London South Bank University

EST 1892

IT: Acceptable Use Policy

Executive Board Sponsor:	CCO (Chief Customer Officer)
Senior Owner:	Group Director of IT & Digital Transformation
Approving Committee/Body:	ITSRB
Author	Head of IT Security
Last Approved:	February 2020 / July 2021 / January 2022
Next due for review:	January 2024
Version Control	V4.0
Brief Summary of Purpose:	Provides acceptable uses for LSBU IT Systems
Notes:	Unless otherwise stated, this corporate policy applies to all LSBU workers.

LSBU Acceptable Use Policy

1. This Policy forms part of the University's Information Technology Services Security Policy.

2. Information and communications technology (IT) 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 Group Director of IT & Digital Transformation or the Group Head of Information Security, as appropriate, and only in accordance with this Policy (as amended from time to time).

3. The IT 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 IT 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.

4. The University reserves the right to monitor all communications and other use of IT systems in order to ensure compliance with this Policy. Monitoring will only be undertaken to such extent as is necessary in the circumstances.

5. Access gained through permitted use of the University's IT to other computing centres and facilities linked to those at this University is governed by this Policy, in addition to any policies in force from time to time for use of the IT facilities at the remote site.

6. Usernames and other allocated resources shall be used **only** by the registered holder. Users shall maintain a strong and secure password to control access to their University accounts. Users shall ensure that passwords are not shared with anyone else, or stored in locations that can easily be accessed by anyone other than the authorised password holder. Please refer to the IT Password Policy for more information.

7. No person shall by any wilful or deliberate act, or omission, or by failure to act with due and reasonable care, jeopardise the Confidentiality, Integrity or Availability of any IT 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 are not limited to)**:

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

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

7.3 the scanning of ports on external computers;

7.4 circumvention of Network Access Control;

7.5 monitoring or interception of network traffic;

7.6 connecting or associating any device to network access points, including wireless, to which you are not authorised;

7.7 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;

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

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

7.10 the passing on of electronic chain mail;

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

7.12 install and use software without the appropriate authorisation and licences

7.13 the unauthorised use of programs on University machines, which consume such resources as to reduce significantly a server's performance for other users.

8. IT shall not be used to access or create material of an offensive nature. This includes **(but is not limited to)** material containing:

- Racist or sexual terminology;
- offensive references to disability, religion or sexual orientation;
- pornographic images or other content deemed as harassment or bullying;
- terrorist or other content deemed to support extremism; or
- any content or activity deemed illegal under UK law

9. Unauthorised access to computer material (ie a program or data) and unauthorised modification of computer material are forbidden by law (Computer Misuse Act 1990).

10. 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 the Group Director of IT & Digital Transformation. Any charges incurred in contravention of this rule will be recovered from the user.

11. 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 IT unless prior written permission has been received from, and charges have been agreed with, the Group Director of IT & Digital Transformation.

12. IT facilities available for use within the University may be used only for:

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

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

14. Prior permission from the Group Director of IT & Digital Transformation, must be obtained in writing if use could possibly fall outside of the terms defined above.

15. No person shall use, copy or transmit any software from University IT equipment unless a licence from the copyright holder permitting such act is in force.

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

17. 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 2018 and GDPR 2016/679. Any person wishing to use the facilities to hold or process personal data shall be required to:

- inform in advance the Group Director of IT & Digital Transformation;
- inform in advance the University's Data Protection Officer; and
- comply with any restrictions the University may impose concerning the manner in which the data may be held or the processing carried out.

18. Staff who are provided with 'Administrator' accounts in addition to their LSBU accounts, to maintain and support our systems, should only log into those accounts when performing administrative tasks. Once those tasks are completed they should log out of their 'Administrator' account and log back in with their LSBU account to perform their work.

19. Whilst logged in as 'Administrator' staff should avoid performing day to day tasks such as emailing or general web browsing, as if the account is compromised while performing those tasks, these 'Administrator' accounts could be used to more easily attack and compromise our IT systems.

20. 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 the LSBU network and its machines.

21. Breaches of this Policy 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 this Policy, he or she may be denied access to all IT facilities pending the conclusion of disciplinary proceedings against him or her.

22. The University reserves the right, in appropriate circumstances, to treat breaches of this Policy as offences of gross misconduct. In addition, breaches of this Policy which are also breaches of English law may leave the person in question open to legal action from external bodies and/or the University.