Information Security - Acceptable Use Policy

A University wide Information Security policy produced for the Information Security Strategic Risk Group.

DOCUMENT CLASSIFICATION	Public
DOCUMENT REF	ISMS-POL-AU-001
VERSION	1.0
DATED	01 August 2026
DOCUMENT AUTHOR	Cybersecurity Manager
DOCUMENT OWNER	Cybersecurity Manager

Table of Contents

1. Introduction

The University of Strathclyde provides information and communication technology (ICT) facilities to support teaching, learning, research, and administration. Responsible use of these facilities is essential to protect the University's information, maintain compliance with legal and contractual obligations, and safeguard the University's reputation.

This policy sets out the acceptable use of University ICT facilities by staff, students, contractors, and authorised third parties.

2. Scope

This policy applies to:

- All staff, students, visitors, contractors, and third parties using University ICT resources.
- All devices connected to the University's networks (wired, wireless, VPN, or cloud-hosted).
- All information systems, digital data, and electronic communication services owned or provided by the University.

a. Use of these facilities is also bound by the **JANET Acceptable Use Policy** and the University's overarching **Information Security Policy**.

3. Policy

3.1 User Identification and Authentication

- Each user shall be assigned a unique user identifier (username). User accounts are for individual use only and must not be shared under any circumstances.
- Users must take reasonable steps to protect their authentication credentials, including passwords, tokens, and Multi-Factor Authentication (MFA) codes. Credentials must never be disclosed to others, including colleagues or IT staff.
- Multi-Factor Authentication (MFA) must be used where available.
- Users are accountable for actions performed using their account and must take reasonable steps to protect their credentials.
- Users must immediately report any suspected or actual compromise of their account, credentials, or authentication mechanisms to the IT helpdesk.
  Email - help@strath.ac.uk
  Phone - 0141 548 4444
- Where misuse, negligence, or failure to follow security requirements is identified, users may be held accountable for activity performed under their account.

3.2 Access and Password Controls

- Users must not deliberately attempt to access systems, data, or services for which they are not authorised, nor attempt to bypass or weaken security controls.
- Privileged accounts must only be used for approved administrative activities and must be protected using Multi-Factor Authentication (MFA).
- All user passwords must be unique per system or service and meet the password guidance published here – they shall not be reused across internal University systems or external services.
- Users shall provide a personal email address for password resets and for contact should a user's account be suspended.

3.3 Cybersecurity Awareness Training

- All staff must complete the mandatory Cybersecurity Awareness Training as provided by the University, including refresher training where required. The mandatory training policy can be found here.
- Students must complete Cybersecurity Awareness Training where it is mandated by their academic department, programme, or the University, based on the nature of their access to university systems or data.
- Third parties, including contractors, consultants, and partners, must complete Cybersecurity Awareness Training where required by the University, particularly where they are granted access to university systems, networks, or information.
- Failure to complete Cybersecurity training may result in performance management and/or disciplinary action, in accordance with the University's disciplinary procedures for staff and action in accordance with relevant contractual, academic, or regulatory processes for students, contractors, or third parties.

3.4 Use of Email and Messaging

- University-provided email, messaging and collaboration services must be used for all official University business and for the communication of university information.
- Personal email or messaging accounts must not be used to conduct University business or to transmit University information, except where explicitly authorised for incident response or business continuity purposes, and only when University communication systems are unavailable.
- The automatic forwarding of university email to external email providers or accounts is prohibited, unless explicitly approved by the University.
- Messaging must be professional and must not contain offensive, defamatory, discriminatory, unlawful, or otherwise inappropriate content.

3.5 Personal Use

- University ICT facilities and services are provided primarily for university business, teaching, research, study and administration.
- Personal use of University ICT facilities and services should be avoided where possible.
- Any personal use must not:
    - interfere with the user's work or study, or that of others;
    - be excessive;
    - involve the storage of excessive amounts of personal information or files; or
    - breach University policies, contractual obligations, applicable legislation or law.
- The use of University ICT facilities for cryptocurrency mining or similar resource-intensive activities is prohibited.

