Anglia Ruskin University

Cambridge Chelmsford Peterborough

Regulations for the use of our IT resources, systems and services

January 2016

Introduction

Our Information Technology (IT) resources, systems and services are essential to the day-to-day operation of our University. We have designed this document to provide you with brief and easily comprehensible information relating to the acceptable use of our IT facilities.

For simplicity, the document is divided into three complementary parts:

1. A simplified summary that lists the essentials with which all our students, staff and other users should be familiar;
2. A set of ten core principles of acceptable use that will remain stable as technology and legislation change;
3. A suite of related guidance and examples that include some, but not all, of the specific activities that we regard as unacceptable or inappropriate.

Part One and Part Three are exempted from our formal approval process so that we can revise them, when required, in order to maintain currency or to highlight specific issues to you. Our IT Services Directors' Team manages them.

Part Two is subject to regular review and approval by our Corporate Management Team.

We have designed this document to work with, rather than supersede, our existing regulations, policies and guidance as well as those of our partners and suppliers and current UK and international law, to which we will refer but not reiterate or summarise.

Part One: Acceptable Use, Summary

This is a short summary of governance and expected behaviour related to the acceptable use of our IT resources, systems and services, which we will collectively refer to as **facilities**. You are also expected to be familiar with the detail of our ten core principles of acceptable use, which are outlined on pages 5-8 of this document and at http://web.anglia.ac.uk/it/policy/it_acceptable_use_2016.pdf

Behaviour

- Do not waste IT resources or interfere with others' legitimate use;
- Do not behave towards others in a way that would be unacceptable in the physical world;
- Do not assume that because an action is possible, it is by implication, acceptable or permitted.

[core principles | guidance]

Governance

- Abide by all of our policies and regulations;
- Follow all of our guidance;
- Observe the policies, regulations and guidance of any third party whose facilities or resources you access unless they contradict our own;
- Do not break local or international law.

[core principles | guidance]

Identity

- Do not allow anyone else to use your IT credentials;
- Do not disguise your online identity;
- Do not attempt to obtain or use credentials or identity details belonging to anyone else.

[core principles | guidance]

Information

- Safeguard your personal data;
- Respect other people's information;
- Do not abuse copyright material;
- Remember that mobile devices are not always the most appropriate or secure way to store or handle information;
- If in doubt, do not use hold our data locally on a personal mobile device.

[core principles | guidance]

Infrastructure

- Do not put our IT facilities at risk by introducing malware, interfering with hardware or loading unauthorised software.

[core principles | guidance]

Part Two: Acceptable Use, Core Principles

We have established ten core principles of acceptable use to ensure that our Information Technology (IT) resources, systems and services, collectively referred to as our IT facilities, are used lawfully, safely and equitably.

The issues covered by our core principles are complex. We strongly urge you to read our extended guidance, to be found on page 9-18 of this document and at http://web.anglia.ac.uk/it/policy/it_acceptable_use_2016.pdf, which will provide more detailed supporting information that we hope you will find useful.

1. Scope

Anyone using hardware, software, data, networks, online services, third-party services or IT credentials such as username(s), password(s), email address(es) or other identity-related hardware or information provided by, or arranged by, our University must adhere to our regulations and the ten core principles of acceptable use for our IT facilities.

[guidance]

2. Governance

While using any of our IT facilities and resources, you remain subject to all of the same laws and regulations that apply in the physical world.

You must always ensure that your conduct is in accordance with the laws of the United Kingdom. Ignorance of an aspect of the law is an inadequate defence for misconduct.

You are bound by all of our internal regulations, policies and guidance while using our IT facilities.

When accessing our IT facilities from a location that falls under another jurisdiction, you must abide by all relevant local laws, as well as those applicable to our location.

When accessing a service via eduroam, the educational roaming wireless network service, you are subject to our regulations and those of the institution providing your eduroam access as well as those of any intermediate service provider.

You must abide by any regulations applicable to another organisation whose services you access, such as Joint Academic Network (Janet), Eduserv and the Joint Information Systems Council (JISC) Collections.

Some of our software licences will include obligations to which you must strictly adhere. If you use any software or resources covered by a Combined Higher Education Software Team (CHEST) agreement, you are deemed to have accepted the Eduserv User Acknowledgement of Third Party Rights, (http://arul.ink/chest-uo).

