Author(s)	Chief Information Officer, Pro-Director Research and Enterprise, Director of Legal and Governance Services and Head of Governance
Owner	Chief Information Officer
Version	2
Date	11th February 2019
Approved By	Executive Board
Date for Review	February 2022

SOAS Email Acceptable Use Policy

1. Introduction

1.1. Email is an essential tool for communication at SOAS. This document sets out policy, procedures and advice for the use of email by SOAS staff, students and other users of SOAS email accounts.

2. Policy Statement

2.1. SOAS provides email and other communications facilities primarily for the conduct of SOAS institutional matters and to support learning and research activities. Individuals will be held personally accountable for their improper use of these facilities and improper use may result in disciplinary action. The rules governing proper and improper usage are outlined in Section 4 of this policy document.

3. Responsibilities

3.1. The Chief Information Officer is responsible for ensuring that a reliable email system is made available for the use of SOAS staff, students and designated other individuals.

3.2. The Head of Service Delivery and Infrastructure is responsible for creating email accounts and overseeing the day-to-day regulation of the email system.

3.3. All users of the SOAS email system are responsible for ensuring that their use of email is in line with this policy and other SOAS regulations, policies and guidelines.

4. Proper and improper Use of Work & Personal Email

4.1. When determining if email has been used in an appropriate manner, the following factors relating to the email will be taken into consideration:

- it does not create a risk of bringing SOAS into disrepute;
- it does not breach staff employment contracts;

- it does not contain material that is defamatory, libellous, harassing, threatening, discriminatory or illegal;
- it does not breach student regulations;
- it does not seek to bully or harass any identifiable individual;
- it is not discriminatory, for example based on gender, ethnicity or religion;
- it is not generally recognised as potentially offensive to others;
- it is not used to impersonate anyone, whether by unauthorised access to an account or by address spoofing;
- it does not breach the terms of the Computer Misuse Act 1990 or other legislation.

4.2. Personal use of SOAS equipment and facilities is a privilege that SOAS reserves the right to withdraw without notice. Reasonable and proportionate use of SOAS email for personal communications is permitted. In establishing whether personal use is acceptable, the additional following criteria will be used as a general rule:

- it does not maliciously interfere with SOAS business or educational operations;
- it does not incite or promote any group activity which may affect operational activities negatively without prior approval by a manager;
- it does not interfere with proper use of SOAS resources;
- it is not a disproportionate use of SOAS resources;
- it does not promote a political or religious ideology.

5. Provision and retention of email accounts

5.1. Members of staff. Staff accounts are created on the basis of a formally logged request at the IT Service Desk for a new email account for new members of staff. The request must be logged by a line manager or approved departmental administrator.

5.1.1. Employees on the payroll will have their accounts linked to their HR/Payroll record and the lifecycle and access provision will be managed in accordance with that record.

5.1.2. Staff not on the payroll (Research Associates, external contractors and others) will have an expiry date applied at the outset. This can be extended via a formally logged request by a line manager or departmental administrator.

5.2. Generic/role accounts. Where a service is being provided it is good practice to establish a generic email account (for example, dataprotection@soas.ac.uk) that can be accessed by more than one member of staff within a service area. Requests for such accounts must be logged via the LIS Service Desk. These accounts are for email use only and must not be used to login to computers or to the network.

5.3. Students. The process of pre-enrolling students with confirmed offers of admission (known as BATE) is an automatic process which triggers the creation of email accounts for all new students (the majority of these being at the start of a session).

5.4. Staff who leave SOAS (resignation, voluntary severance or dismissal). Email accounts will be retained for 3 months after a member of staff has left SOAS. After this point, the account and its contents will be deleted unless the member of staff's line manager or a member of Executive Board logs a request via the LIS Service Desk for the account to be retained for an additional fixed period of time (normally no longer than one month to allow corporate emails to be retrieved). Staff leaving SOAS through resignation, voluntary severance or dismissal do not have the right to request that they retain their email accounts for use after leaving SOAS.

