University of Northampton
Working in partnership with

LONDON SCHOOL OF BUSINESS AND MANAGEMENT

Email Acceptable Use Policy

Index

Document Version Control

Document Version	Committee	Committee Action	Date
v1.0	SMLT	Approved by Chair's Action	29 May 2016
		Date in force	**1 June 2016**
v2.0	SMLT	Approved by Chair's Action	15 September 2017
		Date in force	**15 September 2017**

This Email Acceptable Use Policy will be reviewed annually by the IT Manager. Any amendments require the approval of the Senior Management and Leadership Team (SMLT).

1. Introduction

Email is one of our key mechanisms for communication. In many cases it is becoming the default means of communication reducing the cost and environmental impact of paper-based communications.

This Email Acceptable Use Policy applies to all staff (including temporary staff), Student Guild, visitors, contractors, and students using the London School of Business and Management (LSBM) IT facilities and resources. Those using the IT facilities and resources provided by Birkbeck College under the terms of our arrangement with Birkbeck College are expected to abide by the latter's IT policies whilst on their premises.

This policy should be read in conjunction with our other institutional policies (including our Internet: Acceptable Use Policy) and UK and international law. See Appendix A for details of the UK legislative framework within which we operate. Please note that the contents of this policy are not intended to contradict or contravene UK or international law.

The purpose of this policy is to set out acceptable use of email by our students, staff, visitors and contractors. It is intended to:

- ensure that the content of any email communication does not constitute a breach of any institutional policies or the legislative framework within which we operate.
- ensure that any message has a high chance of delivery, thereby improving the chances of it being read, while reducing the inconvenience to users.
- reduce the likelihood of outgoing email being regarded as Spam by recipient systems.
- eliminate problems or complaints regarding the service.

2. Principles

The following guidelines draw upon research into best practice in the area and the guidelines offered by the large providers, including Google, Hotmail, Yahoo and AOL. The guidelines should be followed in order to ensure compliance with LSBM policies and the legislative framework within which we operate including compliance with our Prevent Duty. They should also be read in conjunction with our House Style Guidelines.

3. Information regarding Staff

Use of email by staff is permitted and encouraged where such use is suitable for business purposes and supports our goals and objectives. Email is to be used in a manner that is consistent with our standards of business conduct and as part of the normal execution of an employee's job responsibility.

LSBM email accounts are to be used for LSBM business and email messages are treated as potential LSBM corporate messages. Limited personal use is considered acceptable. LSBM may directly access staff email accounts in the pursuit of an appropriately authorised legal or disciplinary investigation.

The introduction of the Student Self-service Portal (SSP) allows students to maintain their own contact details (this could be an LSBM-based email account or the student's personal email address). It is important that all our staff use this student contact email information for all email correspondence with the students.

LSBM reserves the right to redirect the email of staff that have left for legitimate business purposes. For more information please refer to Staff Departures: IT Procedures. Use of email may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.

Staff should be conscious that anything they write in an email relating to LSBM business may be subject to disclosure under the Freedom of Information Act 2000 or Data Protection Act 1998.

Staff must set up an out of office reply if they are going to be away from work for any length of time.

4. Information regarding students

New students will be automatically allocated LSBM mailboxes, and their personal contact email address will be collected during the admissions process. Students must be informed of the purposes for which their email address will be used, and informed of the "no publicity" flag, which will be used to reduce offence caused by Unsolicited Bulk Email (Spam).

Students are responsible for maintaining their contact email address via SSP. This needs to be communicated to all students. All our students will, in any case, be asked to confirm/update their contact email address as part of the annual on-line re-enrolment process.

No messages should be sent from anonymous email addresses, or invite a response to an unmonitored mailbox.

Use of multiple addresses for the same student is not permitted.

5. Email lists

Email lists based upon set criteria (e.g. a list of all HND students or Degree students) can be created within our student management system and shared among the relevant staff. Sending to the distribution list can be restricted if needed. This facility is ideal for large recipient groups, and where periodic messages are being sent to the same groups of recipients. Additional distribution lists may be requested from IT Services.

A number of staff distribution lists are available through our email system and the Divisional and Departmental Heads are responsible for updating these distribution groups regularly. This facility is suitable for messages sent to recipients numbering up to a few hundred, but limitations in the email client may restrict larger recipient lists, and a distribution list should be used.

A copy of students' contact information is held within the VLE. Staff and students using the VLE may send to selected students or groups.

6. Specific guidelines for use

6.1 General

- Staff and students are expected to check their LSBM email accounts on a regular basis.
- Our email etiquette is that we do not send emails outside of 8am to 8pm Monday to Fridays and, wherever possible, refrain from emailing at weekends.
- Staff responses to staff emails should be within 24 hours [the response can be just a 'holding reply'].
- Staff responses to student emails should be within 48 hours [the response can be just a 'holding reply'].
- Be careful not to prevent the transmission of viruses by not opening attachments received from unsolicited sources.