A breach of any applicable law or third party regulation will be regarded as a breach of our student regulations or your contract of employment, as applicable.

[summary | guidance]

3. Authority

Our core principles of acceptable use are issued with the approval of our University's Corporate Management Team (CMT). Responsibility for day-to-day interpretation and application is delegated to our IT Services Directors' Team and Head of Infrastructure, who will consult with other internal and external concerned parties, as appropriate.

You must not use our IT facilities without permission. Consent may be associated with your status as a registered student, an employee of our University or another authorised user. Consent may also be inferred through the use of a specific service such as eduroam.

You must comply with any reasonable verbal or written instructions in support of our core principles of acceptable use when issued by a delegated authority.

Use of our IT facilities and resources is a privilege not a right. We may withdraw your access to them temporarily, while investigating possible misuse, or permanently as a consequence of such an investigation and any resultant disciplinary action.

[guidance]

4 Intended Use

Our IT facilities are provided for use in support of your course of study, research, employment or other approved activities that are associated with the aims and objectives of our University.

Some licences are granted for academic use only and may be governed by the codes of conduct published by CHEST (http://arul.ink/chest), JISC (http://arul.ink/jisc) or another provider or authority. You must adhere to these agreements at all times.

You may use our facilities for a limited amount of personal activity, provided that it does not compromise your studies, research or work, infringe any of our regulations or interfere with valid use of others.

You must not use our IT facilities for unapproved commercial purposes or for personal gain.

[guidance]

5. Identity

You must take all reasonable precautions to safeguard any IT credentials that are issued to you, including username(s), password(s), email address(es), smart card(s) and other identity-related hardware or information. You must not allow anyone else to use your IT credentials.

Nobody has authority to ask for your password and you must not disclose it to anyone under any circumstances. We will never ask you to validate information such as IT credentials, to confirm account details or to reactive/extend services either by email reply or by visiting an off-site webpage or other service.

You must not attempt to obtain or use anyone else's IT credentials, even in circumstances where permission is implied.

You must not impersonate someone else or otherwise disguise your identity when using our IT facilities.

[summary | guidance]

6. Infrastructure

You must not engage in any activity that has the potential to jeopardise the integrity of our IT infrastructure, such as:

- Damaging our equipment;
- Reconfiguring or moving our equipment without prior approval;
- Loading software on our equipment, other than in approved circumstances;
- Connecting equipment to our network other than by approved methods and in appropriate circumstances;
- Setting up servers or services on our network without prior approval;
- Deliberately or recklessly introducing malware;
- Attempting to disrupt or circumvent IT security measures.

[summary | guidance]

7. Information

You must adhere to our Data Protection and Information Security policies, which are available, along with guidance, at http://arul.ink/DPAandIS.

You must take all reasonable steps to safeguard and secure any personal, confidential or sensitive information to which you may have access as part of your studies or work. You should give particular consideration to any output sent to a printer as well as to the security of portable or personal equipment such laptops, tablet devices and smartphones.

You must not store personal, confidential or sensitive information on third-party storage such as cloud-based device backup services, since we cannot guarantee their quality or security.

We retain ownership of any information downloaded from our systems to a mobile device and reserve the right to delete it, without notice, where it is appropriate to do so. In such circumstances we can offer no guarantee to preserve any other information on the device.

Portable media, such as USB storage devices, removable hard drives, CDs or DVDs, that are used to hold personal, confidential or sensitive data must be securely stored on-premises and appropriately encrypted if used off-premises.

Mobile devices including laptops, tablets and smart phones must be password or Personal Identification Number (PIN) protected and, where appropriate, encrypted.

Encryption key(s) must be securely stored in a manner that will not hamper legitimate investigations by a legal authority.

If in doubt, do not remove personal, confidential or sensitive information from our premises or access it using a medium that cannot be adequately secured.

You must not create, download, store or transmit unlawful material or material that is indecent, can cause offense, be threatening or discriminatory. We have policies to approve and manage valid academic research related to such material available from http://arul.ink/ethicspolicy. You must gain appropriate authorisation, as described in this document, before accessing any prescribed information and must notify our IT Services of your intention to do so.

