Policy title:	IT Acceptable Use Policy
Policy owner:	Chief Information Officer
Department:	I&T Directorate
Date approved:	May 2022
Date of review:	May 2024
Approval route:	Executive Board
Circulation:	All staff and students
Publication:	External

IT Acceptable Use Policy

The aim of this policy is to help ensure that SOAS' IT facilities can be used safely, lawfully and equitably.

The issues covered by this policy are complex and you are strongly urged to read the accompanying guidance document, available at https://www.soas.ac.uk/governance//policies. This gives more detailed information that we hope you will find useful.

1 Scope

The policy applies to anyone using the IT facilities (hardware, software, data, network access, third party services, online services or *IT credentials*) provided or arranged by SOAS.

2 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 https://www.soas.ac.uk/admin/governance/policies/

You must abide by the regulations applicable to any other organisation whose services you access such as Jisc.

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. (See accompanying guidance for more detail.)

Breach of any applicable law or third party regulation will be regarded as a breach of this Acceptable Use Policy.

3 Authority

These regulations are issued under the authority of 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 the chair of the IT Governance Group in the first instance or students may invoke the complaints procedure, see https://mysoas.sharepoint.com/directorates/its/btg/icr/Pages/student-complaints.aspx .

4 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.

Use of these facilities for personal activities (provided that it does not infringe any of the regulations, and does not interfere with others' valid use) is permitted, but this is a privilege that may be withdrawn at any point.

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). https://www.chest.ac.uk/user-obligations/ . See the accompanying guidance for further details.

5 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. You must not allow anyone else to use your IT credentials. Nobody has the authority to ask you for your password and you must not disclose it to anyone.

You must not attempt to obtain or use anyone else's credentials.

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

6 Infrastructure

You must not do anything to 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.

7 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 Classification and Information Security policies and guidance, available at https://mysoas.sharepoint.com/directorates/its/Pages/home.aspx , particularly with regard to removable media, mobile and privately owned devices.

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

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/ and must be observed.

8 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 https://www.soas.ac.uk/admin/governance/policies/file104606.pdf

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.

9 Monitoring

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

- The effective and efficient planning and operation of the IT facilities;
- Detection and prevention of infringement of these regulations;
- Investigation of alleged misconduct;
- Meeting the School's legal obligations; and
- Supporting the essential business functions of the School.

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.

10 Infringement

Infringing these regulations may result in sanctions under SOAS' disciplinary processes https://www.soas.ac.uk/hr/procedures/emprel/ (staff) or

https://www.soas.ac.uk/admin/governance/policies/file59817.pdf (students) . Penalties may include withdrawal of services and/or fines. Offending material will be taken down.

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 https://www.soas.ac.uk/admin/governance/policies/file37343.pdf .