Guidelines 3

Security considerations in outsourced IT management arrangements

Approved with minor edits by ISWG - 5 May 2015

Arrangements involving third party access to LSHTM's computer systems should be set out in a formal contract to ensure compliance with the School's general and supplementary policies on Information Security and the accepted Codes of Practice.

A risk assessment should be carried out before entering into a contract with any supplier. Potential risks, particularly involving small companies, include non-performance, delays in attending on site, expertise being invested in a single person and under resourcing, for example, owing to other contractual obligations. Any Contract or Agreement should be drawn up by LSHTM, rather than by a Supplier; it should require acceptance of LSHTM Terms and Conditions. It is particularly important to reach agreement on public liability insurance and damage liability. The contract should list target time-scales, agree how evidence of work completed to schedule will be presented and specify payment penalties if schedules are not met.

The contract should be in place **before** access to any system is provided and a copy of the relevant policies and codes of practice provided to the vendor/ supplier (including the Information Management and Security Policy). Anyone with access to LSHTM systems is bound by the Information Management and Security Policy.

The following items should be considered for inclusion in the contract:

(a) a description of each computer system to be made available to the contractor;

(b) a requirement to maintain a list of individuals authorised to use the contracted service;

(c) the times and dates when the contracted service is to be available;

(d) the respective obligations, responsibilities and liabilities of the parties to the agreement;

(e) procedures regarding the protection of LSHTM's assets, Intellectual Property Rights and the confidentiality of the information contained therein;

(f) restrictions on the copying and disclosure of information;

(g) responsibilities to comply with current UK/EU legislation and LSHTM policies;

(h) conditions determining the right of access to the JANET network;

(i) the right of LSHTM to monitor and revoke user activity;

(j) measures to ensure the return or destruction of information and assets at the end of the contract; contractors must guarantee to erase all disks, tapes and other media returned to them (for example under warranty or field service exchange). Contractors must indemnify LSHTM against any liability arising from any failure of their data erasure procedures.

(k) responsibilities regarding hardware and software installation, maintenance and protection which must include a commitment to implement best-practice security procedures;

(l) involvement by the third party with sub-contractors and other participants.

Data Protection Act 1998

Note also the responsibilities of contractors and other third parties in relation to the processing of personal information on behalf of LSHTM, as set out in the LSHTM's Data Protection Policy and Procedures.