IT Acceptable Use Policy

Document type:	Policy		
Document number:	IT-098	**Version**	02
Department:	Information Technology		
Approved by:	Executive Board		
Date approved:	12/05/2025	**Review Date**	12/05/2028
Publication:	SOAS website		
Related Documents:			

Note: All policies must be read in conjunction with all other SOAS policy, procedure and guidance documents. Printed copies of policies may not be the most up to date, therefore please refer to the policy pages on the SOAS external website or intranet for the latest version.

1. Introduction

The aim of this policy is to ensure that SOAS' IT facilities, M365 applications such as email and Teams and IT hardware and software services are used safely, lawfully, and equitably. This policy applies to all members of the SOAS community, including students, faculty, staff, and any other individuals granted access to SOAS IT and email services.

2. Scope

This policy applies to all members of the SOAS community as above and covers the use of IT facilities (hardware, software, data, network access, third-party services, online services, or IT credentials) and email services. It covers all email activities conducted using SOAS email accounts, whether for academic or administrative purposes.

3. SOAS Work Account Ownership and Access Statement

Your SOAS work account is the property of SOAS University of London and is provided for your professional use in carrying out your duties.

While SOAS retains ownership of the account and its contents, users can expect to work with a reasonable degree of privacy and without routine interference. The university respects the confidentiality of professional communications and recognises the importance of trust in the workplace.

However, in circumstances where access is required to ensure operational continuity such as unexpected absence, emergency situations, or business-critical needs, access to your account may be granted to your line manager, but only with prior authorisation from the Head of your Directorate or Department.

Such access will be:

- limited to what is necessary
- logged and overseen by IT Services
- handled with discretion and in accordance with SOAS policies and data protection laws

By using a SOAS account, you acknowledge and accept these terms as part of your professional responsibilities.

SOAS staff accounts will be disabled 3 days after termination of contract. Student accounts will remain accessible for 4 months after the completion of their studies.

There may be exceptional reasons such as participation in joint academic activities where a leaver may be granted access to their account following the leaving date. These can be requested by a senior or executive manager (such as Head of department or Director) and approved based on an assessment of the data protection and security risk by the CIO.

4. Governance

When using IT, you remain subject to the same laws and regulations as in the physical world.

It is expected that your conduct is lawful. Furthermore, ignorance of the law is not considered to be an adequate defence for unlawful conduct.

When accessing services from another jurisdiction, you must abide by all relevant local laws, as well as those applicable to the location of the service.

You are bound by SOAS' general regulations when using the IT facilities, available at Policies and procedures | SOAS and Information Compliance | SOAS

When using services via Eduroam, you are subject to both the regulations of SOAS and the institution where you are accessing services.

Some software licences procured by SOAS will set out obligations for the user – these should be adhered to. If you use any software or resources covered by a Chest agreement, you are deemed to have accepted the Chest User Acknowledgement of Third Party Rights.

Breach of any applicable law or third-party regulation will be regarded as a breach of this policy.

5. Authority

These regulations are issued under the authority of the Chief Information Officer (CIO) who is also responsible for their interpretation and enforcement, and who may also delegate such authority to other people.

You must not use the IT facilities without the permission of the CIO.

You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of these regulations. If you feel that any such instructions are unreasonable or are not in support of these regulations, you may appeal to the chair of the IT Governance Group in the first instance or students may invoke the complaints procedure, see Making a complaint | SOAS

6. Intended Use

The IT facilities are provided for use in furtherance of the mission of SOAS, for example to support a course of study, research or in connection with your employment by the institution and not for personal use, this includes printing.

Use of these IT facilities for non-institutional commercial purposes, or for personal gain, requires the explicit approval of the Chief Operating Officer (COO).

Use of certain licences is only permitted for academic use and where applicable to the code of conduct published by the Combined Higher Education Software Team (CHEST). Chest - User obligations as well as compliance with the Responsibilities of Janet-Connected Organisations | Jisc community and Acceptable use of the network | Jisc community

7. Identity

You must take all reasonable precautions to safeguard any IT credentials (for example, a SOAS username and password, email address, smart card or other identity hardware or software) issued to you. This includes using strong, unique passwords, enabling multi-factor authentication where available, and regularly updating and demarcating your passwords.
It is not permitted for staff and students use their SOAS accounts to sign up for personal business such as LinkedIn, Amazon accounts, personal social media etc. We recommend that you

- create email addresses to demarcate personal and professional personas
- sign up to a password manager to manage passwords and use the password manager in resetting all accounts to a unique password and
- set up MFA on all important personal accounts.

You must not allow anyone else to use your IT credentials. No-one has the authority to ask you for your password and you must not disclose it to anyone. You must ensure you are vigilant against phishing attempts and that any communication requesting your credentials is verified through official channels. SOASreserves the right to conduct phishing simulations and mandate that members of staff refresh their Cyber Security training.

You must not attempt to obtain or use anyone else's credentials. Ensure that any sharing of information respects privacy and follows the appropriate guidelines.

You must not impersonate someone else or otherwise disguise your identity when using the IT facilities. Always use secure and reputable services to protect your identity and personal information.

