**London South Bank University**
**Email Usage Regulation version 2.5**

1. **Scope**
   This email usage regulation (the Regulation) covers:

1.1    the deployment and use of London South Bank University's (the University's) e-mail system, including electronic notice-boards hosted thereon;

1.2    specific protocols and guidance concerning the Data Protection implications to the University;

1.3    all use of email within the University and in external communications.


2. **Objectives**
   E-mail and other electronic information systems will, in accordance with the University's Information Strategy, reduce the need for paper-based communication. The University makes available e-mail systems for use by its staff and students and encourages the appropriate use of e-mail as an alternative to paper based communication. The objectives of the Regulation are to ensure as far as is reasonably possible that:

2.1    The University's e-mail system is coordinated and managed by the University's Information & Communications Technology Department (ICT). No other e-mail system (server or client) is recognised or supported within the University.

2.2    All email communication between staff, staff and students, Faculties and students, students and the University must normally be carried out using the LSBU email system as this is the only way in which an audit trail for the email message(s) can be provided.  This requirement must be communicated by the Faculties to all students on enrolment.

2.3    The University avoids and/or is protected from damage or liability resulting from use of its facilities for purposes contrary to the law of the land or the University's Memorandum and Articles.

3. **Legislation and Other Policy**
   The Regulation is to be read in the context of the following legislation (in each case, where appropriate, as amended from time to time):

   - Data Protection Act (1998);
   - Copyright, Designs and Patents Act (1988);
   - Computer Misuse Act (1990);
   - Criminal Justice and Public Order Act (1994);
   - Regulation of Investigatory Powers Act (2000);
   - Malicious Communications Act (1998);
   - Trade Marks Act (1994);
   - Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000;
   - Human Rights Act (1998);
   - Freedom of Information Act (2000);
   - Communications Act (2003)
   - Terrorism Act 2006; and
   - any other relevant legislation.

3.1 The University has adopted as policy the guidance issued by the Universities and Colleges Information Systems Association on the Computer Misuse Act.

3.2 The University is obliged to comply with and endorses, the following:

- Joint Academic Network (JANET) Acceptable Use Policy issued by the United Kingdom Education and Research Networking Association (UKERNA);

    and

- Code of Conduct on the Use of Software and Datasets issued by the Joint Information Systems Committee (JISC) of the Department for Education and Skills (DfES).

## 4 Application of the Regulation

### 4.1 Enforcement
It is the specific responsibility of ICT to ensure that the Regulation is fully implemented. All students and staff have a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with this Regulation.

### 4.2 Breach
It is the duty of ICT to take appropriate action to prevent breaches of the Regulation.

### 4.3 Review and Audit
The Information Strategy Board (ISB) is responsible for regular review of the Regulation in the light of changing circumstances.

## 5 Use of E-mail
5.1 The e-mail systems are University property and the University reserves the right to monitor and to access any e-mail messages.

5.2 The use of e-mail for incidental and occasional personal purposes is permitted for convenience but should not be used for private confidential correspondence. The University cannot guarantee the total security of private emails.

5.3 All users are responsible for ensuring that their e-mail usage is within the regulations and is ethical and lawful. The sending of text or images that contain sexual terminology, racist views, offensive references to disability, religion or sexual orientation, indecent or obscene material is prohibited.

5.4 Access to the University e-mail systems for staff and students is available off-campus.

5.5 Provided the appropriate security guidelines are followed (ICT Security Policy), e-mails sent from one user to another on the same e-mail system are relatively secure - any other e-mails should at all times be regarded as having the same status as a postcard. E-mail is an inappropriate medium for the transmission of sensitive or confidential information. If in doubt, alternative methods of communication should be employed, or advice sought.

5.6 Users of e-mail should be aware of formal requirements and good practice in the use of e-mail as set out in the LSBU email usage guidelines.

5.7 E-mail may be used for any legal activity in furtherance of the aims or policies of the University, subject to the conditions listed below. The following uses (but not limited to) are prohibited:

5.7.1 Any use that violates University policies, standards or administrative notices including the ICT Security Policy.

5.7.2 The use of another individual's e-mail account using that individual's identity (i.e. the individual's username/password details).

5.7.3 Impersonation or misrepresentation of another individual.

5.7.4 Alterations of source or destination address information.

5.7.5 The use of e-mail that could result in the inadvertent commitment of the University to a contract or agreement if it appears to the other party that he/she has authority to do so.

5.7.6 The e-mailing of some sensitive messages, for example employment decisions.

5.7.7 The use of e-mail for personal reasons to promote or denigrate companies or organisations, or defame other employees.

