University of East Anglia

University of East Anglia Regulations for Acceptable Computing Use

Document Control Information

Security Classification:	Open
Version:	2.0
Date Last Reviewed:	25 July 2025
Document Author:	Steve Knight *Chief Information Officer*
Approved by:	Anne Poulson *Senior Information Risk Owner*

Contents

1. Purpose

The University of East Anglia seeks to promote and facilitate the positive and extensive use of information and computing technologies in the interests of supporting the delivery of learning, teaching, innovation and research to the highest possible standards.

This is a formal statement of what is acceptable and unacceptable when using the University's IT facilities and network. They assist the University in maintaining a secure, safe and robust IT environment by identifying and promoting responsible behaviour and good practice in line with legal compliance frameworks.

Should you need any advice and/ or clarification of these Conditions please contact the IT Service Desk in the first instance by calling **01603 59 2345** or emailing **it.servicedesk@uea.ac.uk**

2. Scope

The Conditions set out in this Regulation applies to Users (staff, students, visitors, partners, contractors and others) of the University's IT and computing facilities.

It applies to any activities involving online, digital, computing, communication technology and networking facilities provided by the University, or for the University's purposes.

Limited use of the University network and IT facilities for personal purposes other than UEA work or study, for instance access to the internet, is permitted. However, such use must not interfere with work or studies, must be legal and must be strictly in accordance with the requirements laid down in these Conditions.

It is applicable to University owned, third party, and personally owned devices used to access and use University IT services whether on campus or elsewhere.

All Users are expected to read and comply with these Conditions and those set out in the supportive documentation outlined in Section 6.

3. Terminology

This document uses a range of language, some of which may not be common parlance. The below table establishes specific definitions to such terms.

Term	Definition
Computer	PCs, desktop systems, servers, laptops and notebooks.
Conditions	The requirements and expectations set out within this document.
Device	All equipment which can be connected to the UEA network including PCs, servers, laptops, as well as mobile devices such as phones, tablets and so on.
IT facilities	Computing equipment such as servers, PCs, laptops, tablets, smartphones and printers; software, data and information held on those systems; information systems used for administrative and other purposes; network access via wired and wireless connections; online services; and the user credentials used to identify you and manage access to facilities.
Personal Data	any information relating to an identified or identifiable living person such as – but not limited to - a name; identification number; contact details; location data; health data; religious, political or philosophical views; ethnicity; biometric data
Transmit	The processing of data including to: create, upload, download, stream, share, or publish.
Users	Any student, employee, worker, contractor, partner, franchisee or other individual who has, by virtue of their role or relationship with the University, any degree of access to the University's devices, information, data, files, or systems.

This section sets out the requirements of all Users, including those with additional responsibilities because of their role.

4.1 All Users

Have a responsibility:

- to read, understand, the Conditions set out in this document;
- to adhere to the Conditions set out in this document;
- to notify the ITCS Service Desk should they be aware of a contravention, or potential contravention, of the Conditions set out in this document.

4.2 Users with additional responsibilities

4.2.1 Information Asset Owners

In relation to their information assets, have a responsibility, to:

- ensure Users processing data, or operating devices, are aware of these Conditions
- prevent intentional deviations from these Conditions and – if appropriate – raising an exemption request with the SIRO for consideration.

4.2.2 IT and Computing Service (ITCS)

Have a responsibility to:

- ensure all Users are aware of these Conditions before enabling a UEA IT account or UEA owned device
- published these Conditions, in a location accessible to all Users
- implement and operate controls to monitor compliance with these Conditions;
- and to report instances of non-compliance to the Chief Information Officer, Data Protection Officer and/or Senior Information Risk Owner as appropriate.

4.2.3 Senior Information Risk Owner (SIRO)

Is responsible for considering and, if appropriate:

- authorising proposed changes to these Conditions and the associated Policies and University Regulations relating to Information Risk Management.
- approving any exemptions to these Conditions where appropriate.
- ordering the cessation of an activity that is non-compliant with these Conditions.

4.2.4 Chief Information Officer (CIO)

Is responsible:

- for reviewing these Conditions and submitting any proposed changes to the SIRO for review and approval. The task of reviewing of these Conditions may be delegated but responsibility remains with the CIO.
- for considering and, if appropriate, ordering the cessation of an activity that is non-compliant with these Conditions.

4.2.4 Data Protection Officer (DPO)

Is responsible:

- for considering and, if appropriate, ordering the cessation of an activity – that impacts upon personal data - that is non-compliant with these Conditions.

5. Regulations Statement

5.1 Device Management

To ensure appropriate device and network management measures, you must:

1. only connect devices to the wired or residence network in line with the ITCS device registration processes.

2. ensure the operating system is currently supported within the product lifecycle, i.e. the operating system must have been released, not preview or beta, and still be in receipt of security patches from the software vendor.

3. ensure the application software security patches are applied and, where feasible, up to date anti-virus/anti-malware software installed.

4. set security on the device to prevent unauthorised access, especially where synchronisations to university data or systems are established.

5. report the loss of any University device or device storing University data to the IT Service Desk as soon as possible.

6. cease to use any device at the direction of the University's Senior Information Risk Owner, Chief Information Officer, or Data Protection Officer.

5.2 Network Security

To ensure appropriate network security, you must:

1. not undertake any penetration testing, vulnerability scanning, or the monitoring or interception of network traffic unless approved by the CIO/SIRO.

2. not use any method, tool, or system apart from the University's virtual private network (VPN) for remote access to the facilities or services unless approved by the CIO/CIRO. This includes a prohibition on the use of proxy or anonymising services to bypass security controls or access restricted content.