Cyber security training is mandatory for use of a SOAS staff account. Further and updated information is available via staff and student intranets:

- Cyber security safety - Cyber Security Safety for Staff
- Cyber safety for students - Cyber Security

We reserve the right to withdraw access to your account should this training not be completed and we may conduct sporadic phishing simulations and other cyber monitoring activities.

8. Infrastructure

You must not jeopardise the integrity of the IT infrastructure by, for example, doing any of the following without approval:

- damaging, reconfiguring or moving equipment
- loading software on SOAS' equipment other than in approved circumstances
- reconfiguring or connecting equipment to the network other than by approved methods
- setting up servers or services on the network
- deliberately or recklessly introducing malware
- attempting to disrupt or circumvent IT security measures

Users must not jeopardise the integrity of the IT infrastructure or handle personal, confidential, or sensitive information improperly. Compliance with SOAS' Data Protection Policies is required.

9. Information

If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it and must observe SOAS' Data Protection (Data Protection Policy | SOAS), and Data Classification Policy particularly with regard to removable media, mobile and privately owned devices as well as your responsibilities for data held in a third party cloud.

You must not infringe copyright or break the terms of licences for software or other material. If you need to re-use or re-purpose copyrighted works for non-commercial purposes to support your teaching, research or administrative activities at SOAS, please contact copyright@soas.ac.uk before proceeding.

You must not attempt to access, delete, modify or disclose information belonging to other people without their permission, or explicit approval from the CIO.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory. SOAS has procedures to approve and manage valid activities involving such material; these are available at https://www.soas.ac.uk/research/ethics/ must be observed.

10. Information Security

At SOAS, we are committed to maintaining a secure and resilient environment for all staff, students, and stakeholders. Information security is a shared responsibility, and together we uphold the principles of confidentiality, integrity, and availability of data.

SOAS is committed to:

- protecting information systems against cyber threats through robust security measures, continuous monitoring, and timely system updates
- ensuring personal data is protected by default through secure system design
- providing governance through the IT Governance Group, maintaining an IT risk register and cyber security backlog
- responding swiftly to security incidents and learning from them
- delivering regular training and awareness programmes to strengthen digital resilience

Colleagues are expected to:

- use SOAS accounts and systems responsibly and professionally
- adhere to security policies, including protecting passwords and sensitive information
- respect the privacy of others while recognising that work accounts are owned by SOAS and may, under exceptional circumstances, be accessed with proper authorisation to ensure operational continuity
- promptly report any security incidents or suspicious activity to the IT ServiceDesk
- engage with information security training and stay informed about evolving threats

11. Use of AI Tools

The growing appetite for AI tools and generative AI in the IT sector is undeniable, as these technologies promise to revolutionise various aspects of business operations, from automation to enhanced decision-making capabilities. However, this enthusiasm must be tempered with a vigilant approach to security whilst still encouraging AI innovation. We must ensure that the deployment of AI systems is accompanied by stringent security protocols to safeguard sensitive data against potential breaches.

Therefore, a risk assessment is crucial before adoption or procurement takes place to help identify and anticipate potential failures, biases and security threats. A structured approach ensures compliance with regulations, builds trust across the institution and enhances the overall reliability of AI systems. Any planned or potential use of AI tools requires users to contact their IT Business Partner in the first instance. Continuous monitoring of AI activities, regular updates to security measures, and comprehensive training for personnel are essential to mitigate the risks associated with AI applications.

12. Behaviour

Real world standards of behaviour apply online and on social networking platforms, such as Facebook, Instagram, WeChat, Snapchat, TikTok and Twitter. You must not cause needless offence, concern or annoyance to others. You must also adhere to SOAS' social media policy available at Policies and procedures | SOAS

You must not send spam (unsolicited bulk email).

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

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

13. Collaboration and Communication Tools

Encrypted instant messaging platforms (eg Whats App)
SOAS mandates the use of its own business systems for the conduct of its business and the management of the records created therein.

It is recognised that there will be exceptional circumstances where the use of certain instant messaging platforms may be necessary, including out of hours incident management and emergency communications with students and staff where access to SOAS online systems poses a challenge due to local restrictions or a natural disaster, or other state of emergency.

Microsoft 365 tools
Microsoft 365 (M365) tools are a vital part of the technological ecosystem for both staff and students, providing essential services such as email, document creation, collaboration, and storage. To ensure these tools are used responsibly and effectively, it is important to follow guidelines that promote safe and productive use.

General Principles

- respect: all users must treat each other with respect and professionalism when using M365 tools including the promotion of inclusive language practices (Inclusive language guidance for staff)
- security: users must safeguard their login credentials and not share sensitive information.
- compliance: users must adhere to institutional policies and legal requirements regarding the use of these tools.
- integrity: users should ensure the accuracy of the information they share and avoid the spread of misinformation.

