Acceptable Use of Computer and IT Facilities within the Liverpool School of Tropical Medicine

Policy number	POL_IT002
Version:	5.0
Superseded Version:	4.0
Date approved by Audit Committee	29 June 2016
Originator	Director of IT Services
Date for Review:	June 2017

Target Audience	
People who need a detailed knowledge of the Policy	All staff of LSTM
People who need a broad understanding of the Policy	All students of LSTM
People who need to know that the Policy exists	Partners of LSTM and other stakeholders

Contents

1 Introduction and Context

The intention of the policy is to inform all staff and students about their responsibilities in handling corporate information, advise on risks and outline required actions.

The aim of the policy is to make all users aware of the importance of looking after LSTM's corporate information and data.

2 Scope

This policy applies to all staff, students and any visitors or contractors who may have access to LSTM information and/or IT services during the course of their work.

3 Roles and Responsibilities

In their use of Computer & IT facilities, LSTM staff and students must comply with:

- UK legislation;
- LSTM policies and regulations;
- JANET Acceptable Use Policy;

And must:

- Show consideration for the impact their use may have on other users.

4 Outline of risks

Many users will handle information and data as a routine part of their job, this may involve travelling abroad and carrying laptops or other mobile devices, processing information in an open-plan office or working from home. Use of personal devices for work purposes is not encouraged, however, there may be occasions when this is acceptable if certain criteria are fulfilled e.g. if working from home. Some advice on home working is included below. LSTM are able to provide all employees with the equipment they need to carry out their role and there are significant risks to its information assets being retained on non-LSTM owned devices.

Some examples of key issues and risks follow, however, the list is not intended to be exhaustive and if you have any concerns about information you are handling, please seek help and support from the contacts listed in section 7 below.

5 Passwords

Proper use of passwords is the first line of defence in the security of LSTM information assets. You will be required to create secure passwords to access almost all systems. The general principle is that if it is possible to password protect a device then you must do so.

6 Portable memory storage (including USB Sticks)

These are very useful for carrying around information for presentations e.g. Powerpoint or other documents. However, if using these to carry important LSTM information you should ensure that you use an encrypted drive. Information on the purchase of encrypted pen drives is available on Knowledge eXchange.

7 Smartphones

Smartphones are widely used to access email and files. It is only permissible to access LSTM email and files from a Smartphone after accepting a policy that installs software on the phone to allow IT Services to manage the security setting of the phone, including the remote wipe of data in the event of loss of the phone. If a phone is lost or stolen it must be reported to IT Services immediately.

8 Portable hard drives

While portable hard drives may appear a cheap and easy solution to back-up your PC or laptop they have a number of short-comings:

- They can fail and do
- They are not secure against theft, vandalism, fire or water damage

All LSTM data must be backed up on recognised corporate systems. These currently include the networked P: and S: drives; and *Dropbox for Business* operated by IT Services. If you have storage needs which cannot be accommodated using these methods you must discuss other options with IT Services.

9 Laptops

All laptops must be password protected and the hard drive must be encrypted. If a Laptop is lost or stolen it must be reported to IT Services immediately.

10 Screen visibility

If you are working in a public place or travelling so that your device may be visible to others, you should ensure that you do not access personal or confidential data. Steps you can take to reduce risks include:

- Use the Windows key + L to lock your computer before leaving it or if anyone approaches;
- Use a privacy filter

11 Home working

Home working presents a number of issues for security which staff should be aware of. If processing sensitive corporate or personal data you should ensure that other member of the household do not have access to it. Items could be at risk of theft from the home, whether papers of equipment such as laptops and this needs to be taken into account. You must use a virus detection package such as Sophos which is available from Knowledge exchange to download for home use.

You should never hold the LSTM documents or data on a personal home computer, documents should be held and accessed from Office365 portal if using a non-LSTM device.

12 Data Protection

Many of the issues of security relate to the Data Protection Act and you should also familiarise yourself with the LSTM policies on Knowledge exchange.

13 Cloud Computing

Office365 is the School official cloud based collaboration service and can be used for all information classed as public, private or confidential. It should not be used for information classed as restricted. There are many other cloud applications available often with no charge for the basic version. One of the most popular of these is “Dropbox Personal or Pro”. Staff are advised that there are security risks associated with the use of these, and potentially their use may breach the 8th principle of the Data Protection Act that personal information must not be transferred to other countries without adequate protection. The general advice for Dropbox is to only use “Dropbox for Enterprise” as the security settings are centrally controlled by IT Services.