You must not attempt to access, delete, modify or disclose information that belongs to other people without their permission.

You must not infringe copyright, or break the terms of licences for software or other material.

[summary | guidance]

8. Behaviour

You must behave in reasonable and appropriate manner at all times while online and when using any social networking platform, including Facebook, Twitter, Google+ and Blogger.

You must not cause needless offence, concern or annoyance to others and abide by our Dignity at Work and Study policy, available from http://arul.ink/dignity, at all times.

You must not distribute information electronically or in print that might adversely affect our reputation or that of others.

You must not send unsolicited bulk email, commonly known as spam.

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

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

[summary | guidance]

9. Monitoring

We reserve the right to monitor and record your use of our IT facilities for the purposes of:

- Effective and efficient planning and operation of our services;
- Detection and prevention of any unacceptable use of our facilities;
- Investigation of any alleged misconduct.

We will comply with all lawful requests for information from local, national and international governments and law enforcement agencies.

You must not attempt to monitor the use of our IT facilities by others or capture any data transmitted on our networks without explicit authority to do so.

[guidance]

10. Infringement

Infringing our regulations can result in sanction through our disciplinary processes. Penalties may include fines, withdrawal of all access to our IT facilities or disciplinary action that could lead to the termination of your studies or dismissal.

We will remove access to offending material immediately.

If appropriate, we will pass information about an infringement to the appropriate law enforcement agencies and any other organisations whose regulations you have breached.

We reserve the right to recover any costs incurred as a result of your infringement from you, including any expense incurred during the restoration of data by appropriate third parties.

You must inform us by email to itsecurity@anglia.ac.uk if you become aware of any infringement of our regulations. Failure to do so may be regarded as collusion on your part at a later date.

[guidance]

Part Three: Acceptable Use, Guidance Notes

This guidance expands on our ten core principles of acceptable use and includes some specific situations that will help you to relate your everyday use of our Information Technology (IT) resources, systems and services, collectively referred to as our IT facilities, to the *dos* and *do not's* of our regulations.

Also included some common examples, which are neither exhaustive nor all-inclusive.

We have drawn upon the Universities and Colleges Information Systems Association (UCISA) model IT Regulations (http://arul.ink/ucisaregs) and guidance from other institutional bodies such as the Joint Academic Network (Janet) and Eduserv relating to recent changes in industry and Higher Education best practice, such as:

- Increased use of social media by both users and institutions;
- Wider provision of Wi-Fi and the use of personally-owned devices to access our network and the Internet, commonly known as *Bring Your Own Device* or BYOD;
- Proliferation of cross-institutional and transnational resources;
- Institutional adoption of cloud-based services;
- Growing importance of cyber security.

1 Scope

1.1 Users

Our core principles of acceptable use apply not just to students and staff but also to **anyone** who makes use of our IT facilities, including, for example:

- External partners, contractors and agents based onsite and using our network, or offsite and accessing our systems;
- Tenants of our University using either our computers, servers and network or their own;
- People accessing our online services from off campus;
- Visitors using our Wi-Fi;
- Visitors to our websites;
- Third parties using our eduroam infrastructure to access the Internet or facilities at another institution.

1.2 IT facilities

IT facilities is a broad term that includes:

- IT hardware, such as PCs, laptops, tablets, smart phones and printers;
- Audio visual (AV) and media hardware located in our teaching spaces, at various other locations on our premises or for loan in support of your studies, employment or other approved activities;
- Software such as operating systems, office automation software, web browsers and commercial application packages, often accessible through specially negotiated deals or arrangements;
- Data that we provide, or to which we have arranged access, which might include online journals, data sets or citation databases;
- Access to our networks and those of our partners and agents, such as network connections in halls of residence, on-campus Wi-Fi and connections to the Internet from our PCs;
- Online services to which we have arranged access, such as Microsoft Office 365, Google Apps and the Joint Information Systems Committee's (JISC) online resources;
- IT credentials, such as your username(s) and password(s) or any other token(s), including your email address(es), smartcard(s) or dongle(s), that we have issued to you and that you use to identify yourself when using our IT facilities.

[core principles]

2 Governance

You should always remember that using our IT facilities will have consequences in the physical world.

