

London School of Economics & Political Science

IT Services

Policy

Electronic Messaging Policy

Jethro Perkins
Information Security Manager

Summary	This document outlines LSE's approach to using email and other electronic messaging systems provided by or used on behalf of LSE.
Version	Release 1.3
Date	28/06/13
Library reference	ISM-PY-102

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Information Security Policy	3	12/03/13	Jethro Perkins
Information Classification Standard	3	12/03/13	Jethro Perkins
Policy and Guidance on the Use of Social Media for Staff	1.0	07/06/12	
Monitoring and Logging Policy	1.2	18/06/13	Jethro Perkins

Version history

Date	Version	Comments
04/03/13	0.1	Initial version
23/04/13	1.0	Released to ISAB
07/05/13	1.1	Amendments following ISAB
18/06/13	1.2	Amendments following comments by MB
25/06/13	1.3	Amendments following meeting with HR (Steve Harris and Rob Butler)

Review control

Reviewer	Section	Comments	Actions agreed
ISAB	3.3.2	Request to incorporate a paragraph about ownership and responsibilities around shared mailboxes.	Section updated
ISAB	3.5	Request to emphasise that LSE email is provided for business use	Section updated
Mike Bragg	3.3.2	Concern that the policy as it stands may lead to line managers having access to mailboxes of staff who may have raised a grievance, and that the de-allocation of access rights may not happen.	Insertion of phrase “subject to a written request to the Information Security Manager,” to ensure access is not automatically granted. Further consultation to be held with HR.
HR (Steve Harris and Rob Butler)	3.3.2	Subject to agreement of Information Security Manager, line managers can request access to mailbox of staff who have left for up to 30 days	Section updated

HR (Steve Harris and Rob Butler)	3.7	<ol style="list-style-type: none">1. Any mailboxes existing outside references of employment / study tenure must be reconfirmed annually2. Any LSE-owned mobile devices will be wiped at the end of employment3. Mailboxes not logged into for period of 1 year will be disabled. If no request for re-enablement within 3 months, they will be permanently deleted.	Section updated
-------------------------------------	-----	--	-----------------

Table of contents

1 Introduction	5
1.1 Purpose	5
1.2 Scope	5
2 Responsibilities.....	6
3 Policy.....	7
3.1 Accessing LSE Email	7
3.2 Sending and receiving information.....	7
3.3 Email Security	7
3.3.1 Usernames and Passwords.....	7
3.3.2 Access to other people's personal mailboxes	7
3.3.3 Shared email accounts	7
3.3.4 Confidentiality and Privacy	8
3.3.5 Data Breaches through Email.....	8
3.4 Spam, Viruses and Phishing	8
3.5 Appropriate use of LSE Email Systems	8
3.6 Privacy.....	9
3.7 Mailbox termination	9
3.8 Further Policies, Codes of Practice, Procedures and Guidelines	9
3.9 Review and Development	10
4 APPENDIX A: Suspended Accounts	11
4.1 SUSPENDED ACCOUNTS.....	11
4.2 Compromised email accounts	11
5 Appendix B: Generic mailbox creation.....	13
5.1 Generic Mailbox creation process	13
5.2 Additional Information.....	13
6 Appendix C: Account Extensions	14
6.1 Extending user and email accounts beyond the end of an employment contract (retirement / different job)	14
6.2 Emeritus staff	14
6.3 Departmental servers and services.....	14
6.4 Non-departmental generic mailboxes	14

1 Introduction

This policy sets out the proper use of email and other electronic messaging systems, whether provided by or used on behalf of LSE. Further information is laid out in the 'Conditions of Use of IT Facilities at LSE,' the 'Information Security Policy' and other supporting policies.

1.1 Purpose

The primary purpose of this policy is to:

1. Ensure all users are aware of their responsibilities when using LSE email or other electronic messaging systems on behalf of LSE or as representatives of LSE.

1.2 Scope

This policy covers all electronic messaging utilized by authorised LSE users.

The primary means of electronic messaging provided by LSE for its staff and students is currently Microsoft Exchange email. LSE is planning to outsource provision to Microsoft's O365 service.

