Information Communications Technology Security Policy

1. Scope

This security policy (The Policy) covers:

1.1 the deployment and use of London South Bank University’s (the University’s) information communications technology (ICT) (i.e. all computers, communications devices, peripheral equipment, networks, software and data) within and between University property, or belonging to the University but located elsewhere;

1.2 the use of information systems not owned by the University and located outside of its property, where such use is effected from or via equipment located on University property, or by equipment belonging to the University;

1.3 all use of the University’s ICT infrastructure and wide area and local area networks;

1.4 the security of hardware, software and data;

1.5 the security of personnel using information systems;

1.6 the security of the University’s assets that may be placed at risk by misuse of information systems; and

1.7 copyright and data protection aspects, the use of information systems not owned by the University or located on its property, but used by University students or staff for study or business purposes connected with the University.

2. Objectives

The University seeks to protect its assets from loss and to provide a secure working environment for its students and staff. The objectives of the Policy are to ensure as far as is reasonably possible that:

2.1 the University’s assets are secure against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence; and

2.2 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 Charter and Statutes.

3. Legislation and Other Policy

The Policy 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);
- Human Rights Act (1998);
- Freedom of Information Act (2000);
- Communications Act (2003);
- Terrorism Act 2006; and
- any other relevant legislation.
The University has adopted as policy the guidance issued by the Universities and Colleges Information Systems Association on the Computer Misuse Act.

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 Policy

4.1 Enforcement
It is the specific responsibility of the ICT Department to ensure that the Policy 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 Policy.

4.2 Breach
It is the duty of ICT to take appropriate action to prevent breaches of the Policy. Where such action is outside of the remit of ICT, the Director of ICT will notify the University Secretary.

4.3 Review and Audit
The Information Strategy Board (ISB) is responsible for regular review of the Policy in the light of changing circumstances. The University Secretary has a brief to ensure that the Policy is appropriate for the protection of the University's interests.

5. Acceptable Use of ICT
Acceptable use is use for the purposes of:

- teaching and learning;
- research;
- personal educational development;
- administration and management of University business;
- development work and communication associated with the above; and
- consultancy work contracted to the University.

5.1 Reasonable use of ICT facilities for personal correspondence, where not connected with any commercial or illegal activity, is at present regarded as acceptable. However, the University may monitor the use of ICT for personal use, and if personal use is deemed by the University not to be acceptable then access to ICT facilities may be withdrawn and/or disciplinary action may be taken.

5.2 Use for other purposes may be permitted by the ISB, subject to report when required by the University Secretary.

5.3 The Rules for Use of ICT from time to time (the current version of which is set out in Appendix A) form part of this Policy, and are binding on all staff and students. The Rules will be regularly reviewed by the ISB for adequacy, and any amendments shall similarly form part of this Policy and be binding on all staff and students.

5.4 It is University policy that all use of the ICT facilities shall be lawful, honest and decent, and users shall have regard to the rights and sensitivities of other people.

5.5 ICT has responsibility to take all reasonable steps to stop unacceptable use of information systems. If ICT is unable to carry out the duty required, the responsibility will fall to the University Secretary. These officers will be
guided on policy issues by the ISB and appropriate external bodies.

5.6 ICT shall not be used to access or create material of an offensive nature. This includes material containing:
- racist or sexual terminology;
- offensive references to disability, religion or sexual orientation; or
- pornographic images or other content.

6. Registration
The following are eligible to register as users:
- any student on a course leading to a recognised qualification taught within and awarded by the University, or other student of the University;
- any person holding a contract of employment with the University;
- any person holding an honorary position recognised by the University; and
- any person recommended by the Head of Department and approved by the ISB.

6.1 Use of ICT facilities including information systems and networks shall be restricted to registered users. The Head of Department, as appropriate, has responsibility for implementing such access restrictions.

7. Advice and Training
7.1 It is the responsibility of the Head of Department to ensure that all users are made aware of the risks of security breaches and of their responsibility to take adequate precautions.

7.2 All training, documentation and publications provided to users in relation to ICT will contain relevant advice on good practice relating to security.

