IT Acceptable Use Policy

1 Overview

SOAS maintains a wide range of IT services for the use of staff, students and visitors to facilitate the goals of the Institution. These IT assets must be safeguarded, operated and administered in the best interests of the School and its community. This policy outlines the guiding principles that ensure SOAS users stay safe, operate in a legally acceptable manner and that IT facilities are maintained in a cost effective and appropriate way. While the policy strongly acknowledges and supports Academic Freedom, it also ensures that the interests of individuals or sections within SOAS do not override the requirements for provision and continuity of service for the remainder of the School.

2 Academic Freedom As It Pertains To Areas This Policy

SOAS encourages a wide range of academic debate, research and freedom, which might at times run against some of the principals of this policy.

It is not the expectation that this policy should curtail any of the principals for which SOAS stands. However, there will be times when Academic Freedom must be handled in a way that does not introduce risk to the institution.

Where legitimate academic interest requires access to resources that might seem inappropriate the user must find a way to access those resources in a way that does not cause offense or concern to others or risk to the School. In such cases working in locations where such materials cannot be accidently viewed by others might be appropriate. Additionally if the access and storage of materials that might be considered of risk to the IT estate are required, then Information Systems can provide secure facilities for the access of these materials (examples include virtual machines).

3 SOAS IT Resources

IT resources may only be used for the purpose they are intended and in a manner consistent with how they were configured. Only LIS staff, their approved contractors or others with approval from the LIS Assistant Director (Information Systems) or Director of LIS are permitted to change the use or system configuration of SOAS IT services and software. *Note: Users are permitted to change user preferences to suit their working practice or style provided the settings do not compromise security or alter operability for others.*

No user may use a computer system in any way which puts files or information belonging to someone else at risk of damage. In particular, knowingly introducing a computer virus is a serious offence which may result in disciplinary action. Users must also cooperate with LIS in preventative or remedial action concerning equipment and data security. Furthermore the publishing, or communicating (without the authority of either the LIS Assistant Director (Information Systems) or the Director of LIS) any information which allows a third party to breach the security of the IT systems is an offence. Examples include sharing user's passwords or security holes which a user may come across accidentally whilst making legitimate use of the facilities.

3.1 Specific User Requirements

School systems may not be used to create, transmit, store, share or access materials that:

- Contain offensive, obscene, indecent, or menacing images, data, or other material, or any data capable of being resolved into such images or material, except in the case of the use of the facilities for properly supervised research purposes when that use is lawful
- Contain software or materials that can harm the SOAS IT estate (such as viruses)
- Seeks to harm or infringe others' human rights;
- Seeks to harass or bully another individual in contradiction to SOAS' Dignity at Work policy
- Will consume sufficient network or server resource as to impede the effective use of systems by other users;
- Might endanger other user's work or data through data corruption or data loss
- Contain inaccurate or deceiving information;
- Use techniques that capture or otherwise display third party information is such a way as to give the impression that they come from anywhere other than the original source.
- Is likely to incur unwarranted costs on the School;

Note: SOAS also maintains an Email Acceptable use policy that specifically governs the use of Email at SOAS.

No material may display the School logo or name, or otherwise give the impression that they are official School documents, except in accordance with approved SOAS policy.

No material may imply or form a contract on behalf of the School except in accordance with approved SOAS policy.

Personal use of IT systems is acceptable where the consumption of IT resources does not impinge on other operations and where the activities do not contradict this policy or wider SOAS policies.

Trade Union representatives and members may use School systems for School-related Trade Union communications as regulated by the appropriate policy.

SOAS staff should not make use of tools designed to mask their Internet browsing such as the use of the Tor browser without permission from either the Assistant Director (IS) or the Director of LIS.

4 User Access

4.1 User Accounts

Users of the IT systems at SOAS are provided User Accounts to access systems. User accounts are provided for:

The Network defined as:

- A username and password for logging onto the network, email, desktop PCs, Remote Desktop Sessions and single sign on systems

SOAS Systems defined as:

- The software and services SOAS deploys that are not linked into the centrally administered sign on and that have local accounts

All users will be allocated their own User Accounts. The use of shared accounts will be avoided.

