SCHOOL OF ADVANCED STUDY
UNIVERSITY OF LONDON

Students' Code of Conduct for the use of University of London IT equipment and systems

1. This document outlines the School of Advanced Study, University of London's standards for the use of IT equipment and systems. It should be read in conjunction with the School's Code of Good Practice in Research.

2. Much of the Code of Conduct is common sense and will help to ensure that you are able to use the University's systems efficiently and effectively. Deliberate misconduct under the code will be handled appropriately under the University Disciplinary Procedures.

APPROPRIATE USE OF SOFTWARE, EQUIPMENT AND INFORMATION

3. **If you are using University of London equipment, you must not:**

a. In compliance with Section 26 of the Counter-Terrorism and Security Act 2015, staff, students and visitors using University IT systems should not create, transmit, receive, view or store material with the intent to radicalise themselves or others. If a member of the University community believes they may have encountered a breach of this provision, they should contact the Office of the University Secretary immediately.

b. Download, install or use any software unless it has been expressly approved in advance by the University of London Computer Centre. If you know of any unauthorised software on any of the University's IT equipment, you must let School staff know.

c. Access, copy, amend or delete any information which you do not have authority to access. Sensitive, personal or confidential data should not be posted on shared drives without password protecting the file.

d. Insert any storage media unless you are certain that they do not contain viruses or other malicious programs. If you are uncertain seek assistance from staff.

4. **Please do:**

a. Ensure all software is correctly installed by authorised staff. Software must be used in accordance with licensing agreements. Failure to do so is illegal and may lead to serious financial penalties for the University or loss of reputation.

b. Tell the staff or service@london.ac.uk if you are warned of, or suspect the reception of, a computer virus infection, hoax or persistent spam.

c. Ensure that any critical or personal data is not stored on our workstation's local C drive.

d. Ensure that any screensavers on your machine are suitable and are not likely to give offence.

WORKING SECURELY

Passwords

5. Your password must be at least 8 characters in length, contain at least one uppercase, one lowercase and one non-alpha character (e.g. a number or punctuation mark), not contain a significant portion of your username, not be any of your previous ten passwords and cannot be changed more than once in any 24 hour period.

6. Do not write down your password. If you believe someone else knows your password, change it immediately.

7. **You must not:**

a. Use another person's account or let someone else use your nominated account, to access any system or to send e-mails.
b. Leave your terminal, or portable computer, unattended without locking the screen or logging out.

c. Copy software or data belonging to the University to any third party, unless this has been expressly approved by School staff. d. Attempt to circumvent or defeat the security and audit controls in any way.

e. Reply to spam, including phishing emails that ask for your username and password.

8. **Please do:** use the password protection facility on your screen saver.

9. **Please alert School staff immediately:**

a. If you suspect or have knowledge of someone of trying to access data for which they do not have authorisation.

b. Following the theft or loss of any piece of equipment or data, e.g. laptops, tablets or storage media such as memory sticks, etc.

APPROPRIATE USE OF YOUR SCHOOL EMAIL ACCOUNT

10. The contents of an email are not necessarily private. Any comments you make about an individual in an email may be disclosed to them if they make a Subject Access Request under UK Data Protection legislation. Members of the public may also have a right of access to information contained in emails under the Freedom of Information Act 2000. Emails can be restored from backup tapes and read, even if you have ostensibly deleted them.

11. Auto-forwarding to online email accounts is not secure. Confidential or sensitive personal information should be sent by password protected attachments, and the password sent in a separate message or preferably by phone.

12. Reasonable personal (non commercial) use of your School email account is acceptable where it does not have a detrimental impact on your work or on University resources.

13. **You must not:**

a. Open emails or attachments which appear self-evidently dubious or suspicious in any way. Report the email to service@london.ac.uk b. Use your School email account to knowingly subscribe to mailing lists which are pornographic, obscene or offensive.

b. Send defamatory, abusive or offensive emails from your School account either internally or externally. Emails are subject to monitoring. Be aware that there are circumstances under which emails are considered to be legally binding.

c. Use your university email account for personal financial gain or for private commercial purposes, for example on line auction sites, since the University may become jointly liable for any transactions.

d. Use your School email account to initiate or forward email chain letters and/or unsolicited joke emails. They may offend the recipient, be intrusive and give rise to a claim against you and the University. They may also be perceived as discriminatory.

APPROPRIATE USE OF THE INTERNET

14. **If you are working on a School computer or laptop you must not:**

a. Knowingly visit or download pornographic, obscene or offensive material. This is viewed as serious misconduct and will lead to disciplinary action.

b. Download executable files (files which run programs on your computer) from external sources, including bulletin boards, unless this has been approved by School staff. The risk is that viruses could be imported and software might be in breach of copyright.

c. Access the internet from University of London networked machines by any connection other than the network itself.

RESPONSIBLE USE OF ONLINE FORA

15. If you participate in blogs and other online fora and make postings which relate to your studies or fellow students, you must accept full responsibility for the items you post and ensure that you do not submit:

- any defamatory or libellous posts;
- any material that infringes and / or violates any right of a third party or any law.
- any vulgar, obscene, discourteous, or indecent language or images.
- any software or materials that contain a virus or other harmful component.

Any material you submit must not bring the reputation of the University or your fellow students into disrepute and must not breach any of the University's policies. A deliberate breach of these conditions will be treated under the University's disciplinary procedures.

MONITORING

16. Emails, internet use, computer equipment and telephone logs may be monitored if you are reasonably believed to be knowingly and deliberately accessing or circulating material which:

a. is illegal; or

b. which contravenes the standards of behaviour set out in published University regulations; or

c. which brings the University into disrepute (for example viewing or circulating pornography); provided an impact assessment of the proposed monitoring and its justification have first been considered by the Director of ULCC or his/her nominee together with the Dean of SAS or his/her nominee. Monitoring will normally continue for a maximum of 3 months but may be extended if justified in the light of an updated impact assessment.

17. The Impact Assessment will take into account the need to observe academic freedoms.

18. Any information collected during the course of monitoring will be held securely in accordance with the University's data protection policies. You will be given the opportunity to see and explain any data collected, as part of any disciplinary or grievance procedures that may result.