7.3 The University will also endorse good practice in all publicity of the ICT facilities where appropriate.

8. Physical Security
Equipment will be secured against theft and damage to a level that is cost-effective.

9. Operational Practice
9.1 It is the responsibility of ICT to attend to the following: securing the integrity of data and code held and processed on the University's information systems;
- securing the integrity of common-access computers;
- ensuring filestore of common-access computers is purged of inappropriate material;
- in the event of a suspected security breach, enforcing appropriate restrictions to the service until confidence is restored;
- provision of appropriate supported security tools for use by students and staff on computers under their control;
- provision of effective controls on access to restricted ICT facilities (e.g. networks, administrative computers);
- carry out the procedures and to handle any notices served to LSBU under the Terrorism Act 2006 and to take all reasonable steps on behalf of LSBU to prevent further offences.

9.2 It is the responsibility of the computer user to attend to the following:
- taking appropriate security precautions to ensure security in respect of computers under his/her control;
- observing good practice recommendations for security in respect of facilities provided on multi-access computers and networks;
• backing up data on their desktop and or portable PC and or private computers;
• notifying ICT of security problems that may arise on their desktop and or portable PC and or private computers, and responding in a timely manner to security alerts published and or distributed by ICT;
• preserving the confidentiality of passwords; and
• complying with the Rules for the use of Information Communications Technology.

9.3 Damage to equipment, software or data resulting from failure to observe this Policy is deemed to be the responsibility of the defaulter, and will be dealt with in accordance with the staff or student disciplinary code as appropriate.

9.4 Control of access to personal data is the remit of the University Secretary, who will ensure that information about rights and responsibilities under the Data Protection Act (1998) is made available.

10. Monitoring

10.1 The University may monitor general use of ICT to identify any misuse in accordance with this Policy.

10.2 The Director of ICT or the Head of Department, as appropriate, is responsible for ensuring that usage of resources will be logged in sufficient detail to identify defaulters where technically possible.

10.3 The Director of ICT or the Head of Department, as appropriate, will authorise ICT support staff, whose duties require it, to monitor and police the use of computer facilities. Monitoring data will be collected only to assist investigation of a suspected security breach or other misuse.

10.4 ICT support staff shall not monitor personal information except in specific instances where a suspected breach of security or other breach of this Policy requires it. Every such incident will be reported to the University Secretary; also details of the incident will be logged promptly in a central record which will be made available for inspection by personnel authorised by the University Secretary.

10.5 The University Secretary is empowered to authorise a software audit of University equipment, where it is deemed necessary.

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

• establish the existence of 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.

10.7 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.

10.8 As a public authority, the University may monitor or record communications in the interests of national security.
11. Duties of System Administrators

11.1 System administrators have responsibility for maintaining the integrity of computer systems and data held on them, and for ensuring the systems are not misused.

11.2 System administrators are provided with privileged access to computer systems in order to carry out their responsibilities. They have a duty to use such access at all times in a professional manner and within the interest of the University.

11.3 System administrators who are responsible for email services that connect either to the internet or public telephony services should make all reasonable efforts to inform their users that traffic may be recorded or monitored in compliance with the Regulation of Investigatory Powers Act (2000).

11.4 The Director of ICT or the Head of Department, as appropriate, is responsible for ensuring that the duties of system administrators are carried out.

11.5 The Director of ICT or the Head of Department, as appropriate, will publish and maintain details of system administrators and the domain of their responsibilities.
These Rules form part of the University's Information Communications Technology Security Policy.

1. Information communications technology (ICT) administered by London South Bank University (the University) may be used only by students and staff of the University and other persons authorised in writing by the Director of the Information Communication Technology Department (ICT) or the Head of the Department administering the relevant computer facility, as appropriate, and only in accordance with these Rules (as amended from time to time).

2. The ICT systems are used on the understanding that the University will not accept any liability whatsoever for loss, damage, or expense which may result from the ICT facilities, except to the extent that such loss, damage, injury or expense are attributed to negligence, fraudulent misrepresentations or breach of statutory duty on the part of the University or any of its servants or agents acting in their capacity as such.

3. The University reserves the right to monitor all communications and other use of ICT systems in order to ensure compliance with these Rules. Monitoring will only be undertaken to such extent as is necessary in the circumstances.

4. Access gained through permitted use of the University's ICT to other computing centres and facilities linked to those at this University is governed by these Rules, in addition to any rules in force from time to time for use of the ICT facilities at the remote site. In particular, there are also specific rules relating to the use of the Student Residences Network.

5. Usernames and other allocated resources shall be used only by the registered holder. Users shall maintain a secure password to control access to their usernames and accounts. Users shall ensure that passwords are not stored in locations that can easily be accessed by anyone other than the authorised password holder.