- Ensure your terminal is locked or logged out when you leave your desk; a malicious user could send messages in your name.
- An email will only be deemed confidential if it is labelled as such.
- Never reply to spam.
- Do not send any scripts and avoid HTML emails if possible.
- Do not use an old email to initiate a new email exchange because the subject in the title box will be misleading later.
- Be careful when replying to emails previously sent to a group. With such emails it may not always be appropriate to “Reply All”.
- Archive effectively - use folders and delete any messages no longer needed.
- Do not overuse the "URGENT" flag as it will lose its value.
- Avoid using email for sensitive or emotional messages.

6.2 Content of the message

- Take care in drafting emails, taking into account any form of discrimination or harassment, LSBM representation, data protection issues and the legislative framework within which we operate.
- Draft emails with the same care as letters as staff emails are a form of corporate communication.
- Re-read messages before sending to check for clarity and to make sure that they contain nothing which will embarrass the organisation or make it liable.
- The email must be relevant to the recipients.
- Where appropriate, emails from staff to students should be personalised if possible.
- Chain messages should never be forwarded.
- Subject lines must accurately describe content.
- Recipients should never ask for personal information or passwords in email.
- Avoid the use of ‘PS’ or the inclusion of additional information after the end of the main body of the email. Such text can often be overlooked by the reader, especially if the reader suffers from any visual impairment.
- Great care should be used when linking to HTTP URLs, which should not link to IP addresses or non-standard ports.
- Messages should include an email “signature” with sender and institutional contact details. The signature must follow institutional guidelines.
- Avoid images in email where possible – include ALT tags on all images that are sent.
- Send mail in plain text format where possible.

- Use file compression techniques for large documents or send them using an alternative method.

6.3 Email addresses and addressees

- The email addresses of other recipients should never be revealed.
- Use only LSBM addresses in the “From:” and “Reply-to:” header addresses. They must be valid addresses capable of receiving email.
- Use shared mailboxes if appropriate, rather than individuals’ addresses for sending email.
- Understand how to use CC and BCC: only CC in people that really need to receive the email.
- When permission from all within the group has not been received for their email addresses to be viewed by other members within the group, use BCC.

6.4 Bulk emails

- Use distribution email lists where possible.
- Avoid 'Mail Storms' - long discussions sent to a distribution list - consider verbal communication or use a bulletin board.
- In case of sending bulk emails, keep all the recipients email addresses in BCC.
- Bulk email should be tailored and targeted to smaller groups of recipients where possible.

6.5 Unacceptable use or behaviour

It is unacceptable to:

- Solicit emails that are unrelated to business activities or are for personal gain.
- Send or receive any material that is obscene or defamatory, or which is intended to annoy, harass or intimidate another person.
- Send or receive any material that is linked to a proscribed terrorist organisation or information that generally promotes or incites acts of violence or terrorism.
- Represent personal opinions as those of the institution.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the institution, or the institution itself.
- Reveal or publicise confidential or proprietary information which includes, but is not limited to financial information, databases and the information contained therein, computer network access codes, student information and business relationships.

7. Dealing with complaints

- Complaints relating to non-delivery of messages will be investigated by the IT Services team, but are limited to establishing whether the recipient mail servers accepted the message.

- The relevant member of staff should respond by email to any student complaints or requests raised through the Student Self-service Portal (SSP).

- Messages which generate a NDR (Non Delivery Report or bounced message) must be acted upon.

- “Permanent” error messages must be acted upon immediately.

- Staff must stop sending mail to any individual at their request.

8. Monitoring and sanctions

LSBM accepts that the use of email is an extremely valuable business, research and learning tool. However, misuse of such a facility can have a detrimental effect on other users and potentially LSBM’s public profile. The distribution of any information through LSBM’s network is therefore subject to scrutiny. LSBM reserves the right to determine the suitability of email content and any illegal use of the email service will be dealt with appropriately. For example, the police can have a right of access to recorded data in pursuit of a crime.

Accordingly:

- LSBM maintains the right to access user email accounts in the pursuit of an appropriately authorised investigation.

- The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

- LSBM is obliged to monitor to fulfil our responsibilities with regard to UK law. Referrals will be made to the IT Manager and Head of Quality in her Prevent Capacity.

- Action (including disciplinary action) may be instigated, as deemed appropriate, by the IT Manager and Managing Director, or other representatives such as Deputy Academic Principal and Academic Registrar.

- Related regulations, policies and procedures

9. Related regulations, policies and procedures

- Staff Departures: IT Procedures

- Internet Acceptable Use Policy

10. Review of the Email Acceptable Use Policy

This Email Acceptable Use Policy will be reviewed annually by the IT Manager. Any amendments require the approval of the Senior Management and Leadership Team (SMLT).

Appendix A: Legislative framework for our Email Acceptable Use Policy

The following list is not exhaustive:

- Communications Act 2003
- Computer Misuse Act (1990)
- Counter-Terrorism and Security Act 2015
- Criminal Justice and Immigration Act 2008
- Criminal Justice and Public Order Act 1994
- Data Protection Act (1998)
- Equality Act 2010
- Freedom of Information Act (2000)
- Human Rights Act (1998)
- Malicious Communications Act 1988
- Obscene Publications Act 1959
- PREVENT Duty Guidance (2015)
- Regulation of Investigatory Powers Act (2000)