Acceptable Uses

- using email and messaging tools for official communication and academic purposes.
- collaborating on documents and projects using platforms like Microsoft Teams and OneDrive.
- storing academic and professional documents securely using OneDrive.
- participating in online meetings and classes using Microsoft Teams.
- creating presentations, spreadsheets, and written reports using M365 apps like Word, Excel, and PowerPoint.

Unacceptable Uses

- using M365 tools for personal commercial activities or outside business ventures
- sharing passwords or compromising the security of the institution's systems
- sending spam or engaging in phishing activities

Staff need to be aware that any information created during SOAS work activity and stored within the M365 environment, including in users' email accounts and OneDrive, is subject to Freedom of Information (FOI) and Subject Access Requests. This means that information can be requested and may need to be disclosed under legal provisions, emphasising the importance of accurate, respectful and responsible information creation and handling to maintain compliance and protect sensitive information and avoid any untrue or defamatory content.

Email

Professional Communication: Online communication such as email should be written in a professional and courteous manner. Use appropriate language and tone, avoiding slang, jargon, or offensive expressions. Ensure that the content is clear, concise, and relevant to the recipient.

- Confidentiality and Privacy: do not share sensitive or confidential information via email, unless it is encrypted and necessary for official purposes. Respect the privacy of others by not disclosing personal or private information without consent. Use blind carbon copy (BCC) for mass communications to protect recipient privacy

- Use of Teams chat: use Teams chat for quick, real-time, internal team discussions, and email for longer messages, formal updates, or when you need external communication or record-keeping

- Email Management: regularly clean out your inbox to manage storage and improve efficiency. Organise emails into folders and categories for easy retrieval and reference

- Response Time: aim to respond to emails within a reasonable timeframe, typically within 24-48 hours. Set up an out-of-office reply during periods of absence to inform senders of your availability.

- Use of Signatures: include a professional email signature with your name, title, and SOAS affiliation. Avoid using excessive graphics or promotional content in your signature

- Accessibility: ensure that emails are accessible to disabled recipients by using plain text and avoiding complex formatting. Provide alternative contact methods for individuals who may require assistance

14. Monitoring

SOAS reserves the right to monitor email usage to ensure compliance with this policy. Any violations may result in disciplinary action, including suspension or termination of email privileges. Users are encouraged to report any breaches of this policy to the IT department.

SOAS monitors and records the use of its IT facilities for the purposes of:

- protecting the institution from suspicious email and threat activity alerted via our end point detection platform
- the effective and efficient planning and operation of the IT facilities
- detection and prevention of infringement of these regulations
- formal investigation of alleged misconduct
- meeting the University's legal obligations
- supporting the essential business functions of the University.

SOAS will comply with lawful requests for information from government and law enforcement agencies.

You must not attempt to monitor the use of the IT facilities without explicit authority of the CIO

15. Incident Reporting and Response

Anyone who has authorised access to the IT facilities at SOAS is responsible for reporting any IT security incidents and/or service interruptions they encounter. The process is to immediately report to the IT Service Desk providing all relevant details.

Once an IT incident is reported, the IT department follows a structured process to manage and resolve the issue. This process includes:

- immediate response: the IT team quickly assesses the incident to determine its scope and impact. Initial containment measures are implemented to prevent further damage.
- investigation: a thorough investigation is conducted to understand the cause of the incident, identify affected systems, and gather evidence. This may involve forensic analysis and collaboration with external experts.
- communication: regular updates are provided to stakeholders, including the person who reported the incident, affected users, and senior management. Transparent communication ensures everyone is informed about the progress and any required actions.
- resolution and recovery: the IT team works to resolve the incident by removing any threats, restoring affected systems, and ensuring that normal operations are resumed safely.
- review and documentation: after the incident is resolved, a detailed report is prepared, documenting the incident, actions taken, and lessons learned. This helps improve future incident response and prevention strategies
- use official channels: ensure the incident is reported through official communication channels, such as email or the IT Service Desk portal, to ensure it is logged and tracked appropriately.

16. Training & Awareness

Those accessing IT facilities must take proactive steps to stay informed about the latest security threats, training programs and awareness initiatives. This includes any updated mandatory training and guidance covering new policies and cyber security prevention techniques. Additionally, they should familiarize themselves with University's protocols and best practices to mitigate risks associated with cyber threats. By doing so, they contribute to creating a secure and compliant environment that protects sensitive data and supports the overall integrity of the IT infrastructure.

17. Use of Personal Devices

The University permits access to SOAS accounts and data via personal devices but reserves the right to manage this data on such devices.

18. Infringements

Infringing these regulations may result in sanctions under SOAS' disciplinary processes Disciplinary Policy and Procedure (staff) or Student disciplinary procedure | SOAS pdf (students). SOAS has the authority to withdraw IT services due to policy violations, misconduct and/or serious breach of company policy.   SOAS reserves the right to temporarily suspend services during investigations.

Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.
SOAS reserves the right to recover from you any costs incurred as a result of your infringement.

If you become aware of any infringement of these regulations, you must inform the IT Service Desk, or for sensitive issues, a member of the I&T senior management. If you prefer to remain anonymous, you must report the matter through the Whistleblowing procedure, see whistle-blowing-policy.pdf