Forms of electronic messaging not provided by LSE, but used on its behalf, such as LSE Facebook and Twitter accounts, are also covered by this policy. Use of social media accounts on behalf of LSE must also conform to LSE's ['Policy and Guidance on the use of Social Media for Staff'](#).

2 Responsibilities

Members of LSE:

All members of LSE, LSE associates, agency staff working for LSE, and alumni may have LSE email accounts for which they are responsible.

Appointed staff may also have access to social media or other electronic messaging facilities used on behalf of LSE, the security and content of which are their responsibility.

Department of Information Management and Technology:

Responsible for administering LSE's email systems, suspending and re-activating accounts that have sent out spam or otherwise been compromised, submitting spam and other malicious email to LSE's mail gateway services.

Information Security Manager:

Responsible for interviewing staff unaware of how their account was compromised, and authorising re-activation.

Communications (External Relations Division)

Responsible for LSE Blogging Service.

Information Security Advisory Board

Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

Information Technology Committee

Responsible for approving information security policies.

3 Policy

3.1 Accessing LSE Email

LSE email accounts are given to staff, students and alumni, all of whom will have signed the '[Conditions of Use of IT Facilities at LSE](#)', which provides information about how LSE IT systems and services can be used.

LSE email systems can be accessed from LSE workstations, external computers and other mobile devices (such as smart phones and tablets). Access is only controlled by single-factor authentication (the possession of 'something you know' – a username and password) and is available anywhere on almost any device.

This may have implications for the transmission of any information LSE would classify as 'Confidential' – please see the Information Classification Standard for information on data classification and appropriate measures to take for 'Confidential' information.

3.2 Sending and receiving information

The Department of Information Management and Technology (IMT) recommends that all material sent from, received by, uploaded to or downloaded from LSE email servers or other third party applications must be handled in a manner appropriate to its information classification.

Please refer to the [Information Classification Standard](#) for guidance.

Payment Card Industry data (credit/debit card numbers or other account details) must not be sent by email.

3.3 Email Security

3.3.1 Usernames and Passwords

Usernames and passwords are for individual use only, and must not normally be disclosed to third parties, whether within or outside LSE.

Any user knowing or believing that they have disclosed their account details, or who knows or suspects that their email account has been compromised, must contact the IT Services Desk (staff and postgraduate researchers) or IT Help Desk (undergraduates and taught postgraduates) immediately in order to outline the situation.

In order to maintain the confidentiality, integrity and availability of LSE systems and services, and also to ensure that LSE is not blacklisted by Internet Service Providers and data carriers, or has its internet access removed by its own service provider, JANET, compromised email and user accounts will be dealt with in a uniform manner, the details of which are available in Appendix A. There will be no exceptions.

3.3.2 Access to other people's personal mailboxes

Requests for access to another user's personal mailbox (as distinguished from any resource mailboxes a person may have access to) must be made in writing using the *Request for Access to Another User's Data* form

(<http://www2.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/reqForAccToAnoUsePerDat.pdf>)

Where a person has left employment with LSE, that person's line manager shall, subject to a written request to the Information Security Manager and the Information Security Manager's written consent, be granted access to that person's mailbox for up to 30 days after the leaving date. Beyond 30 days, the mailbox shall be terminated.

3.3.3 Shared email accounts

There may be some legacy generic email accounts where a single username and password for the mailbox are shared by a number of people, in which case the logon details should not be distributed beyond those people who need access.

Shared mailboxes and resource mailboxes (for example: academic_subject@lse.ac.uk) should not be used to convey personal information, and are not exclusive to the people who currently have access. The Group / Departmental Manager has the right to view the contents and appoint different people to view it at any time.

3.3.4 Confidentiality and Privacy

Email, social network sites and other forms of electronic communication are considered an inherently insecure method of communication. There is no guarantee that the recipient of a message is in fact genuine, nor is there any guarantee that the sender of a message is genuine. IMT advises that data classified as Confidential should not normally be sent by email unless additional measures are taken (such as sending the data to be transmitted in an encrypted attachment – see LSE's [Encryption Guidelines](#) for further information)

Once a message has been "SENT", recipients may intentionally or accidentally forward the message to other individuals. Therefore users of electronic messaging should have no expectation that any electronic message will remain private.

