LONDON SCHOOL of HYGIENE &TROPICAL MEDICINE

LSHTM Information Management and Security Policy - a summary

LSHTM's Information Management and Security Policy seeks to ensure information security within LSHTM and protect the confidentiality, integrity and availability of the School's data.
The policy has been approved by senior management and applies to all staff and students and anyone else who has been authorised to use our facilities.
The policy comprises a main policy and supporting policies such as the Data Protection Policy and the Acceptable Use Policy, as well as policies on email, connection to the LSHTM network and monitoring of activity on the network.

What do I need to know?

You must be aware of, and comply with, the policy as it forms part of the School's policies and procedures. Anyone with access to LSHTM systems has responsibility for protecting those systems - even if only to keep their password secret.

What can I and what can't I do?

The IT Acceptable Use Policy (AUP) sets out what you can and cannot do. It also defines what is considered reasonable personal use - this does not include commercial activity, activity which is illegal or is likely to cause offence, or which, because of volume or frequency, distracts from work. Personal use must not cause problems for other users, add significantly to running costs, or risk bringing the School into disrepute.
Breaches of policy can result in disciplinary action. If you are not sure about something, check with your manager or with IT services.

Data Protection and Information Handling

If you are going to be holding or working with data that can identify a living person, you must read and comply with the LSHTM Data Protection Policy. LSHTM can advise you as to appropriate data handling requirements depending on the sensitivity of information. Particular care may need to be taken when handling the information, e.g. when emailing or printing it.

Email

All staff and students should use LSHTM-provided email systems for School business. You may not use LSHTM-provided systems to send, for example, spam, chain letters or material which is offensive, inappropriate, defamatory, threatening or illegal. Further details are in the email policy.

Connecting to the Network

Any machine using the LSHTM network is subject to the LSHTM Information Security Policy. Further details in the network connection policy.

Monitoring
All staff and students should be aware that their computer usage on and through School systems may be monitored.
Any monitoring which takes place must be properly authorised in accordance with the LSHTM monitoring policy. Penalties for unauthorised monitoring are severe, including possible imprisonment

What if I have (or manage) my own computer?
You must ensure that you keep your machine up-to-date with patches and run appropriate anti-virus software on it.
If you don't know what to do, ask for help!

Disposal of Machines
If you are getting rid of a machine, then you must ensure that no data remains on it. All disks must be properly erased - simple formatting is not sufficient. Further information is available from IT Services.

Lost or Stolen IT Equipment
Any loss or suspected breach involving personal data must be reported to IT Security
Email: csirt@lshtm.ac.uk

Information security Information
See www.lshtm.ac.uk/its/informationsecurity for policies, procedures, good practice guides, training material and internal newsletters.

Contact us
Information security Problems or Questions?
If you have, or suspect you may have, a security problem, or just want to ask something, please let us know - either contact the IT Services helpdesk or, if it is of a particularly sensitive nature, the IT Security team.
IT Services Helpdesk
Email: ITSHelpdesk@lshtm.ac.uk
Tel: +44 (0)20 7927 2186
IT Security
Email: csirt@lshtm.ac.uk
Tel: +44 (0)20 7958 8396