

# Acceptable Use Policy

## (POL-02)

<b>Date approved:</b>	19 February 2026
<b>Approving body:</b>	Senior Information Risk Owner
<b>Date of next review:</b>	January 2028
<b>Review frequency:</b>	Every 2 years
<b>Policy/Regulation Owner:</b>	Chief Information Security Officer (CISO)

If you require more information about this policy/regulation, please contact the Governance Office by emailing [Governance@uea.ac.uk](mailto:Governance@uea.ac.uk) – The Governance Office will direct your query to the relevant team or individual.

## 1. Overview and Purpose

**1.1** The University of East Anglia (UEA) is committed to providing secure, resilient, and well-governed information and technology services that support excellence in teaching, learning, research, and innovation. This Acceptable Use Policy (AUP) defines the standards of behaviour required to protect UEA's digital environment.

**1.2** Users must understand and adhere to this policy to maintain the confidentiality, integrity, and availability of UEA systems, services, and data, and to comply with legal obligations and good security practice.

**1.3** This AUP is aligned with recognised cyber security frameworks and guidance, including:

- UK NCSC Cyber Assessment Framework (CAF) 4.0
- NIST Cybersecurity Framework (CSF) v2.0
- UK NCSC technical and governance guidance

**1.4** For advice or clarification, contact the IT Service Desk on 01603 59 2345 or [it.servicedesk@uea.ac.uk](mailto:it.servicedesk@uea.ac.uk)

## 2. Scope

**2.1** This AUP applies to all users (staff, students, contractors, partners, visitors and associates) accessing, using, transmitting, or managing University data, systems, networks, or devices - whether University-owned, third-party, or personal - on or off campus.

**2.2** Limited personal use is permitted provided it:

- 2.2.1** does not interfere with work, study, research, or system availability;
- 2.2.2** complies with this AUP and the law; and
- 2.2.3** does not introduce risk to UEA systems or data.

### 3. Definitions

Term	Definition
Computer / Device	Any equipment capable of connecting to the UEA network (e.g., laptops, desktops, tablets, smartphones, servers).
IT Facilities	All digital services including hardware, software, network services, cloud services, email, collaboration platforms, storage, and credentials.
Personal Data	Information relating to an identifiable living individual.
Transmit	Create, upload, download, stream, share, store, or publish data.
Users	All individuals authorised to access UEA digital resources.

### 4. Roles and Responsibilities

#### 4.1 All users must:

- 4.1.1** read and comply with this AUP;
- 4.1.2** report any actual or suspected policy violation, security incident, phishing attempt, compromised account, or data breach; and
- 4.1.3** uphold responsible, safe, and lawful use of UEA digital systems.

#### 4.2 Information Asset Owners (IAOs) must:

- 4.2.1** ensure asset security controls reflect CAF and NIST CSF expectations for governance, asset management, and data protection;
- 4.2.2** ensure users understand their obligations; and
- 4.2.3** request exemptions from the SIRO when necessary.

#### 4.3 IT and Computing Services (ITCS) will:

- 4.3.1** ensure users are informed of this AUP before account/device activation;
- 4.3.2** publish and maintain this AUP;
- 4.3.3** implement technical controls, monitoring, and compliance measures aligned with CAF/NIST CSF expectations; and

**4.3.4** report non-compliance to the CISO, DPO, or SIRO as appropriate.

**4.4** The Senior Information Risk Owner (SIRO) will:

**4.4.1** approve changes to the AUP;

**4.4.2** approve exemptions; and

**4.4.3** mandate cessation of non-compliant activities where required.

**4.5** The Chief Information Security Officer (CISO) will:

**4.5.1** oversee AUP review and compliance; and

**4.5.2** mandate cessation of non-compliant activities where required.

**4.6** The Data Protection Officer (DPO) may:

**4.6.1** mandate cessation of non-compliant personal data related activities.

## **5. Policy Statement and Conditions of Use**

**5.1.** UEA requires all users to follow the conditions below to protect University systems, services and information. Breach of these conditions may result in investigation and enforcement action (see section 6).

**5.2** When it comes to **device security and management**, all users must:

**5.2.1** use only supported and vendor-patched operating systems and applications;

**5.2.2** keep devices protected with up-to-date anti-malware (where applicable) and security controls;

**5.2.3** secure devices with strong authentication and auto-lock when unattended;

**5.2.4** store University information only in approved locations and services;

**5.2.5** report lost/stolen devices or suspected compromise immediately;

**5.2.6** comply with ITCS instructions to isolate, remediate or stop using a device where risk is identified;

**5.2.7** NOT disable, bypass or tamper with security controls (e.g., antivirus/EDR, encryption, management profiles); or

**5.2.8** NOT connect devices that are jailbroken/rooted or otherwise unsafe to University services.

**5.3** In terms of **network use and protection**, all users must:

**5.3.1** use University networks and remote access services in line with ITCS guidance;

**5.3.2** take reasonable care not to disrupt services or degrade performance for others;

**5.3.3** NOT perform scanning, penetration testing, packet capture, interception or monitoring without explicit authorisation;