5.5. Retired members of staff. Members of academic staff who are fully retired (in full and immediate receipt of a pension) may apply via the IT Service Desk for their account to be retained in perpetuity for the purposes of Scholarly Communication. If Academic Board has approved Emeritus status, this should be stated in the application as additional rights will obtain.

5.6. Students who leave SOAS and alumni. Email accounts for students will be retained for 3 months after the student has completed the course of study. After this point, notification will be sent and the account and its contents will be deleted. Alumni may choose to use a SOAS "email for life" Alumni account. This will be in the domain @alumni.soas.ac.uk

5.7. Aliases. Individuals are permitted to associate surname-based aliases with their account on a self-service basis. Staff aliases are distinguished by the use of a period as separator - e.g. j.bloggs@soas.ac.uk while student aliases use an underscore - e.g. j_bloggs@soas.ac.uk. These aliases will redirect mail to the associated mailbox. They are not accounts and cannot be used to login to email, the network or for calendar invitations. When the account is closed they automatically cease to function.

5.8. Sending from the Alias. Be aware that, when you send email, it does not automatically send from your alias: you will need to configure this in your email software. If you are subscribed to mailing lists, make sure that the address from which you send matches the address which is registered with the list otherwise your postings are likely to be blocked.

6. Monitoring and access to email

6.1. The Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and Counter-terrorism and Security Act 2015 govern the monitoring of communications including email. Other jurisdictions may also apply (e.g. the Patriot Act in the case of Google email accounts).

6.2 Staff, students and other SOAS email account holders should be aware that all email communications fall under relevant data protection legislation, covered by the School's Data Protection Policy. Individual data subjects have a right of access to personal information held about them which extends to relevant emails. Data subjects may make a Subject Access Request [add hyperlink] through which relevant emails will be sought and disclosed.

6.3. Most monitoring undertaken by SOAS is automated and is aimed at the prevention of viruses, spam, phishing and other threats to the SOAS network that might use email as a route of access. This happens routinely and does not involve any member of staff reading the content of emails or attachments.

6.4. Monitoring of email may also take place to prevent or detect crime or to investigate or detect unauthorised use of email (for example, breaches of this policy). Such monitoring should only apply to use of email for business purposes (in other words, there will be no intentional monitoring of personal emails, except to the extent that they impact on SOAS business).

6.5. If a member of SOAS staff is unavailable (for example, they are away on a sabbatical or long term sick leave), and there is a business reason for accessing their email account (for example, to check that business communications have not been ignored), a member of Executive Board or a Director of a Professional service or the Assistant Director (IS) may provide written authorisation (usually an email) via the LIS Service Desk to grant a named individual (normally the user's line manager) access to the member of staff's email account for business reasons. The named individual must not open any email that appears to be personal.

7. Confidentiality and Email Security

7.1. SOAS staff, researchers and others may from time to time handle information that is confidential or sensitive, for example personal information about members of staff, students or those assisting with research. Users of SOAS email should work on the basis that plain-text email is not private, especially as SOAS email is not hosted on a closed network.

7.2. As a general rule, users should avoid exchanging sensitive personal information via email, or sending any personal information in bulk via email, unless the email and/or its attachment have been encrypted.

7.3. Users should also be aware that individuals have a right of access to information about themselves written in email, which they may exercise through a Data Subject Access request and that email relating to SOAS business may be subject to the Freedom of Information Act.

7.4. Staff wishing to share files that are confidential might opt to use one of the following: • google Drive; • MySOAS; • a Shared Folder location.

7.5. Passwords must not under any circumstances be shared or otherwise disclosed. If an individual believes her or his account security has been compromised she or he must a) change the password immediately, and b) log a call with the Service Desk reporting the compromise.

7.6. In the case of a shared mailbox “role account”, if one member with access leaves SOAS, it is strongly recommended that the shared password be changed for that account.

