstances the University may take reasonable and proportionate steps to lawfully retrieve or access information relating to University business that is held in University systems, including email accounts.

The University has a procedure to regulate when and how requests for information will be granted including the steps that the University should take to minimise any intrusion into a user's privacy.

If you want to use the IT facilities for non-institutional commercial purposes or for personal gain, such as running a club or society, you need explicit permission from the Director of Information Services.

Software paid for and provided by the University is for academic use only and where applicable must adhere to the CHEST 'User Acknowledgement of Third Party Rights'.

Even with permission to conduct personal activity for commercial or personal gain, the use of licences under the Chest agreements for anything other than teaching, studying or research, administration or management purposes is prohibited. You must make sure that licences allowing commercial use are in place. The provider of the service may require a fee or a share of the income for this type of use.

More information on software licensing at Kent.

5. Identity

You must protect your Kent IT Account username and password, email address, KentOne card and any other identity documents, hardware or passwords you have. Do not allow anyone else to use your IT Account. Nobody has the authority to ask you for your password, and you must not disclose it to anyone.

Your IT Account details

- Don't use obvious passwords.
- Don't record passwords anywhere that someone else could find them.
- Don't use the same password at Kent and for personal (ie non-institutional) accounts.
- Don't share passwords with anyone else, even IT staff (even if it seems convenient and harmless).
- If you think someone else knows your password, change it immediately and report it to helpdesk@kent.ac.uk
- Don't use your username and password to log in to websites or services you don't recognise.
- Don't log in to websites that are not showing the padlock symbol.
- Don't leave logged in computers unattended. Log out properly when you are finished.

- Don’t allow anyone else to use your KentOne card or other security hardware.
- Take care not to lose your KentOne card, and if you do, report this at www.kent.ac.uk/kentonecard immediately.
- Do not try to find out or use anyone else’s credentials. Don’t impersonate someone else or try to disguise your identity when using the IT facilities. You must not attempt to usurp, borrow, corrupt or destroy someone else’s IT credentials.

It is only acceptable to remain anonymous if the service you’re using clearly allows anonymous use (such as a public facing website).

6. Respect the 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.

6.1. Don’t do anything to jeopardise the infrastructure

Don’t damage, or do anything to risk physically damaging the infrastructure. This includes being careless with food or drink, or acting inappropriately in a way that could cause accidental damage.

Do not attempt to change the setup of the infrastructure without authorisation. For example:

- don’t change the network point that a PC is plugged in to
- don’t connect a device to an unauthorised network point (unless of course for WiFi or Ethernet networks specifically provided for this purpose).
- don’t alter the configuration of University PCs, laptops etc.
- unless you have been authorised, you must not add software to or remove software from PCs or other devices.
- don’t move equipment without authority.

6.2. No Wi-Fi routers, hubs, hotspots etc

You must not extend the Wi-Fi or wired network without authorization. Such activity, which could involve using routers, repeaters, hubs or Wi-Fi access points, can disrupt the network.

6.3. No unauthorised servers

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

6.4. Protect against malware

You must avoid these types of behaviour that increase the risk of spreading malware (ie viruses, worms and Trojans: software designed to disrupt or subvert security).

Malware is usually spread by:

- visiting websites of a dubious nature
- downloading files from untrusted sources
- clicking links in emails that could be fraudulent
- opening email attachments from people you do not know
- or inserting media that have been created on compromised computers.

Follow our advice and take all reasonable steps to avoid introducing malware to the infrastructure.

7. Information

If you handle personal, confidential or sensitive information (described in the rest of this section as 'protected information') you must take all reasonable steps to safeguard it.

You must observe the University of Kent's Data Protection and Information Security (pdf) policies and guidance. This is vital, especially if you use removable media, mobile and privately owned devices.

You must abide by the University of Kent's Best Practice guidance on communications when using the IT facilities to publish information.

7.1 Protected information

7.1.1. Sending protected information

When sending protected information electronically, you must use a method with appropriate security.

More information on sending protect information electronically at Kent.

7.1.2. Removable media and portable devices including

laptops

Do not store protected information on removable media (such as USB storage devices, removable hard drives, CDs, DVDs) or mobile devices (laptops, tablet, smart phones, or portable mini-pc for hybrid working) 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. See advice on the use of removable media and mobile devices for protected information.

7.1.3. Working and studying off campus

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

Do not work in public locations where your screen can be seen. See advice on working remotely with protected information.