3. not undertake activities with the intention of:
    a. corrupting, destroying, or holding to ransom University data or systems
    b. disrupting the network or causing a denial of service
    c. disrupting or annoying others.
    d. deliberately or recklessly consuming excessive IT resources such as processing power, bandwidth, storage, or consumables.
    e. introducing malware or viruses.

4. cease to any activity in contravention of the above at the direction of the University's Senior Information Risk Owner, Chief Information Officer, or Data Protection Officer.

5.3 Access Control

To ensure appropriate access control measures, you must:

1. ensure computer systems in your care are secure against unauthorised access. This includes preventing others from using your device or account by locking a device when it is not in use.

2. ensure your passwords are confidential; they must be unique and in line with the University's password guidance.

3. ensure you never write passwords down or disclose them to others (including to those purporting to come from the University).

4. use multifactor authentication (MFA) and have available the means for doing so - such as mobile phone with the Microsoft Authenticator application, or use physical keys as provided by the University as necessary;

5. not attempt to circumvent the University's security measures. This includes obtaining or using another person's IT credentials, or disguising your identity when using IT facilities.

6. report any actual or suspected compromised passwords or credentials to the IT Service Desk as soon as possible.

7. reset any password at the direction of an employee of University's IT & Computing Service, or the Information Compliance Team.

5.4 Software

To ensure appropriate software use, you must:

1. not install, disable or remove software unless authorised to do so;

2. not use or transmit unlicensed or pirated software;

3. only using approved processes to install software onto University devices;

4. only copy or distribute software to others where you are authorised to do so, to prevent violations of copyright or licensing agreements;

5. co-operate with persons employed by the University to carry out software and data audits, and where required follow software registration procedures;

6. cease to use any software – including AI products - at the direction of the University's Senior Information Risk Owner, Chief Information Officer, or Data Protection Officer.

5.5 Email use

When using email, you must:

1. not auto-forward emails from a University email account

2. not use University-managed email clients to access personal email accounts.

5.6 Personal Data

To ensure appropriate data processing, you must:

1. only process personal in a manner consistent with the University's Information Risk Policy, Data Protection Regulations, and other associated documents lists in Section 6.

2. only attempt to access University systems, files and data which you are authorised to access.

3. only use your access to University systems, files and data for legitimate work purposes, and not for personal gain.

4. not violate the privacy of others.

5. cease to process data, or amend processing procedures, at the direction of the University's Senior Information Risk Owner, Chief Information Officer, or Data Protection Officer.

5.7 Third-Party processing

Where engaging with third-party processing:

1. If a service provided from outside the University is accessed by means of University facilities, then Users must also abide by that provider's Conditions of use, code of conduct, policies or rules relating to the use of that service.

2. The University is not liable for any financial or material loss to an individual user in accessing the internet for personal use. For example, if a user connects to external services using the University network and internet connection in order to carry out personal transactions such as purchase of goods or banking transactions, the University accepts no liability for those transactions, or for the security of any personal data transmitted.

5.8 Content

The University adheres to principles of academic freedom of expression; however, when transmitting data, you must:

1. not undertake activity to hack or intercept the communications of others.

2. not transmit material that:
    a. is illegal. This includes sites which are specifically designed to promote terrorism or are directly linked to a proscribed terrorist organisation; this does not apply during recognised research or teaching that is permitted under UK and international law.

    b. is offensive, discriminatory or hate speech, malicious, indecent, obscene, threatening, abusive, bullying, causes harassment or distress, or whose effect brings the University into disrepute;

    c. is fraudulent or libellous;

    d. includes personal data without a lawful basis for processing;

    e. unsolicited commercial or advertising material;

    f. is pornographic;

    g. jeopardises the confidentiality, integrity, availability, performance or reliability of the University's IT facilities, resources, or data assets

    h. infringes the copyright, licenses, or intellectual property rights of the University, research funders, or any other person/organisation.

3. ensure that any published information:
    a. is known to be up to date and accurate;

    b. reflects or position of the University, or contains an explicit disclaimer identifying the published information reflects the view of an individual and not the wider School/Faculty/Division or the University.

5.9. Breaches of these Conditions

If there are reasonable grounds for suspecting that a user is engaging in activities which are in breach of these Conditions, the University reserves the right to:

1. investigate fully, including directly monitoring use of the network and computing facilities by the user. Direct monitoring of individual use and/or withdrawal of services in such circumstances may be authorised only by the Chief Information Officer, Senior Information Risk Owner or Data Protection Officer. If appropriate these officers may engage in consultation with Human Resources and/or Academic Registry.

2. withdraw (either temporarily or permanently) the authority of any user or device to use system, or the whole network.

3. initiate disciplinary proceedings. In serious cases, this could result in dismissal for staff or exclusion for students. A significant breach of these Conditions of use is likely to be regarded as serious or gross misconduct.

4. report suspected criminal behaviour to the appropriate law enforcement agencies or regulators.

5. charge Users for the restitution costs, as determined by the University, in relation to any damage they wilfully cause to any IT facilities.

6. seek reimbursement of any costs arising from legal actions taken against the University caused by any failure of a user to comply with the requirements of these Conditions, where this has been due to wilful neglect, deliberate avoidance or criminal act.

6. Supporting Documents

This document is supported by the below documents; these that should be read in conjunction with these Conditions.

6.1 Supporting Policies

- General Information Security Policy
- Data Protection Policy
- Records Management Policy
- Information Classification and Data Management Policy
- Freedom of Information Policy
- Artificial Intelligence (AI) Policy

7. Monitoring & Evaluation

These Regulations were approved by the University's SIRO.

It will be reviewed by the Author at least every two years, or sooner if necessary.

Any major revisions to these Regulations must be approved by SIRO.

8. Version History

Revision	Date	Revision Description
1.0	2023	
2.0	July 2025	Major revision.