Your use of any of our IT facilities is governed not only by our own principles, rules, policy and guidance but also is subject to IT-specific law, domestic law and regulation and potentially that of other countries.

2.1 UK Domestic law

Your behaviour is subject to the laws of the land, including those that may not appear to be IT-related 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;
- Computer Misuse Act, 1990;
- Defamation Act, 1996 and Defamation Act, 2013;
- Data Protection Act, 1998;
- Human Rights Act, 1998;
- Freedom of Information Act, 2000;
- Regulation of Investigatory Powers Act, 2000;
- Freedom of Information (Scotland) Act, 2002;
- Privacy and Electronic Communications (European Community Directive) Regulations, 2003;
- Prevention of Terrorism Act, 2005;
- Police and Justice Act, 2006;
- Terrorism Act, 2006;
- Criminal Justice and Immigration Act, 2008;
- Equality Act, 2010;
- Counter-Terrorism and Security Act, 2015.

For example: you must not create, transmit or cause the transmission of:

- Any offensive, obscene, extremist or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- Material with the intent to cause annoyance, inconvenience or needless anxiety;
- Material with the intent to defraud;
- Defamatory material;
- Material that infringes the copyright of another individual or organisation;
- Unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or otherwise part of, a service to which the user or their organisation has specifically chosen to subscribe;

Or deliberately and without authorisation:

- Access networked facilities or services.

2.2 International law

If you are using services that are hosted in a different part of the world, you may also be subject to specific local laws. With the increased use of cloud-based services it is more difficult to know the location in which a service is hosted and what laws are applicable to that location.

In general, if you apply common sense, obey domestic laws, adhere to the regulations of the service you are using and follow our ten core principles of acceptable use, you are unlikely to go astray.

2.3 General institutional regulations

You should already be familiar with our general regulations, policies and guidance. Key documents for students are available from http://arul.ink/studentkeydocs along with essential information from http://arul.ink/studentessentialinfo.

Staff can access polices and guidance from http://arul.ink/hrpolicies

2.4 Third-party regulations

If you use our IT facilities to access a third-party service or resource you are bound by the regulations associated with that service or resource. Very often, they will be explicitly presented to you when you first use the service. In some cases, however, the system or service may be so pervasive that you will not know that you are using it. If so, your acceptance is implicit to your continued use.

For example: each time you access the Internet from our campuses you are using the Joint Academic Network (Janet), the IT network that connects all UK higher education and research institutions, and you are implicitly subject to:

- The Janet Acceptable Use Policy, http://arul.ink/janetuse;
- The Janet Security Policy, http://arul.ink/janetsecurity;
- The Janet Eligibility Policy, http://arul.ink/janeteligibility.

We have incorporated many of these policies into our own core principles of acceptable use; if you abide by them you should not infringe the Janet policies.

Similar types of arrangement may apply to software licensing and other resources that we provide for you to use during your studies or as part of your day-to-day work. You must only use them according to the applicable terms and conditions.

For example: 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 *Combined Higher Education Software Team (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.

By using these packages you are implicitly accepting the CHEST User Acknowledgement of Third-Party Rights, http://arul.ink/chest-uo.

[summary | core principles]

3 Authority

Our IT regulations are issued under the authority of our University's Corporate Management Team (CMT), who are ultimately responsible for their interpretation and application. Day-to-day responsibility is delegated to our IT Services Directors' Team and Head of Infrastructure.

We grant authority to use our IT facilities in a variety of ways:

- Issuing a username, password or other IT credentials or token;
- Explicit access rights assigned to a specific resource or system;
- Provision of obviously public resources or services, such as our websites, self-service kiosks in public areas or any open, clearly branded and advertised Wi-Fi networks on our premises.

If you have any doubt whether or not you have the authority to use any of our IT facilities you must first seek further advice from our Student Help Desk or, for staff, our IT Services Customer Support Team.

An attempt to use our IT facilities without appropriate permission is an offence under the Computer Misuse Act.

[core principles]

4 Intended use

Our IT facilities, and the Janet network that connects them both with other Higher and Further Education institutions and to the Internet, are part funded by the UK government. It is essential that these facilities be used only for the purposes for which they are intended.