3.6 Connecting Devices

- Personally owned devices may connect to the University's wireless Eduroam network, subject to compliance with security requirements as defined and published in the 'Information Security - Mobile and Remote Working Policy'.
- Only University-managed and approved devices may connect to the University's wired networks or access the University's Virtual Private Network (VPN).

3.7 Cloud and Third-Party Services

- Only University-approved and contractually agreed cloud and third-party services may be used to store, process or transmit University information.
- Where University-provided services do not meet legitimate business requirements, users must engage with their local IT teams to assess, approve, and formally onboard alternative third-party services in line with university procurement, information security, and data protection requirements.

3.8 Remote Working

- Remote and mobile working must be carried out in accordance with the University's Mobile and Remote Working Policy and associated standards.

3.9 Unacceptable Use

Examples of unacceptable use include, but are not limited to:

- Any activity proscribed by the Computer Misuse Act 1990.
- Any activity prohibited by applicable law, including the Computer Misuse Act 1990.
- Any illegal activity, including but not limited to unauthorised system access, copyright infringement, or the misuse of computing resources.
- Accessing, creating, storing, or transmitting material that is offensive, obscene, extremist, discriminatory, or otherwise unlawful.
- Bullying, harassment, intimidation, or abuse of others.
- Activities that may bring the University into disrepute.
- Running unauthorised servers, services, or applications, or using remote access tools without the approval of IT Services.
- Unauthorised scanning, probing, or testing of devices, systems, or services connected to the University network.

- Creating, storing, or transmitting material that infringes copyright or intellectual property rights.
- Creating, accessing, storing, or transmitting defamatory material, obscene or indecent material, extreme pornographic material, or prohibited images of children. Where there is a genuine academic or research requirement to access such material, prior written approval must be obtained from the Chief Commercial Officer before access takes place.
- Sending unsolicited or unauthorised bulk email or messages (spam).
- Using software in a manner that breaches licensing terms or using software licensed for restricted purposes for any other use.

3.10 Information Security Incidents

- Any suspected or confirmed information security incident, including phishing attempts, malware infections, or data loss, must be reported immediately to the IT Helpdesk.
- Where there is a suspected or actual breach of personal data, the Information Governance Unit should also be informed immediately (either by the user or the IT Helpdesk).
- Loss or theft of university-managed or personally owned devices used to access University systems must be reported immediately to the IT helpdesk.
- Users must cooperate fully with investigations and follow instructions issued by the University during the management of an information security incident.

Users may report or contact the IT Helpdesk by:
Email - help@strath.ac.uk
Phone - 0141 548 4444

4. Monitoring

The University monitors the use of its networks, systems, and services for lawful purposes, including ensuring compliance with university policies, detecting and responding to security threats, and supporting investigations.

All monitoring activities will be conducted in accordance with applicable UK data protection and privacy legislation, the Jisc Acceptable Use Policy, and the University's supporting information security, data protection, and governance policies.

5. Non-compliance

Failure to comply with this policy may result in one or more of the following actions, depending on the nature and severity of the non-compliance:

- Restriction or blocking of device access to university systems or services.
- Withdrawal of access to university-managed devices or services.
- Disciplinary action in accordance with the University's disciplinary procedures for staff.
- Action in accordance with relevant contractual, academic, or regulatory processes for students, contractors, or third parties.

6. Supporting Documents

- Information Security Policy
- Jisc JANET AUP
- Legal Framework for ICT
- Mobile and Remote Working Policy
- Mandatory Training Policy
- Data Protection Policy
- Records Management Policy

7. Document Information

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1.0	August 2026	Cybersecurity Manager	First version.
Next Review date			
August 2028			

Distribution

NAME
All users of IT systems.

Approval

NAME	POSITION	GROUP	DATE