LSHTM Information Management and Security Policy

Endorsed by Academic Affairs - Feb 2014

1 Introduction

1.1 Information is one of the School's most important assets. Regardless of the form it takes, or the means by which it is shared or stored, it should always be appropriately protected. This applies to information in printed or written form, electronically stored, transmitted by post or using electronic means, shown on films, or spoken in conversation.

1.2 Information security is concerned with guaranteeing *availability* (ensuring that authorized users always have access to information when they need it), *integrity* (safeguarding its accuracy and completeness), *confidentiality* (ensuring that sensitive information is accessible only to those authorized to use it), and *authenticity.* It must also address proper methods of disposal of information that is no longer required. Security is essential to the success of almost every academic and administrative activity. Effective security is achieved by working within a proper framework, in compliance with legislation and School policies, and by adherence to approved procedures and codes of practice.

1.3 The objectives of this information management and security policy are to:

- ensure that all of the School's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse, and that this protection is cost-effective;
- ensure that all users are aware of and fully comply with this policy statement and all associated policies, and are aware of and work in accordance with the relevant procedures and codes of practice;
- ensure that paper records are kept securely and managed effectively;
- ensure that all users are aware of and fully comply with the relevant UK and European Union legislation;
- create across the School an awareness that appropriate security measures must be implemented as part of the effective operation and support of information management systems;
- ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle;
- ensure that information is disposed of in an appropriately secure manner when it is no longer relevant or required.

1.4 Scope

The policy applies to all staff and students of the London School of Hygiene and Tropical Medicine and all other computer, network or information users authorized by the School or

any department thereof (including visitors). It relates to their use of any School-owned facilities (and those leased by or rented or on loan to the School), centrally managed or otherwise; to all private systems (whether owned, leased, rented or on loan) when connected to the School network; to all School-owned or licensed data and programs (wherever stored); and to all data and programs provided by the School by sponsors or external agencies (wherever stored). The policy also relates to paper files and records created for the purposes of School business.

This policy statement does not form part of a formal contract of employment with LSHTM, but it is a condition of employment that employees will abide by the regulations and policies made by the School. Likewise, these latter are an integral part of regulations for students.

1.5 Definitions of the terms used in this policy statement and supporting documentation may be found in the glossary.

2 Responsibilities for Information Security

2.1 Everyone who uses the School's systems and information has responsibility for protecting those assets. Individuals must, at all times, act in a responsible and professional way in this respect, and must refrain from any activity that may jeopardize security. It is the responsibility of each individual to ensure his/her understanding of and compliance with this policy and any associated procedures or codes of practice.

2.2 The Information Security Working Group (ISWG) is responsible for defining an Information Management and Security Policy and for ensuring it is discharged by all academic and administrative departments. The policy will apply to associated bodies, including LSHTM-owned companies.

2.3 Line Managers are required to implement this policy in respect of both paper and electronic systems operated by their staff. They are responsible for ensuring that staff, students and other persons authorized to use those systems are aware of this policy and its associated codes of practice and they should facilitate compliance with them. Line Managers shall ensure adequate oversight of security, through IT Services or departmental computing support staff.

Staff with supervisory responsibility shall ensure their supervised staff or students are aware of best practice.

2.4 The LSHTM Records Management Policy applies to all records created, received or maintained by staff of the School in the course of carrying out their corporate functions. Records and documentation created in the course of research, whether internally or externally funded, are also subject to contractual record-keeping requirements. The LSHTM Archivist and Records Manager is responsible for the secure storage of non-current and archive files.

2.5 The Information Security Working Group advises on matters related to compliance with this policy, and is responsible for regularly reviewing it for completeness, effectiveness and usability. It will, from time to time, make available supplementary procedures and codes of practice, and promote them throughout the School; once approved by the Senior

Leadership Team (SLT), these will also become School policy and will be binding on departments. ISWG will also arrange for analysis of security assessments received from departments and report on these to SLT.

3 Compliance with Legislation

3.1 The School, each member of staff, and its students have an obligation to abide by all UK legislation and the relevant legislation of the European Union. Of particular importance in this respect are:

- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Data Protection Act 1998
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000.

