LSHTM Information Management and Security Policy

Supporting policy 3: Use of email

Endorsed by Academic Affairs - Feb 2014

1 Introduction

This policy exists to ensure that electronic mail systems provided by the London School of Hygiene & Tropical Medicine are used in accordance with the aims and objectives of the School.

2 Scope

This policy has the scope defined in the main Information Management and Security Policy and includes any School system, any use of email services from School facilities and any email service provided, by a third party, on behalf of the School.

3 Appropriate use of email systems

Use of email services is subject to all the same laws, policies, and codes of practice that apply to the use of other means of communications, such as telephones and paper records, and shall comply with the LSHTM Acceptable Use Policy.

3.1 All members of staff must, wherever possible, use School-provided email systems for conducting School business.

3.2 All students should use School-provided email systems for School work.

3.3 Users may not use LSHTM-provided email services and/or facilities to transmit:

- commercial material unrelated to the legitimate educational business of the School, including the transmission of bulk email advertising (spamming);
- bulk non-commercial email which is likely to cause offence or inconvenience to those receiving it. This includes the use of email listservers at LSHTM and elsewhere, where the email sent is unrelated to the stated purpose for which the relevant email list is to be used (spamming);
- electronic chain letters - unsolicited email messages requesting other users, at LSHTM or elsewhere, to continue forwarding such email messages to others, where those email messages have no educational or informational purpose;

- email messages which purport to come from an individual other than the user actually sending the message, or with forged addresses (spoofing);
- email messages which misrepresent the sender's role in the School;
- material which is offensive or inappropriate;
- material that incites criminal activity, or which may otherwise damage the School's research, teaching, and commercial activities, in the UK or abroad;
- material to which a third party holds an intellectual property right, without the express written permission of the rightsholder or the material is otherwise covered by the School's copyright policy;
- material that is defamatory, libelous, harassing, threatening, discriminatory or illegal ;
- material that could be used in order to breach computer security, or to facilitate unauthorized entry into computer systems;
- material that is likely to prejudice or seriously to impede the course of justice in UK criminal or civil proceedings;
- messages that could imply the creation of an order or contract, between LSHTM and another organisation, contrary to the School's Financial Regulations.

3.4 Caution should be exercised when drafting email which references personal data. Encryption may be used to ensure confidentiality, but if there is any uncertainty about such email, advice should be sought from the Head of IT Security, IT Audit and Compliance.

3.5 Whilst the School provides staff with access to email systems for the conduct of School-related business, incidental and occasional personal use of email is permitted so long as such use does not disrupt or distract the individual from the conduct of LSHTM business (i.e. due to volume, frequency or time expended) or restrict the use of those systems for other legitimate users. (See definition of reasonable personal use in the Acceptable Use Policy.)

3.6 Users must not knowingly allow anyone else to send email using their individual accounts. Users will be deemed liable for any email or activity from their accounts. If you need to send email on behalf of others, please contact the ITS helpdesk for advice.

4 Email Servers

All email servers must be registered with ITS in order to be able to send outgoing external email or receive incoming external email. Such servers must not act as open relays nor may they run open proxies.

5 Viruses

All reasonable steps must be taken to prevent the propagation of computer viruses by email.

Incoming and outgoing email must be routed via central mail hubs (including any such services operated by third parties on behalf of the School) which must run adequate virus detection software.

All user equipment (desktops, laptops, mobile phones) should have anti-virus software installed and both systems and software kept up to date.

6 Penalties for Improper Use of Email Services

Failure to comply with this email policy could result in access to the service being withdrawn or, in more serious cases, to disciplinary action being taken, and/or civil action, and/or criminal prosecution. In determining whether email messages are in breach of this policy, managers may seek advice from the Director of IT Services.

7 Privacy and Security

7.1 Email, like all methods of communication, cannot be assumed to be secure. It cannot be assumed that email will be correctly delivered or that the sender is as claimed in the mail headers. Steps must be taken to minimise the risk of interception or breaches of confidentiality. These steps include:

- not divulging your user passwords to anyone (including in email)
- not knowingly allowing anyone else to send email from your account

You should also consider the following guidelines when sending email:

- ensuring that you identify and use the correct recipient email address
- considering anonymising references to specific individuals
- confirming the identity of an email sender where there is reason to question this
- adopting a risk-based approach to deciding what information is appropriate to be sent by email.

Where an issue is particularly sensitive or confidential, email is unlikely to be a sufficiently secure method of communication and should be avoided.

7.2 Users should be aware that deletion of an email message by both sender and receiver does not mean that the message no longer exists on their systems or on the systems through which it passed. Conversely, when a message has been transmitted, it is not necessarily the case that a record of it will exist or be accessible.

7.3 Any business message must be retained in accordance with the School Records Management Policy. The School Archivist and Records Manager shall issue guidance on how to interpret those policies.

7.4 Users may not, under any circumstances, monitor, intercept or browse other users' email messages.

The School reserves the right to inspect, copy and/or remove user data in order to investigate operational problems or for the detection and investigation of suspected misuse. This includes the authorized interception and monitoring of communications as provided for by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under the Regulation of Investigatory Powers Act 2000.

For example, monitoring of user accounts might occur if the School has reason to believe that its computer facilities were being misused to send unsolicited commercial emails.

Any monitoring of LSHTM systems and networks may be carried out **only** in accordance with the LSHTM Policy on Monitoring Computer and Network Use.

The School reserves the right to access and disclose the contents of a user's email messages, in accordance with its legal and audit obligations, and for legitimate operational purposes. The School reserves the right to demand that encryption keys, where used, be made available so that it is able to fulfill its right of access to a user's email messages in such circumstances.

For the avoidance of doubt, this section does not preclude third parties who operate services on behalf of the School from carrying out lawful monitoring and disclosure on their systems and networks.

7.5 All user equipment holding, or providing access to, mail messages, email addresses or any other confidential material must be password protected.

8 Status of this document

This document is a part of LSHTM's information security policy and has been approved by Senior Leadership Team/Academic Affairs Committee. It is subject to regular review.