Policy concerned with the examination of stored material applies to

However, a general exemption in the RIPA permits LSHTM to intercept certain communications where the interception is by an authorized person for purposes connected with the provision or operation of a service, for example:

¥ email postmasters may examine mis-addressed messages in order to redirect them as necessary, or check email subject lines for malicious code;

¥ system operators may monitor system trafÞc to determine its source, where this is necessary to ensure the effective performance of their mail servers, for example to eliminate unsolicited commercial email (UCE or 'spam').

¥ system and network managers may investigate which system and/or individual is the source of a denial of service attack.

The RIPA LBPR require that persons carrying out routine monitoring under this exemption must be properly authorized either through their job description or by written authorization from their Head of Department (see section 4 below).

Persons carrying out monitoring for operational reasons must be alert to the focus of their investigation changing. If, at any stage, monitoring or access to stored material is required to investigate matters of policy (or legal) compliance the appropriate authorization must be obtained as described in sections 3.2 & 4.2.

3.2 ! Monitoring for policy (and legal) compliance

All other activities falling under the exemptions within the LBPR will constitute monitoring for policy or (legal) compliance. Each individual act of monitoring for this purpose must be speciÞcally authorized and documented as described in sections 4 and 5.2, respectively.

4 ! Who can authorize monitoring of computer or network use?

The law distinguishes between monitoring for operational and policy reasons. However, both classes of activity must be authorized. Note that authorization mechanisms are different in the two cases.

4.1 ! Routine monitoring for operational reasons may be authorized through staff job descriptions or by written authorization from one of the following (or their deputies) as appropriate:

- ! the Head of IT Security, IT Audit and Compliance (in pursuance of security issues)
- !

!

without a lawful purpose, both the ofÞcer of the School and the School may face civil liability.

8.3 ! A complaint is received that a LSHTM email address is being misused to send unsolicited commercial email. This is a violation of the LSHTM Acceptable Use Policy. It is decided to investigate by monitoring messages sent from this email address. Having previously informed users of the relevant email system that monitoring/recording may take place (section 5), the relevant person (as set out in section 4 above) should issue written instructions authorizing the monitoring.

8.4 ! A member of staff is suspected of spending large amounts of time downloading inappropriate material on their computer, to the point where there is an adverse impact on their ability to perform their duties. As an investigation is likely to lead to disciplinary action, the Director of Human Resources should provide instruction on how the matter is to be pursued, and specialist advice may be required on how to preserve evidence. The success of any action may depend on whether it can be shown that the individual concerned had been properly made aware of what constitutes Ôacceptable use'.

8.5 ! Mr. E, who administers a computer system used by a number of departments, discovers that the system disk is almost full. To ensure effective system operation, Mr. E checks users' quotas, and Þnds that one member of staff has Þlled up the disk with what appear to be MP3 music Þles. The presence of these Þles is likely to represent a violation of the LSHTM Acceptable Use Policy. However, before investigating further, Mr. E should seek authorization from the appropriate person (c.f. sections 5.1 and 5.2 above).

9 ! Status of this document

This document is a part of LSHTM's information management and security policy and has been endorsed by the Senior Leadership Team/Academic Affairs. It is subject to regular review.

10 ! References

A very clear document containing examples of how the legislation applies in practice has been produced by the Joint Information Systems Committee, which promotes the use of information systems and information technology in Higher and Further education across the UK. It can be downloaded from:

http://www.jisclegal.ac.uk/LegalAreas/InterceptionandMonitoring/InterceptionandMonitoringLawEssentials.aspx

Relevant legislation includes:

1. The Regulation of Investigatory Powers Act 2000

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

2. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 .

http://www.hmso.gov.uk/si/si2000/20002699.htm

3. The Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

4. The Data Protection Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

5. The Employment Practices Data Protection Code Part 3 Monitoring at work

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_3-monitoring_at_work_1.html