4.1 Use of our IT facilities for purposes that further our mission

Our IT facilities are provided in support of our mission. Use can include learning, teaching, research, knowledge transfer, public outreach and our commercial activities, as well as the administration necessary to support these activities.

4.2 Personal use

You can use our IT facilities for a limited amount of personal use, provided that it is not at odds with our core principles of acceptable use and does not interfere with, or prevent, other people from using our facilities for purposes of study or work.

For example: a student needing to complete an assignment on an open access computer will take precedence over others who want to access a social media site such as Facebook or Twitter for leisure purposes.

Employees using our 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.

Personal use is a concession. It is not a right, and can be withdrawn temporarily or permanently at any time.

4.3 Commercial use and personal gain

Use of our IT facilities for personal gain or for commercial purposes unrelated to our business activities will require the explicit approval of the Director of IT Services. You may be required to pay usage fees or provide a share of any income generated by this type of use. For more information, contact our IT Services Customer Support Team.

Even with such local approval, the terms and conditions and licensing of some facilities and resources may preclude their use. You must ensure that appropriate commercial usage arrangements are in place, we will not do so on your behalf.

The activities of some student clubs and societies may qualify as commercial use. You should seek advice from Anglia Students Union, http://arul.ink/studentclubs, before establishing any arrangements.

[core principles]

5 Identity

Many of our IT systems and services require that you identify yourself, so that we know that you are entitled to use them. To this end, we will normally provide you with a username and password, but other forms of IT credentials such as an email address, a smart card or some other form of security device may also be used when appropriate.

5.1 Protecting your identity

You must take all reasonable precautions to safeguard any IT credentials that we issue to you:

- You must change any password when we first issue it to you and at regular intervals thereafter or as instructed;
- Do not use simple, easily-guessed passwords, and do not record them where there is a likelihood of them being found or accessed by a third party;
- Do not use the same password for your personal accounts or accounts associated with other organisations;
- Do not share your IT credentials with anyone else, no matter how legitimate, convenient or harmless it may seem.

We will never ask you to validate your username and password or confirm other details either by email response or online. Scams of this sort, called phishing, are common on the Internet. They are used to gather information that will be subsequently used for identity theft or to gain inappropriate access to IT facilities.

Phishing messages can appear legitimate because they include our University crest or refer to our IT Services or support desks. They will often imply that you will lose access to a service if you do not respond immediately. This is social engineering, designed to cause panic. You can learn more about phishing from our online video at http://arul.ink/phishingvideo.

If you receive a request of this sort, or have any doubts about the authenticity of an email message, do not respond. Instead, please forward it as an attachment to phishing@anglia.ac.uk.

If you believe that someone else knows your password then change it immediately and report the matter to our Student Help Desk or to our IT Services Customer Support Team.

5.2 Using your identity online

Always check the details of any website that you wish to access:

- Do not use your username and password to login to services that you do not recognise;
- Do not login to websites that fail to show a padlock symbol next to the web address.

If you are working on any of our open access computers or remotely accessing our IT facilities in a public location:

- Do not leave your computer logged in and unattended;
- Log off properly when you are finished and wait until you are certain that the process is complete.

You must not allow anyone else to use your smartcard or other security hardware. Take care not to lose them, and if you do, report the matter at one of our student iCentres or to our IT Services Customer Support Team immediately.

5.3 Impersonation and identity misuse

You must never use another person's IT credentials, or attempt to disguise or hide your real identity while using any of our IT facilities. If you become aware that someone else is doing so you must report the matter to our Student Help Desk or our IT Services Customer Support Team immediately. By failing to do you are complicit to the activity.

You may remain anonymous if a system or service clearly allows such use, for example a public-facing website.

5.4 Attempting to compromise another person's identities

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

[summary | core principles]

6 Infrastructure

Our infrastructure encompasses everything that makes our systems and services function. It includes servers, networks, cabling, Wi-Fi, computers, printers, operating systems, databases and 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 engage in any activity that could jeopardise our IT infrastructure.

6.1 Physical damage or the risk of damage

Do not damage, or do anything that might result in physical damage of our IT infrastructure.

For example: carelessness with food or drink at an open access computer or other activities that are inappropriate to a given location.