**5.3.4** NOT connect unauthorised networking equipment (e.g., rogue Wi-Fi access points, switches, hubs);

**5.3.5** NOT bypass security controls (e.g., unauthorised proxies, tunnelling tools, non-UEA VPNs where prohibited); or

**5.3.6** NOT introduce malware, malicious code, or carry out activities that disrupt services (including DoS/DDoS).

**5.4** In regard to **Access control and authentication**, all users must:

**5.4.1** keep credentials confidential and use them only for their own access;

**5.4.2** use MFA where available/required;

**5.4.3** lock screens and log out of shared systems when finished;

**5.4.4** report suspected account compromise immediately and follow instructions to reset credentials;

**5.4.5** NOT share accounts or passwords, or allow others to use their credentials;

**5.4.6** NOT attempt to access systems, data or accounts without authorisation; and/or

**5.4.7** NOT attempt to escalate privileges, impersonate users, or circumvent access controls.

**5.5** When using **Software, services and AI tools**, all users must:

**5.5.1** use only approved software and services for University activity;

**5.5.2** comply with software licensing terms and University guidance;

**5.5.3** obtain approval where required before adopting new tools (including AI tools) for University purposes;

**5.5.4** NOT install, modify or remove software on managed devices without authorisation;

**5.5.5** NOT use unlicensed/pirated software; or

**5.5.6** NOT use unapproved AI tools for University data where this would create security, privacy, legal or contractual risk.

**5.6** Whilst using **Email, messaging and collaboration tools**, all users must:

**5.6.1** use University-approved platforms for University business where required;

**5.6.2** treat messages and email as official records where applicable;

**5.6.3** NOT auto-forward University email to external accounts without explicit approval; or

**5.6.4** NOT use University-managed email clients to access personal email accounts where prohibited.

**5.7** In terms of **Information handling, personal data and privacy**, all users must:

**5.7.1** handle University information in line with classification, confidentiality and handling rules;

**5.7.2** process personal data only where there is a lawful basis and in accordance with UK GDPR and University policy;

**5.7.3** access only the data they are authorised to access and need for legitimate purposes;

**5.7.4** report suspected data loss, unauthorised disclosure or breaches promptly;

**5.7.5** NOT store or share confidential/personal data using unapproved services or insecure channels; or

**5.7.6** NOT disclose University or personal data without authority, consent or lawful basis.

**5.8** When accessing **Third-party services or conducting personal transactions**, all users must:

**5.8.1** comply with third-party terms of use when using external services via University networks;

**5.8.2** understand that personal transactions are conducted at the individual's own risk and responsibility;

**5.8.3** NOT enter into third-party processing arrangements involving University data without appropriate approvals and contractual safeguards.

**5.9** When considering **Content standards and lawful use**, all users must:

- 5.9.1** behave lawfully and respectfully when using University systems and networks;
- 5.9.2** make clear when views expressed are personal (where there is a risk of association with UEA);
- 5.9.3** NOT create, access, store, transmit or publish material that is unlawful (including extremist content, except where lawfully required for approved research);
- 5.9.4** NOT create, access, store, transmit or publish material that is discriminatory, hateful, harassing, threatening or abusive;
- 5.9.5** NOT create, access, store, transmit or publish material that is defamatory, fraudulent or misleading;
- 5.9.6** NOT create, access, store, transmit or publish material that is obscene or otherwise inappropriate for a University environment;
- 5.9.7** NOT create, access, store, transmit or publish material that is infringing intellectual property rights; or
- 5.9.8** NOT create, access, store, transmit or publish material that is likely to cause security risk, reputational harm, or operational disruption.

## **6. Compliance and Monitoring**

- 6.1** Compliance with this Acceptable Use Policy is mandatory. UEA may take proportionate action to protect its systems, services, users and information, and to meet legal and regulatory obligations.
- 6.2** UEA may monitor the use of University systems and networks where necessary and lawful (including to detect security threats, misuse, or policy breaches);
- 6.3** UEA may investigate suspected breaches, including reviewing logs, access records and relevant content where authorised; and
- 6.4** Breaches may be escalated to the SIRO, CISO, DPO, HR, Student Services, Legal, Internal Audit or external authorities as appropriate.
- 6.5** Where a breach is suspected or confirmed, UEA may:
  - 6.5.1** require immediate cessation of the activity;
  - 6.5.2** require removal of unauthorised software, services, content or data;
  - 6.5.3** restrict, suspend or revoke access to accounts, devices, systems or networks;

**6.5.4** isolate devices or services to contain risk and support remediation;

**6.5.5** mandate security actions (e.g., password reset, MFA enablement, patching, device rebuild); and/or

**6.5.6** apply compensating controls or time-bound restrictions to manage residual risk.

**6.6** When considering the **disciplinary, legal and financial consequences** of a breach, UEA may:

**6.6.1** take action under staff disciplinary procedures or student regulations (which may include dismissal or exclusion);

**6.6.2** refer suspected criminal matters to law enforcement;

**6.6.3** report issues to regulators where required; and/or

**6.6.4** recover reasonable costs arising from negligent or malicious acts that cause damage, disruption, or legal/financial exposure to the University.

## **6.7 Reporting requirements**

**6.7.1** Users must report suspected security incidents, account compromise, phishing, data loss, or policy breaches promptly via the IT Service Desk (or other published reporting route); and

**6.7.2** Users must cooperate with reasonable instructions to support investigation, containment, and recovery.

## **7. Related Documents**

- Information Risk Management Policy
- Data Protection Policy
- Records Management Policy
- Information Access and Publication Policy

## 8. Revision History

Version number	Approval date	Approval mechanism	Details of change
1.0	2023		
2.0	July 2025	SIRO	Major revision
3.0	19 Feb 2026	SIRO	Major revision

### 8.1 Policy review triggers

In addition to the standard review cycle, this policy will be reviewed sooner where:

- there is a significant security incident or trend that changes UEA’s risk exposure;
- there are material changes to law, regulation, or sector expectations;
- there are significant technology changes (e.g., core platforms, identity, endpoint, network); or
- audit/assurance findings require policy amendment.