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.

(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.