3 Monitoring

3.1 Principles

Networks, computers, internet usage and email usage may be monitored by members of the Networks, Systems and Information Security teams within IMT, or third parties contracted on behalf of IMT, and usage logged. Logs are kept secure and are only available to networks, Systems and Information Security teams, and will only be kept as long as necessary, in line with current data protection guidelines.

LSE's networks, computers, internet usage and email usage may be monitored and logged for all lawful purposes including:

1. Tracking the flow of network traffic
2. Facilitating and improving capacity planning
3. Identifying areas for improvement, including provision of teaching and learning facilities
4. Maintaining good availability of network bandwidth
5. Ensuring use of resources is authorised
6. Management of systems
7. Protecting against unauthorised access
8. Ensuring system security
9. Compliance with LSE policies and regulations and any other appropriate regulations all LSE users must comply with (e.g. the Joint Academic Network [JANET] Acceptable Use Policy)
10. Avoiding or mitigating legal liabilities and complying with legal obligations
11. Preventing and detecting crime

Monitoring will include active attacks by users authorised by the LSE to test or verify the security of its systems.

During monitoring, information may be examined, recorded, copied and used for authorised purposes.

All information, including personal information, placed on or sent over LSE systems may be monitored.

During the monitoring process, personal data may be inadvertently seen or accessed by staff authorised to perform monitoring.

Monitoring will be automated in the detection and removal of viruses, malware, spam, pornography, inappropriate content and other activities not lawful to LSE business.

3.2 Email scanning

Incoming e-mail will be scanned by LSE mail filtering system. This includes using virus-checking software.

The software may block unsolicited marketing e-mail (spam), e-mail which has potentially inappropriate content or unscannable attachments, e-mail which breaks any legal or contractual agreement held by LSE or which contains any other inappropriate material.

A trace log of emails sent by user accounts will be kept on a 30-day rolling basis.

3.3 Consent

Use of LSE information technology, authorised or unauthorised, constitutes consent by the user to the monitoring of these systems.

3.4 Unauthorised Use

Unauthorised use, as outlined in the *Information Security Policy* and associated policies, may give rise to disciplinary procedures and/or criminal prosecution.

Evidence of unauthorised use collected during monitoring may be used subsequently in disciplinary, criminal or other proceedings.

3.5 Laws and regulations affecting LSE monitoring and logging

3.5.1 Regulation of Investigatory Powers Act 2000

The legislation requires LSE to intercept communications without consent, where directed by law enforcement officials, for purposes such as recording evidence of transactions, detecting crime or unauthorised use. LSE is not required to gain consent before intercepting for these purposes, but needs to inform staff and students that interception may take place. This does not imply that all communications are monitored, just that they may be for the above purposes. The Act is available here:
http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1

3.5.2 Data Protection Act 1998

IMT hold user registration data and information on the use of the LSE's computer systems and network in accordance with the stipulations of the Data Protection Act, to ensure personally-identifiable information is not made accessible outside of the identified groups in *Section 2* above. Information concerning when and where users have accessed systems, print logs, Internet caches, access control system data, network traffic statistics and other similar data may be logged, but access will be strictly controlled and logs will be held for no longer than necessary.

While normally only used for resolving operational problems, these logs will be analysed in a controlled environment (under the remit of the LSE's Information Security Policies) in the case where a breach of LSE regulations and policies, or other misuses and abuses of facilities, is suspected.

Information contained within the logs referred to above may also be used to communicate with users to alert them to malfunctions within LSE IT facilities or to request action to correct the malfunctions which may be putting normal operations of the IT facilities in jeopardy.
If log information is held outside LSE, it will still be held under the auspices of the Data Protection Act, with access accordingly controlled.

The Data Protection Act 1998 is available here:
http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

3.5.3 Terrorism Act 2006

The Terrorism Act 2006 makes it an offence to write, publish or circulate any material that could be seen by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism.

It also prohibits the writing, publication or circulation of information which is likely to be useful to any one or more persons in the commission or preparation of terrorist acts or is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the purpose of being so useful.

In addition, it prohibits the glorification of the commission or preparation (whether in the past, in the future or generally) of terrorist acts or such offences; and the suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances. The Terrorism Act is available here:

http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en_2

3.5.4 Janet Acceptable Use Policy

LSE's internet service provider, Janet (the Joint Academic Network) requires that LSE is able to identify any person using the service.

The Janet Acceptable Use Policy can be found here:
https://community.ja.net/library/acceptable-use-policy

3.5.5 Counter-Terrorism and Security Act 2015 – Statutory Guidance

The statutory guidance accompanying the Counter-Terrorism and Security Act 2015 (Prevent duty guidance for higher education institutions in England and Wales https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance_For_Higher_Education__England__Wales_.pdf) requires LSE to have "due regard to the need to prevent people from being drawn into terrorism."

The Act imposes certain duties under the *Prevent* programme, which is aimed at responding to "the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views." The Prevent programme also aims to provide "practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support".

LSE must balance its existing legal commitments to uphold academic freedom and (under the Education (No. 2) Act 1986) freedom of speech within the law against the new Prevent duty, and seek to ensure that its IT facilities are not used to draw people into terrorism.

3.6 ISO27001 controls governing LSE use of monitoring

The necessity of monitoring and logging is covered by the International Standards Organisation's information security standard ISO27001, in the following control sets:

A.10.3.1 – Capacity Management: "The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance."

A.10.10 – Monitoring: "To detect unauthorized information processing activities" and including such processes as:

A.10.10.1: Audit logging: "Audit logs recording user activities, exceptions and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring"

A.10.10.2: Monitoring system use: "Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly"

A.10.10.3: Protection of log information: "Logging facilities and log information shall be protected against tampering and unauthorized access."

A.10.10.4: Administrator and operator logs: "System administrator and system operator activities shall be logged."

A.10.10.5: Fault logging: "Faults shall be logged, analysed, and appropriate action taken."

3.7 Further Policies, Codes of Practice, Procedures and Guidelines

This policy sits beneath LSE's overarching *Information Security Policy*. Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on LSE's website. All staff, students and any third parties authorised to access LSE's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

The below list of current policies is in no way authoritative and new policies will be published on the LSE website as they become available.

Associated polices:

Information Security Policy
Anti-Virus Policy
Conditions of Use of IT Facilities at LSE
Conditions of use of the residences network
Password Policy
Asset Management Policy
Data Protection Policy

Standards and Guidelines:

Information Classification Standard
Encryption Guidelines
Remote and Mobile Working Guidelines
Guidelines on the use of Cloud storage

3.8 Review and Development

This policy shall be reviewed and updated regularly by the Information Security Advisory Board (ISAB) and an auditor external to IT Services as appropriate to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.