6. No person shall by any wilful or deliberate act or omission or by failure to act with due and reasonable care jeopardise the integrity of the ICT equipment, its operating systems, systems programs or other stored information, or the work of other users, whether within the University or in other computing locations to which the facilities at the University allow connection. Such acts include (but not limited to):

   6.1 the creation of network traffic high enough to degrade significantly network performance for other users;

   6.2 the use of tools to alter the behaviour of network devices;

   6.3 the scanning of ports on external computers;

   6.4 circumvention of Network Access Control;

   6.5 monitoring or interception of network traffic;
6.6 associating any device to network access points, including wireless, to which you are not authorised;

6.7 the copying, downloading, distribution or storage of music, video, film or other material, for which you do not hold a valid licence or other valid permission from the copyright holder;

6.8 the distribution, copying or storage by any means of pirated or unlicensed software or music;

6.9 the deliberate viewing, printing, storage and/or distribution of pornographic images;

6.10 the passing on of electronic chain mail;

6.11 the use of University mailing lists for non-academic purposes;

6.12 the unauthorised use of programs on central servers, which consume such resources as to reduce significantly the server's performance for other users.

7. ICT shall not be used to access or create material of an offensive nature. This includes (but not limited to) material containing:
   • Racist or sexual terminology;
   • offensive references to disability, religion or sexual orientation; or
   • pornographic images or other content.

8. Unauthorised access to computer material (ie a program or data) and unauthorised modification of computer material are forbidden by law (Computer Misuse Act 1990) and by these Rules, which endorse the Guidance on the Computer Misuse Act published by the Universities and Colleges Information Systems Association.

9. Use shall not be made of facilities at other locations if a charge for such use will be incurred by the University unless such use has been authorised by Director of ICT or the Head of the Department administering the relevant computer facility, as appropriate. Any charges incurred in contravention of this rule will be reimbursed by the user.

10. All work for which payment from outside the University (excluding payment by Research Councils and bona fide LSBU research contracts) is received, is classified as chargeable and no such work must be undertaken using the University's ICT unless prior written permission has been received from, and charges have been agreed with, the Head of ICT or the Head of the Department administering the relevant computer facility, as appropriate.

11. ICT facilities available for use within the University may be used only for:
   • teaching and learning;
   • research;
   • personal educational development;
   • administration and management of University business;
   • development work and communication associated with the above; and
   • consultancy work contracted to the University.

12. Reasonable use of ICT facilities for personal correspondence, where not connected with any commercial activity, is at present regarded as acceptable. Any instances of excessive use could lead to access to ICT facilities being withdrawn and disciplinary action being taken where appropriate.

13. Prior permission from the Director of ICT or the Head of the Department administering the relevant computer facility, as appropriate, must be obtained in writing if use could possibly fall outside of the terms defined above.
14. No person shall use, copy or transmit any software from University ICT equipment unless a licence from the copyright holder permitting such act is in force. All persons to whom the University provides copies of software for personal use must sign a declaration acknowledging copyright. (Copies of the declaration, and a list of software licensed for use within the University are available from ICT).

15. Any restrictions placed from time to time on the use of ICT administered by the University or amendments to these rules from time to time must be observed.

16. No person or persons shall use the University’s information systems to hold or process personal data except in accordance with the provisions of the Data Protection Act 1998. Any person wishing to use the facilities to hold or process personal data shall be required to:

- inform in advance the Director of the Information Communication Technology Department (ICT) or the Head of the Department administering the relevant computer facility, as appropriate;
- comply with any restrictions the University may impose concerning the manner in which the data may be held or the processing carried out; and
- inform the University's Data Protection Officer.

17. All use of the facilities shall be honest and decent, and shall have regard to the rights and sensitivities of other people. All users are bound to adhere to English law in their use of computing facilities.

Breaches of these Rules are offences under the rules of the University and will be dealt with under the University's disciplinary codes for students and staff. If after investigation it appears that a member of the University, whether staff or student, may have acted in breach of these rules, he or she may be denied access to all ICT facilities pending the conclusion of disciplinary proceedings against him or her. The University reserves the right, in appropriate circumstances, to treat breaches of this Policy as offences of gross misconduct. In addition, breaches of these rules which are also breaches of English law may leave the person in question open to legal action from external bodies and/or the University.