8. Record keeping

8.1. Email is often used to carry out SOAS business, and emails are important records of that business. SOAS staff must ensure that email is managed in line with the SOAS Records Management Policy.
(https://www.soas.ac.uk/infocomp/recordsmanagement/policy/)

8.2. In particular, emails that record important decisions and transactions must be organised in such a way as to facilitate future retrieval by themselves and colleagues (if necessary by saving them outside the email system) and must be retained in line with the SOAS retention schedule.

9. Email etiquette

9.1. Use email only when it is the most appropriate means of communication. If the subject matter is lengthy or complex, a conversation might be more appropriate.

9.2. Only send emails to those who need to read them to avoid breaches of confidentiality or causing irritation.

9.3. Think before use of the email “CC” field:

- As a sender, are you sure that the recipients on the “CC” line need to see the email?

- If you expect someone to respond to email, you should make sure it is “TO” that person, not “CC”.

9.4. You should not, in general, forward emails to others in cases where you were not the main recipient.

9.5. If you decide to forward an email to others who were not in the original distribution, be careful to read the entire body of the email before pressing “send”: there may be a long string of emails in the message; are you certain that everything in the message is appropriate material to forward?

9.6. Be mindful of the “tone” of your email. Be careful to ensure that you do not use email in a manner which would potentially put you at odds with the Respect at SOAS policy and procedures. Bold or capital letters can be considered shouting and may be experienced as bullying. Some word choices can make an email sound abrupt or contentious.

9.7 Attachments should only be sent via email when absolutely necessary (see Section 7). Minimise the size of files where necessary, for example by using formats such as portable document format (pdf). Be careful, if you do send an attachment, to ensure that it does not contain information that you would not be willing to put into the body of the email as the attachment is no more private than the email itself.

9.8. The School mailing list system provides for a number of automatically generated email groups to aid communication with different types of staff and students. These include: core lists covering cross-departmental, departmental, course, and programme groupings, to which staff and students are automatically subscribed; independently managed discussion lists relating to a project or area of shared interest to which individuals can subscribe. The rules of acceptable use and etiquette apply to use of these lists. In particular, persons authorised to post to the core lists that do not allow for opt in/out should be very careful not to abuse or overuse these channels. Additionally, independent lists may apply their own rules of conduct to which subscribers should adhere.

9.9. The use of all staff and all student e-mails is restricted and managed by the communications team. If you judge that an all staff or an all student email is needed for an item of SOAS activity, please contact comms@soas.ac.uk who will advise on best communications approaches.

9.10. Where it is necessary to send an email to large number of individuals not using the mailing list system (especially where recipients are outside of SOAS) remember to place email addresses in the “BCC” field so that recipients will not be able to see other recipients’ email addresses. Not doing so is a potential breach of their privacy.

Note that, depending on email software in use, the BCC'd recipients' addresses may be visible to each other, even while concealed from the primary recipients.

9.11. Email signatures (text which is automatically appended to the bottom of an email) should be used to convey useful information, typically • • • SOAS, University of London • Russell Square • London WC1H 0XG • • http://www.soas.ac.uk • Extraneous information should not be placed in email signatures.

9.12. Be aware that, if you use multiple devices for your email (e.g. the Google web interface, Outlook, Applemail, Thunderbird, an iPhone, iPad, Android phone or Tablet), you will need to set up your signature on each device if you want your emails to be consistent regardless of how you send them.

10. Breach of policy

Users of SOAS email accounts and others who breach this email policy may be subject to disciplinary action under the relevant disciplinary procedure (staff or students).

11. Review of policy

This policy will be reviewed regularly and, in any case, at least every 4 years.

12. Relevant legislation and standards

• GDPR 2018
• Regulation of Investigatory Powers Act 2000
• Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
• The Employment Practices Code of Practice, Information Commissioner's Office, 2011
• The Counter Terrorism and Security Act.