6.2 Reconfiguring or altering settings

You must not attempt to alter the connection, configuration or settings of our IT infrastructure without authorisation, including changing network points or cables for a computer or another device, connecting a personal device to our networks - with the exception of Wi-Fi or Ethernet points specifically provided and signposted for that purpose - or altering the configuration of any piece of our equipment.

You must not add software to or remove software from our computers, smart devices or other hardware, including the application of firmware upgrades and patches, unless you have been given explicit written permission

Do not move equipment without authority.

6.3 Inappropriately extending our network

You must not add, extend or append to our cabled or Wi-Fi networks without authorisation. Such activities, often involving the use of routers, bridges, repeaters, hubs or local Wi-Fi access points, can disrupt our network and are likely to be a breach of the Janet Security Policy.

6.4 Introducing servers or services onto our network

You must not set up any hardware or software that would provide a service, to yourself or others, on our network without explicit permission. Examples would include gaming servers, file sharing services, IRC servers, mail servers or local websites.

In circumstances where permission has been given for a specific installation, you must provide details of the equipment, its configuration and an assessment of the potential network load that will be added to our IT systems and services. Should the installation cause disruption to our services at a later date we reserve the right to isolate it, without notice, until the cause has been appropriately addressed.

6.5 Introducing malware

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

The term malware covers many things such as viruses, worms and Trojans, but can be broadly regarded as any software that might disrupt operation or subvert security. It is usually spread by visiting high-risk websites, downloading files from untrusted sources, opening email attachments from unknown third parties or inserting media that have been created on or in contact with a previously compromised computer.

If you avoid these types of behaviour, keep your own antivirus software enabled and up to date and run preventative scans of your computer on a regular basis, you should not experience problems.

We reserve the right to recoup any costs incurred while addressing the cause and outcome of a large-scale malware outbreak.

6.6 Subverting security measures

We take measures to safeguard the security of our IT infrastructure, including the use of workstation and server antivirus software, firewalls and spam and malware filters and site blacklists.

You must not attempt to subvert or circumvent these measures in any way.

[summary | core principles]

7. Information

7.1 Personal, sensitive and confidential information

During the course of your studies or your work you may handle information that is protected under the Data Protection Act 1998, regarded as confidential or is potentially sensitive in some other way. For the rest of this section, we will group these different types of data collectively as *protected information*.

Safeguarding the security of protected information is a highly complex issue, with organisational, technical and human aspects. We have policies and guidance regarding the protection of data and the management of information, available from http://arul.ink/DPAandIS. If you handle protected information in any capacity, you must make yourself familiar with, and abide by, these policies.

You must at all times take all reasonable steps to safeguard and secure any protected information to which you have access as part of your studies or work. If in doubt, do not remove protected information from our premises or access it using an inappropriately secured medium.

Collected printer output immediately. Do not leave your own or that of other people in a location where it can be access by a third party.

7.2 Storing protected information

Portable media, such as USB storage devices, removable hard drives, CDs or DVDs, that are used to hold protected data must be stored securely on-premises and should never be left unattended while in use. They must be appropriately backed up and encrypted if used off-premises.

Some mobile devices include an online cloud storage provision that you can use to automatically backup essential settings and other information such as email messages and photographs. Examples include the Apple iCloud, Microsoft OneDrive and Google Backup Services. You must not store protected information on these third-party services, since we cannot ensure the security of the environment. Personal mobile devices should be configured to exclude protected data.

Mobile devices including laptops, tablets and smart phones must be password or Personal Identification Number (PIN) protected and, where appropriate, the storage contained in these devices should be encrypted.

Encryption key(s) must be securely stored in a manner that will not hamper legitimate investigations by a legal authority.

Advice on hardware and data encryption is available from our IT Services Customer Support Team.

We retain ownership of any protected information downloaded from our systems to a mobile device and reserve the right to delete it, without notice, where it is appropriate to do so. In such circumstances we will offer no guarantee to preserve other information on the device.

7.3 Transmitting protected information

You must use an appropriately secured method to transmit or transfer protected information by electronic means. Email is not inherently secure but may be made more so through the use of password-protected archive files and message encryption.

Advice about how to send protected information electronically is available from our IT Services Customer Support Team.