3.3.5 Data Breaches through Email

Any data breaches caused via email will be handled in accordance with all relevant School policies, including the [Conditions of Use of IT Facilities at the LSE](#).

3.4 Spam, Viruses and Phishing

LSE has spam filters and anti-virus filters at our email gateways. These filters are there to protect LSE's information systems resources from viruses and unsolicited email. Whilst these filters are constantly updated we cannot guarantee that they will provide 100% protection against all viruses, phishing attempts and spam. If any users feel that they are receiving excessive amounts of unsolicited email or are being caused distress by the receipt of offensive email they may contact the IT Service Desk for further guidance.

Phishing emails are attempts to persuade users to impart their user account details to scammers, who will then use the account to send out large quantities of spam. LSE provides advice on how to avoid responding to phishing at

<http://www2.lse.ac.uk/intranet/LSEServices/itservices/infosec/phishingAdvice.aspx>

3.5 Appropriate use of LSE Email Systems

The use of LSE-provided email or any other electronic messaging system provided by or used on behalf of LSE is subject to all relevant laws, policies, codes of practice and guidelines. All users must comply with LSE's [Information Security Policy](#), the [Information Classification Standard](#) and the [Conditions of Use for IT Facilities at LSE](#).

LSE email is provided for conducting School business, and while individuals may use their personal accounts for personal communication, the account remains the property of the School, and any communication using it should not be considered private. LSE email is subject to the monitoring conditions laid out in *Section 3.6* below, and also the *Monitoring and Logging Policy*.

Official LSE business should normally be conducted from email accounts provided by or on behalf of LSE. Although it is recognised that this might be necessary in some exceptional circumstances, users should be also be aware that the use of third-party email providers for LSE work may breach contractual, legislative, ethical and policy requirements.

Users of email or other third party supplied electronic messaging used on behalf of LSE:

- must not send messages or message content that may harass or offend (including racist, sexist, defamatory or obscene material).

- must not send messages from someone else's account except under proper "delegate" and "send on behalf of" arrangements which retain individual accountability.
- must not use LSE email or messaging systems operated on behalf of LSE for personal gain or profit.
- must not use LSE email or messaging systems operated on behalf of to represent themselves as someone else.

3.6 Privacy

Under the terms of this policy no person shall monitor another user's email account unless written authorisation has been granted to do so, or access has otherwise been granted under section 3.3.2. The monitoring and or inspection of email accounts may only occur in accordance the *Information Security Policy* and the *Monitoring and Logging Policy*.

LSE, in accordance with its legal and audit obligations, and for legitimate operational purposes, reserves the right to access and disclose the contents of users' email messages. LSE also reserves the right to demand where necessary the disclosure of decryption keys so that it may fulfil its right of access to users' email messages in such circumstances. LSE also reserves the right to monitor or disclose details from users' email accounts where necessary in line with the Regulation of Investigatory Powers Act (RIPA) 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Digital Economy Act 2010 and the Terrorism Act 2006.

3.7 Mailbox termination

Staff mailboxes will be disabled at the point of termination of the staff member's employment.

Student mailboxes will be terminated at the end of the term after the student course has finished.

Alumni and other mailboxes that continue to exist after a person's tenure of study or employment shall be marked for review and re-conformation annually.

LSE-owned mobile devices which are used to connect to LSE-provided mailboxes or which contain data owned by or held by LSE will be wiped at the termination of a staff member's employment.

Mailboxes not logged into or utilized for a period of one year will be disabled. If no request is received within a further three months requesting their re-enablement, they will be permanently deleted.

3.8 Further Policies, Codes of Practice, Procedures and Guidelines

This policy sits beneath LSE's overarching [Information Security Policy](#). Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on LSE's website. All staff, students and any third parties authorised to access LSE's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

The below list of current policies is in no way authoritative and new policies will be published on the LSE website as they become available.