7.1.4. Personal or public devices and cloud services

Devices that are not fully managed by the University of Kent cannot be guaranteed to be free of malicious software that could, for example, gather keyboard input and screen displays. Don’t use such devices to access, transmit or store protected information (even if the transmission method would be secure, the device itself may not be).

See advice on the use of personal devices to access University of Kent services (pdf).

When doing University work, use storage services supported by the University with appropriate encryption and security. Do not store protected information in personal cloud services such as Dropbox unless securely encrypted first.

7.2. Copyright information

Don’t infringe copyright, or break the terms of licences for software or other material. Just because you can see something on the web, download it or otherwise access it doesn’t mean you can do what you want with it.

Almost all published works are protected by copyright. If you are going to use material (images, text, music, software), it is on you to make sure that you use it within copyright law. This is a complex area: see copyright training and guidance.

7.3. Others' information

Don’t attempt to access, delete, modify or disclose information belonging to other people without their permission, unless it is obvious that they intend others to do this, or you have explicit approval from your Head of School or Head of Department.

If information has been produced for the University, 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. For more information, see our Information Compliance guidance.

7.4. Inappropriate material

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

We have procedures to approve and manage valid activities involving such material for valid research purposes, where legal, with the appropriate ethical approval. If you have valid reasons to work with such material, you must follow these procedures to approve and manage your activity.

Universities UK has produced guidance on handling sensitive research materials.

There is an exemption covering authorised IT staff involved in preserving evidence for investigating breaches of the regulations or the law.

7.5. Publishing information

- Publishing is the act of making information available to the general public, such as through websites, social networks and news feeds.
- Do not make statements that purport to represent the University of Kent without the approval of your Head of School or Head of Department.
- Do not publish information on behalf of third parties using the institution’s IT facilities without the approval of your Head of School or Head of Department. See more information on communications.

8. Behaviour

Real world standards of behaviour apply online and on social networking platforms. Abusive, inconsiderate or discriminatory behaviour is unacceptable.

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

- Do not cause needless offence, concern or annoyance to others.
- Do not act in a way that could be described as harassment or bullying as defined by the University's Dignity at Work Policy
- Follow the University of Kent's guidelines on using social media. https://www.kent.ac.uk/socialmedia/.
- Don't send spam (unsolicited bulk email) unless in specific circumstances.
- Don't deliberately or recklessly use excessive IT resources such as processing power, storage, bandwidth, printer paper etc. Do not waste paper by printing more than is needed: print double-sided is possible.
- Don't waste electricity by leaving equipment needlessly switched on.
- If using shared IT facilities for personal or social purposes, you should vacate them if they are needed by others with work to do.
- Don't use specialist facilities unnecessarily if someone else needs them.
- Don't use the IT facilities in a way that interferes with others' valid use of them.
- Others have a right work without undue disturbance:
    - keep noise down (turn 'phones to silent if in a silent study area)
    - do not obstruct passageways
    - be sensitive to what others around you might find offensive.

9. Monitoring

The University of Kent monitors and records the use of its IT facilities for the purposes of:

- effective and efficient planning and operation of the IT facilities;
- detecting and preventing infringement of these regulations;
- investigating alleged misconduct;
- monitoring how well facilities are working.

The University doesn't routinely monitor individual users' use of IT facilities and services. You must not attempt to monitor the use of IT without the explicit permission of the Director of Information Services. The University has a procedure that regulates when and how monitoring is permitted, which includes

- how we ensure compliance with GDPR,

- The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018,
- and any other relevant legislation.

Monitoring would include:

- monitoring 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;

Where IT is itself the subject of study or research, special arrangements will have been made. Contact your course leader, research supervisor or Head of School for more information.

In certain circumstances the University may be obliged to disclose information or undertake more detailed monitoring under the Regulation of Investigatory Powers Act 2000.

10. Infringement

If you breach these regulations you may be sanctioned under the institution's disciplinary processes. Penalties may include withdrawal of services and/or fines. Offending material will be taken down.

If we believe that unlawful activity has taken place, we will refer the matter to the police or other enforcement agency including any other organisations whose regulations you have breached.

The University of Kent has the right to recover from you any costs incurred as a result of your infringement.

Breaches of these regulations could have a bearing on your future studies or employment with the institution and beyond. If you are unsure about any of these regulations you should check before carrying out any activity that might infringe them.

You must inform helpdesk@kent.ac.uk if you become aware of any infringement of these regulations.

Document review date

This policy will be reviewed annually by Information Services Senior Management Team.

Policy created: June 2019

Policy reviewed: March 2021