It is recognised that some staff share roles and while a user will have their own separate email address, a role based accounts will be provided where needed.

4.2 Rights

Within systems users will be assigned the rights that they need to perform the functions of their role at SOAS. This will include access to file systems, network shares and different online resources. Users should request elevated rights if they need them through the correct channels (typically the IT Service Desk).

4.3 Security

All users are responsible for the protection of their User Accounts. This includes the use of passwords that are sufficiently complex as to not be simply guessed (e.g. the use of upper and lower case characters, the inclusion of numerals and the avoidance of dictionary words). Users should treat their passwords as they would other high security information such as credit cards details.

It is the responsibility of all users to maintain the security of their own passwords and PIN. Any user who fails to take reasonable steps to do so breaches this policy and may be liable for any consequences which follow if another person makes use of one of them.

If, for legitimate operational or training reasons and with the approval of the department manager, a password is divulged to someone else, the password must be changed as soon as possible.

SOAS recognises that is good practice to periodically change a password. SOAS also requires that users who suspect that their password has become known to someone else change it immediately.

A user should not leave a PC logged in unattended where it might allow their account to be used by another individual. No individual should use a PC left logged in by another user without the user whose account is logged into the systems permission.

It is not normally permitted for a user to log in using someone else's user name in order to make use of their file space, to share files or for any other purpose.

A user must login to a shared system only with a user name which he or she has been allocated. Logging in to a machine using someone else's username, password or PIN number is an offence unless it is for legitimate operational or training reasons and with the approval of the department manager.

A manager may consider it necessary to access an absent member of staff's files or email messages in order to maintain continuity of service. Where the absent member of staff's password is not known, LIS should be contacted in order to gain access. For a teacher or expert advisor to take over a terminal session for the purpose of instructing another person in the use of a system or investigating problems is legitimate once the person has logged in. However, procedures should not normally require a user seeking assistance to divulge his or her password to anyone else, including the teacher or advisor.

5 Examining & Accessing Users' Data

SOAS retains logs of user access to the Internet. These logs are kept in a way as to make browsing a user’s Internet history difficult so as to not accidentally reveal a user’s browsing history.

The creation of a readable history of a user’s Internet browsing will be done only where there is a clear operational need.

The Head of ICT and the Assistant Director (IS) and other designated System Administrators are authorised to read any file stored on the system and, if it is necessary to safeguard the integrity of the system, to delete any file without warning. System Administrators have the right to access users’ files and examine network traffic, but only if necessary in pursuit of their role as System Administrators. System Administrators must endeavour to avoid specifically examining the contents of users’ files without proper authorisation (either from the user or the user’s line manager or tutor or Academic Registrar)

6 Removal of Materials

The School reserves the right to remove material from its systems or systems operated on its behalf which it deems to be of a threat to the IT systems. Removal of material may be governed by this policy but where this is not applicable the authority is vested in the LIS Assistant Director (Information Systems) and his authorised deputy.

7 Removal of Computers Or Devices From the Network

The School reserves the right to remove a computer or device from the network where its configuration, operation or current status is shown to present a clear threat to SOAS’ IT. Examples would include a computer or device behaving in a way consistent with a virus infection. SOAS might quarantine or completely remove the devices access o the network until the IT Service Desk can ascertain whether the device is a threat.

8 IT Resources Governed By Other Policies

Software and computer-readable datasets made available on the SOAS network might be subject to the relevant licensing conditions, and, where applicable, to the Code of Conduct published by the Combined Higher Education Software Team ('CHEST'). Users should be cognisant of any restrictions placed upon them and the use of these resources. The IT Service Desk can assist with this

School access to JANET and the Internet is governed by JANET "Acceptable Use" Policy which allows for education, research and institution business. All users must comply with this policy.