7.4 Sending protected information by post or courier

If you are dispatching removal media that contains protected information to an external destination you must use a secure, tracked and signed for service so that you know it has arrived safely. The media itself should be appropriately encrypted.

7.5 Remote working and access to protected information

You must ensure that you are using an approved connection method when accessing protected information from off-campus, in order to reduce the risk of data interception or loss. Wherever possible you must use our remote desktop facilities in preference to other solutions.

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

7.6 Personal or public devices and cloud services

Personal and third-party computers and smart devices cannot be guaranteed to be free of malware that could capture data as it is input, output or transmitted. You must not use equipment of this sort to access, transmit or store protected information.

You must not store protected information in personal cloud services, such as Dropbox, Google Drive or Microsoft OneDrive.

7.7 Copyright information

With a few exceptions, most published works are protected by copyright. If you are going to use material such as images, text, music or software, the onus is on you to ensure that you use it within copyright law. We provide guidance at http://arul.ink/copyright and http://arul.ink/dcscopyright, but as a rule of thumb you should remember that access to material on the Internet it does not imply ownership or the right to modify.

7.8 Other people's information

You must not attempt to access, modify, delete or disclose restricted information that belongs to other people without their permission unless it is obvious that they intend others to do so or that you have received appropriate approval.

7.9 Access to information on our servers

Information stored on our servers is the property of our University. In circumstances where you are unavailable for an extended period, we reserve the right to access information that has been produced during the course of your studies or employment, for business continuity purposes. We will take every care to avoid compromising any personal information that you have chosen to store on our facilities but cannot guarantee privacy.

7.10 Inappropriate materials

The Terrorism Act 2006 prohibits the publication of any statement that directly or indirectly promotes, encourages or endorses acts of terrorism retrospectively, at present or in the future. Sections of the Act mandate against the access, transmission and storage of such materials locally or on the Internet.

We have a statutory duty under the Counter-Terrorism and Security Act 2015, commonly known as *PREVENT,* to take all necessary steps to prevent people from being drawn into terrorism.

You must not create, download, store or transmit any unlawful material, or material that is extremist, indecent, offensive, defamatory, threatening, or discriminatory. We reserve the right to block or monitor access to such material at any time.

Our policies to approve and manage valid academic research that requires access to or storage of such material are available at http://arul.ink/ethicspolicy. You must gain appropriate approval before accessing any prescribed information, even if it is readily available from open or unsecure Internet locations.

Universities UK provides useful guidance on handling sensitive materials at http://arul.ink/UUKsensitivematerials.

7.11 Publishing information

Publishing is a blanket term that encompasses the release of any information to the general public through print and electronic means including websites, social networking and news feeds. While we generally encourage publication, there are some general guidelines to which you must adhere:

- You must not make statements that purport to represent our University without the approval of our Pro-Vice Chancellor, Corporate Marketing and International Development Services or a delegated authority;
- You must not publish information on behalf of third parties, using our IT facilities, without the approval of Director of IT Services.

[summary | core principles]

8. Behaviour

How you behave when using our IT facilities should be no different to how you would behave under other circumstances. Abusive, inconsiderate or discriminatory behaviour is unacceptable.

8.1 Online conduct and social media

Our dignity at study and work policy http://arul.ink/dignity extends to the use of social media and other online services.

8.2 Spam

You must not send unsolicited bulk emails or chain emails, other than in specific circumstances.

8.3 Denying others access to our facilities

If you are using our shared IT facilities for personal or social purposes, you must vacate them when they are needed by others with work to do. Do not occupy limited access specialist facilities unnecessarily if someone else has need of them.

Do not prevent other people from accessing our IT facilities by obstructing passageways, inappropriately rearranging furniture, disconnecting and moving equipment or reserving space by leaving bags, folders or other personal items while you are absent.

8.4 Causing disturbance for others

Always remember that others have a right study and work undisturbed.

- Keep noise to a minimum while using our shared IT facilities and other spaces;
- Turn down the volume or silence your mobile phone and other portable devices;
- Respect the operation of the silent study areas in our University Library;
- Be sensitive to what others around you might find disruptive or offensive.