This policy satisfies the Data Protection Act's requirement for a formal statement of the School's security arrangements for personal data. The requirement for compliance devolves to all users defined in (1.4) above, who may be held personally responsible for any breach of legislation.

3.2 Relevant legislation is referenced in supporting policies and guidelines. Full texts are available from Her Majesty's Stationery Office.

4 Risk Assessment and Security Review by Departments

4.1 System owners and users shall adopt a risk-based approach to assessing the business value of information handled and the appropriateness of security controls in place or planned. Without proper assessment of the value of information assets, and the consequences (financial and otherwise) of loss of data or disruption to service, efforts to improve security are likely to be poorly targeted and ineffective. Similarly, periodic review is necessary to take into account changes to technology, legislation, business requirements and priorities; and security arrangements should be revised accordingly.

4.2 Heads of Department shall establish effective contingency plans appropriate to the outcome of any risk assessment. They are also required to re-evaluate periodically the security arrangements for their information management systems - at least once every three years, and additionally in response to significant departmental changes (such as turnover of key staff, commissioning of new systems etc.). A formal report must be submitted to the Information Security Working Group which will report to SLT.

5 Breaches of Security

5.1 IT Services will monitor network activity, receive reports from LSHTM IT security staff and other security agencies, and take action or make recommendations to ISWG consistent with maintaining the security of the School's information assets.

5.2 Any individual suspecting that the security of a computer system has been, or is likely to be, breached should immediately inform his/her line manager and the LSHTM Computer Security Incident Response Team (email to CSIRT@lshtm.ac.uk). The team will advise the School on what steps should be taken to avoid incidents or minimize their impact, and identify action plans to reduce the likelihood of recurrence.

5.3 In the event of a suspected or actual breach of security, IT Services or departmental staff may, after consultation with the relevant departmental staff or Head of Department, require that any unsafe systems, user/login names, data and/or programs be removed or made inaccessible.

5.4 Where a breach of security *involving either computer or paper records* relates to personal information, the Head of Department and the Head of IT Security, IT Audit and Compliance (CSIRT@lshtm.ac.uk) must be informed, as there may be an infringement of the Data Protection Act 1998, which could lead to civil or criminal proceedings. It is vital, therefore, that users of the School's information systems comply, not only with this policy, but also with the School's Data Protection Policy and associated codes of practice, details of which may be found on the School's intranet.

5.5 All physical security breaches (e.g. thefts, losses, break-ins, on or off site) should be reported to IT Services Information Security staff at CSIRT@lshtm.ac.uk).

5.6 The Director or his deputy has the authority to take whatever action is deemed necessary to protect the School against breaches of security.

6 Policy Awareness and Disciplinary Procedure

6.1 The Brief Guide to this policy will be given to all new members of staff (by HR, where appropriate) and to all new students (by the appropriate student support office). Existing staff and students of the School, authorized third parties and contractors given access to the School network will be advised of the existence of this policy statement and the availability of the associated procedures, codes of practice and guidelines which are published on the School website. Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

7 Supporting Policies, Procedures and Codes of Practice

7.1 Supporting polices, procedures and codes of practice amplifying this policy statement are published with it and are available on the School website. Staff, students, contractors and other third parties authorized to access the School network to use the systems and facilities identified in paragraph (1.4) of this policy, are required to familiarize themselves with these and to work in accordance with them. Guidance notes will also be published to facilitate this.

7.2 Personal data (as defined by the Data Protection Act 1998) must be stored securely; if such data is held on mobile devices (e.g. laptops) or removable media, it must be strongly encrypted, in compliance with the Data Protection Policy. Other forms of

sensitive business data, intellectual property, etc. should, similarly, be strongly encrypted. IT Services will issue, and keep under review, guidance on what constitutes an acceptable standard of encryption.

All mobile devices must be password protected.

7.3 Any outsourced IT support must be subject to a written contract which must comply with the guidelines in “Security considerations in outsourced IT arrangements”.

8 Status of the Information Management and Security Policy

The School’s senior management have approved this policy statement and delegated its implementation to Line Managers.