## 6 Monitoring

6.1 The University may monitor or record data and or communications transmitted on their ICT infrastructure to:

- establish the facts;
- ascertain compliance with regulatory or self-regulatory practices or procedures;
- ascertain or demonstrate standards which are achieved or ought to be achieved by persons using the system;
- prevent or detect crime;
- investigate or detect unauthorised use of the University's ICT;
- ensure the effective operation of the University's ICT;
- for other reasons as deemed necessary by the Vice Chancellor or Pro Vice Chancellors of the University.

6.2 The University may monitor but not record communications to check the level of personal use of ICT. Monitoring will only be undertaken to such extent as is necessary in the circumstances.

6.3 As a public authority, the University may monitor or record communications in the interests of national security.

6.4 ICT does not routinely monitor or access e-mail. However, all e-mails arriving at the University are automatically scanned for viruses and for "spam" content i.e. whether they match unsolicited, nuisance, e-mails previously sent - any such e-mails are blocked. However, filtering/virus-scanning can never be 100% effective so any unsolicited e-mails/attachments should always be treated with caution. Similarly, an e-mail may be incorrectly marked as infected or "spam" and therefore some e-mails could be blocked unnecessarily. ICT reserves the right of access to users' e-mail and audit logs on both the client workstation as well as the servers for legitimate purposes, such as investigation of complaints of misuse. Contents and audit logs for both sent and received e-mail may be inspected (including personal e-mail) at any time without notice.

6.5 ICT will endeavour to maintain privacy of e-mail. However, there may be special cases where it is essential that e-mail messages are accessed due to, for example, illness of the owner of a mailbox. In these instances, on the request of a Dean of Faculty or Head of Department and on the authorisation of the Director of ICT (or appropriate deputy), ICT may locate and make available e-mail messages for access by a nominated member of staff. The owner of the mailbox will be notified in due course.

6.6 Certain authorised members of ICT may necessarily have access to the contents of e-mail messages in the course of system administration. Any knowledge thus obtained will not be communicated to others, unless required for system administration.

6.7 ICT reserves the right to take special actions in administering e-mail if this is essential to preserve the integrity or functionality of the systems. This may include the deletion of e-mail.

## 7 Deletion and Backups

7.1 E-mail messages are backed up along with other files in accordance with existing ICT operational procedures so messages deleted by the user may still be held in backups. However, restorations of the ICT backup of e-mail messages is only intended for use in the event of a major system failure. Individual messages or mailboxes cannot be restored. The 'deleted item' feature of Outlook can be used to recover any items accidentally deleted.

## 8 Security – Opening and Closing of Accounts

8.1 Computer and e-mail accounts for staff are set up by ICT on receipt of a completed request form. Associated passwords are issued directly to the end user or via Faculty administration. Staff

accounts are deleted when the member of staff leaves the University. Student accounts are created automatically after enrolment of the student and remain active until the end of the course or receipt by ICT of notification of withdrawal. Student passwords are issued via a self-service web site which can be used either on or off campus.

8.2     Before leaving employment at the University, staff should unsubscribe from any e-mail lists that they may have subscribed to and delete any personal e-mails in their account.  If there are any work-related e-mails that need to be transferred to another user then these e-mails should be forwarded on as appropriate.

8.3     Following the departure of a member of staff from the University, their e-mail account will be closed. If requested ICT will arrange for an "out of office" message to be set for a period of 4 weeks, after which time the account will be deleted. University management may request access to be given to the closed mailbox by another member of staff for this duration.

## 9     Disclaimer
9.1     All external e-mail messages sent from the University will include an e-mail disclaimer, as follows:

"This e-mail message may be confidential and is intended only for the use of the individual(s) to whom it is addressed.  It may contain information which is or may be confidential, non-public or legally privileged. Please do not disseminate or distribute this message other than to its intended recipient without permission of the author. You should not copy it or use it for any purpose nor disclose its contents to any other person. If you have received this message in error, please notify me by email immediately and delete the original message and all copies in your computer systems."

The text is to be black Arial 10pt.

## 10    Data Protection
10.1    The following guidelines are specific to e-mail:

10.1.1    Under the Data Protection Act, all e-mail transmissions which contain personal data may be disclosed in response to a request for disclosure, brought forward (through normal procedure), via the University's Archives, Records & Information Access Unit. 'Personal data' can include a sender's opinion of another person;

10.1.2    Under the Data Protection Act, e-mail messages may be disclosed to those referred to in them. The University is not responsible for any subsequent action to which a sender may thereby make themselves liable;

10.1.3    The University's internal and external use of e-mail systems, for bona fide purposes connected with its operations, is registered with the Data Protection Registrar.  For further information contact the Director of Archives, Records and Information Access;

10.1.4    The University's correspondent with the Information Commissioner concerning the use of e-mail, shall be the University Secretary;

10.1.5    The use of e-mail, as a means of internal as well as external communication, falls within the provisions of the Data Protection Act 1998.

_____End of Email Usage Regulation_____