8.5 Excessive consumption of resources and bandwidth

Always use our IT facilities wisely. Do not:

- Consume excessive bandwidth by uploading or downloading more material, particularly audio and video, than is necessary;
- Access online resources, such as gaming sites, that might impact upon the performance of our networks;
- Waste paper by printing more than is needed, or by printing single sided when double sided is available and appropriate
- Waste electricity by leaving equipment switched on needlessly.

[summary | core principles]

9. Monitoring

9.1 Institutional monitoring

We reserve the right to monitor, log and record the use of our IT facilities in order to:

- Detect, investigate or prevent the misuse of our facilities and breaches of our regulations and policies;
- Monitor the effective functioning of our facilities;
- Investigate allegations of misconduct.

We will comply with all lawful requests for information from government and law enforcement 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 our IT facilities without the explicit and time-limited permission. This includes:

- Monitoring or capture of traffic on our cabled and Wi-Fi networks;
- Network or device discovery;
- Installing key-logging or screen-capture utilities that can affect anyone other than yourself;
- Attempting to access our system logs, servers, network equipment.

If you need to gather information about the operation of our IT facilities and resources as part of your studies, you must be sponsored by your course leader or research supervisor. Staff must be sponsored by their line manager.

All requests for permission to monitor our IT facilities should be made by email to itsecurity@anglia.ac.uk and approved by written response before commencing.

[core principles]

10. Infringement

10.1 Disciplinary processes and sanctions

We will manage any breach of our principles of acceptable use through appropriate student or staff disciplinary processes. This could have a bearing on your studies or employment with us and with other organisations in the future.

We reserve the right to impose appropriate sanctions should we find your use of our IT facilities to be inappropriate or unacceptable, which may include restrictions on your use of our facilities and services, removal of access; withdrawal of offending material; fines and recovery of costs incurred by us while taking appropriate remedial action.

10.2 Reporting unacceptable use to other authorities

We will refer unacceptable use to the police or other enforcement agencies if we believe that

unlawful activity has taken place.

10.3 Reporting unacceptable use to other organisations

We will report unacceptable use to a third party organisation If we believe that a breach of their rules, regulations or policies has taken place.

10.4 Reporting unacceptable use

If you are aware of any activity that contraventions our core principles of acceptable use you must report the matter to our IT Services Customer Support Team immediately.

[core principles]

Document Change Record

Regulations for the use of our IT resources, systems and services and Resources: Principles of Acceptable Use	
Version:	1.2 (release)
Date:	8 January 2016
Notes:	Updates following feedback from the PREVENT Working Party. Submission for approval by the Information Management Advisory Group
Author:	Joe McIntyre
Version:	1.1
Date:	10 October 2015
Notes:	Addition to 2.1 and 7.10 to reflect PREVENT legislation, taken to PREVENT Working Party
Author:	Joe McIntyre
Version:	1.0 (release)
Date:	17 June 2015
Notes:	Internal hyperlinks and bookmarks added
Author:	Joe McIntyre, IT Services
Version:	0.1.2.1
Date:	12 June 2015
Notes:	Minor grammar changes and clarification following comment from the Information Management Advisory Group held on 11 June 2015
Author:	Joe McIntyre, IT Services
Version	0.1.2
Date	29 March 2015
Notes:	Updates incorporating comment from the IT Strategy Group, held on 16 February 2015
Author:	Joe McIntyre, IT Services
Version	0.1.1

Date	2 March 2015
Notes:	Updates following second meeting of CMT working party, held on 30 January 2015
Author:	Joe McIntyre, IT Services
Version	0.1.0
Date	27 January 2015
Notes:	Initial draft, based on original UCISA Draft IT Regulations document and feedback from first CMT working party held on 18 November 2014
Author	Joe McIntyre, IT Services
Sponsor	Tony Wright, IT Services
Working Party:	Jackie Barlow, Office of the Secretary and Clerk (for Steve Bennett) Steve Bennett, Office of the Secretary and Clerk Chris Chang, Corporate Marketing and International Development Services Les James, Faculty of Science and Technology Nicky Kershaw, University Library Joe McIntyre, IT Services Denise Thorpe, Human Resource Services Julie Walkling, Student Services Tony Wright, IT Services (Chair) Georgina Laudrum, IT Services (secretary)