Associated policies:

[Information Security Policy](#)
[Conditions of Use of IT Facilities at LSE](#)
[Conditions of use of the residences network](#)
[Password Policy](#)
[Asset Management Policy](#)
[Monitoring and Logging Policy](#)
Data Protection Policy

Standards and Guidelines:

[Information Classification Standard](#)
[Encryption Guidelines](#)
[Remote and Mobile Working Guidelines](#)
[Guidelines on the use of Cloud storage](#)

3.9 Review and Development

This policy shall be reviewed and updated regularly by the Information Security Advisory Board (ISAB) and an auditor external to IT Services as appropriate to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.

4 APPENDIX A: Suspended Accounts

4.1 SUSPENDED ACCOUNTS

LSE mailboxes are prohibited from sending a large number of emails in short succession. Any attempt to send large quantities of emails will lead to the account becoming blocked from sending email.

Members of the Systems Team within IMT are warned by LSE's mail gateway provider when an account is suspended.

In order to get the account re-enabled, the user will have to contact IMT to discuss what happened.

In the event that the attempt to send out large numbers of messages was caused by a compromised account, the process for handling Compromised email accounts (Section 4.2 below) shall be followed by IMT.

4.2 Compromised email accounts

If any user account is discovered to have been compromised and used to send out spam, phishing emails or other malicious content, IMT will perform the following actions:

1. The account will be disabled and the password changed. This is to protect:
 - a. The LSE from reputational damage, censure from its internet service provider, damage to its mail servers and service, and potentially being blocked from accessing some networks
 - b. Reputational damage to the owner of the compromised email account, including potentially being permanently blocked by third parties from sending email to their mail servers
2. If the issue has not been raised by the Service Desk (for staff) or Helpdesk (for students), it will be recorded in Supportworks by the Information Security Manager, the Information Security team or any member of the Systems Team and dropped in the relevant service desk queue for notification.
3. Email sending from the account will have been automatically disabled by Symantec MessageLabs (LSE's mail gateway provider) after 700 messages sent in under one minute or a bulk mailout of over 700 messages
4. Upon the user contacting the service desk, they will be asked if they know how their account was compromised.
 - a. If they know, they will be asked to re-read and re-sign the 'Conditions of Use', to perform a full anti-virus scan on any personal devices, make sure all software is up to date, and be invited to read our website information on phishing (<http://www2.lse.ac.uk/intranet/LSEServices/itservices/infosec/phishingAdvice.aspx>)
 - b. If they don't know, they must book an appointment to speak to the Information Security Officer or, in her absence, the Information Security Manager, in order to try to ascertain what happened and make further recommendations.
5. Upon a satisfactory conclusion to point 4, the Information Security Officer or Information Security Manager will request that Systems Team re-enable the account
6. When we have satisfied Symantec's conditions of investigation into the breach, we can then ask for the account to be re-enabled on the mail gateway (this may take several hours to come into effect)
 - a. Symantec's conditions:
 - i. Was a detailed virus scan of all machines on your network completed?
 - ii. Were any machines found to be infected?
 - iii. Did the user in question respond to an email with their user credentials?
 - iv. Did they follow a link requesting their user credentials?
 - v. Has the password for this user been changed, and is this a strong password which could not be easily guessed?
 - vi. Please confirm the user cannot re-use any of their previously used passwords.

- vii. Has the user been educated to not reply to emails asking for usernames and passwords?
- viii. Have any other users responded to similar emails?
- ix. Please provide a copy of the phishing mail received by the user so we can add detection for it.
- x. Have you read our best practice guidelines located at <http://www.symantec.com/connect/blogs/webmail-security-and-associated-best-practices>?

5 Appendix B: Generic mailbox creation

5.1 Generic Mailbox creation process

1. A request for a generic mailbox must come from a Departmental Manager / Group Manager / Centre Manager and be put into SupportWorks.
 - a. This is to make sure that the request has proper approval, and that the DM has oversight of generic mailboxes operating in her / his department and who has ownership of them.
 - b. It is especially important in the case that a mailbox gets hacked or 'Confidential' data is leaked through a generic mailbox address.
2. In order for IMT to be able to correctly process the request, it must contain the following information:
 - a. The named contact for the mailbox
 - b. The requested email address which should
 - i. start with the departmental prefix (in order that, in the case of a hacked or abused account, it can be easily identified)
 - ii. or contains the year if the address relates to a conference
 - c. Who requires access and what type of access (full control / send on behalf of / read)
 - d. When or if the mailbox will expire
3. IMT ensures the DM and the named contact are made aware that:
 - a. Only users with LSE ITS accounts will be able to access the mailbox.
 - b. The mailbox will need to be renewed on an annual basis
4. Once step 3 has been completed a custom mailbox is created using ITS Reg Screen under the named contact's record
5. A security group is set up in active directory.
6. Once all of the information in steps 1 and 2 has been confirmed with the DM and the user and the email format has been agreed the call is passed to Systems including the
 - a. security group
 - b. mailbox account username
 - c. mailbox name
 - d. names of any additional people requiring access
7. Systems set up the relevant permissions
8. Once the call comes back the user is informed the mailbox is ready and given details on how to set it up in Outlook.

5.2 Additional Information

1. IMT staff should never issue passwords for direct access to a generic account. Access must be via permissions granted to a named personal account only.
2. Occasionally it transpires that a generic account is being logged into directly. When this issue is brought to IMT's attention, IMT will contact the DM requesting the appropriate access rights, set up the individual users with proper Security Group-based access permissions as quickly as possible, and the password on the generic account will be changed.
3. Any exceptions to the departmental prefix must be explicitly justified by the DM.
4. If a non LSE user requires access then they must apply for an LSE account, with sponsorship from a DM. The DM will be responsible for tracking down the user in the event of account misuse.

6 Appendix C: Account Extensions

6.1 Extending user and email accounts beyond the end of an employment contract (retirement / different job)

1. By default, when a member of staff's employment is terminated, their user and email accounts will be closed immediately.
2. If a member of staff needs to retain their LSE email address for a period of time after completing employment at LSE, they should in the first instance raise this with their Departmental Manager / Group Manager / Centre Manager
3. If the DM agrees to the request, the DM should raise the request via the IT Service Desk.
 - a. It is important to note that the retention of an LSE user account and email address means that the person with the account will continue, in effect, to represent LSE
4. In line with other accounts used by non-employees or students, the extended account will be set to expire every year, and the DM will have to request any extension on the account user's behalf.
 - a. This ensures that any unused accounts are closed and the storage resources can be re-used
 - b. It also helps to ensure that LSE's vulnerability to hacking and / or abuse of unused accounts is reduced
5. Any generic accounts for which the user was the named contact must be reassigned to an acting member of staff. This is to ensure that the administration and responsibility for generic accounts and their content actively remains within LSE, in case of hacking, data leakage or account abuse. The authorisation for a new contact should come from the DM.

6.2 Emeritus staff

1. Formal sponsorship of a staff member becoming emeritus needs to be made by the relevant Departmental / Group / Centre Manager, requesting the account be maintained as an emeritus account via the IT Service Desk.
2. The account will need to be renewed annually, with the request being made on the emeritus member's behalf by the relevant Departmental / Group / Centre Manager. This ensures that the relevant department are aware and happy for the emeritus staff to be representing LSE and doing work on LSE's behalf.
3. Any generic accounts for which the user was the named contact must be reassigned to an acting member of staff. This is to ensure that the administration and responsibility for generic accounts and their content actively remains within LSE, in case of hacking, data leakage or account abuse. The authorisation for a new contact should come from the DM.

6.3 Departmental servers and services

If the user whose account is to be extended beyond employment has any access to departmental servers or departmentally-provided IT services, any continued access to these resources is the responsibility of the DM

Access to other resources e.g. Web CMS authoring, departmental or School file shares, will be removed by default, and any access would only be retained by explicit DM request.

6.4 Non-departmental generic mailboxes

Any non-departmental mailboxes for which the user was the named contact, such as union or society accounts, become the responsibility of the union / society / service to appoint someone currently employed by LSE to look after them. As above, this is to ensure responsibility lies within LSE in case of hacking, data leakage or account abuse.