14 Key corporate responsibilities

All staff and students have responsibility for the confidentiality, integrity and availability of corporate data. The daily execution and maintenance of Information Technology and Information Systems is delegated to IT Services under the direction of the Director of IT Services. IT Services staff will offer advice and guidance on best practice and check adherence to LSTM policies.

All LSTM employees have the responsibility to act in accordance with LSTM policies and procedures where applicable.

15 General personal responsibilities

Any staff member at LSTM who has cause to use corporate information has a responsibility to ensure that it is kept secure. Where access to information is controlled e.g. through authority levels and passwords, no one should knowingly contravene this. If a member of staff has higher than normal levels of authority e.g. as a system administrator, then it is incumbent on them not to abuse this.

If a member of staff has concerns about levels of the levels of security applied in their work area or group then they should raise it with their line manager in the first instance. Help and support is available from the contacts in the section below.

All staff and students must be aware of the requirements laid out in the LSTM Prevent Agenda Policy **POL008**. This policy is designed to protect staff and students from harm of radicalisation in any form and to provide a framework for support of all members of staff and students within the School. Use of IT facilities is monitored to ensure early intervention is possible in the event that someone in danger of harm from radicalisation.

All access to the internet via LSTM is monitored and reports are automatically produced when attempted access is made to sites that are blacklisted by LSTM. These include sites that may be linked to terrorist activities. Any reports of attempted access to blacklisted sites will be initially be investigated by IT Services to understand if the report is a false positive. If the attempted access is not deemed to be a false positive then the report will be forwarded to the current LSTM Prevent Officer who will raise the issue with the supervisor of the staff member or student who attempted to access the blacklisted site.

16 Use of Network services, e-mail, messaging and Internet services

Particular attention is drawn to the following. It is prohibited to use the School's resources and facilities to transmit:

commercial material unrelated to the business of the School, including the transmission of bulk e-mail advertising (spamming);

bulk non-commercial e-mail unrelated to the business which is likely to cause offence or inconvenience to those receiving it. This includes the use of e-mail list processors, where the e-mail sent is unrelated to the stated purpose for which the relevant e-mail list processor is to be used (spamming);

- unsolicited messages requesting others to continue forwarding such e-mail messages to others, where those e-mail messages have no educational or informational purpose (chain e-mails);
- messages which purport to come from an individual other than the user actually sending the message, or with forged addresses (spoofing);
- material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive;
- material that advocates or condones, directly or indirectly, criminal activity, or which may otherwise damage the University's reputation;

- text or images to which a third party holds an intellectual property right, without the express written permission of the right holder;
- material that is defamatory, libellous , harassing or threatening;
- LSTM has a statutory duty, under the Counter Terrorism and Security Act 2015, termed “PREVENT”. The purpose of this duty is to aid the process of preventing people being drawn into terrorism and as such, you must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. LSTM reserves the right to block or monitor access to such material. (Please refer to UCISA guidelines)
- material that could be used in order to breach computer security, or to facilitate unauthorised entry into computer systems;
- material that is likely to prejudice or seriously impede the course of justice in UK criminal or civil proceedings;
- material containing personal data (as defined by the Data Protection Act 1998) about third parties, unless their permission has been given explicitly, in the case of sensitive personal data, that data is adequately protected and this use of the data has been formally notified to the Information Commissioner by the School, or the information is covered by a relevant exemption under the Act;
- communications that by intent or otherwise harass the recipient.

In line with School policy, it is noted that the prime purpose of the LSTM computing facilities are for the conduct of LSTM business, however, some occasional use of e-mail facilities for personal use is permitted as long as this does not disrupt or distract the individual from the conduct of LSTM business or restrict the use of those facilities to other legitimate users.

17 Security of LSTM data

LSTM takes the matter of data security very seriously all staff are the effective custodians for LSTM intellectual property (IP) in the form of reports, data and other documents. It is, therefore, imperative that you take best care of these by saving them to a backed up facility. Normally, this would be your P: or S: drive. In certain instances e.g. when travelling this may not be possible and there is now software available called Crashplan Pro available to assist you in these circumstances. For details of the LSTM departmental filestore available please contact the LSTM Help Desk.

18 Electronic Publishing

Anyone who has access to the LSTM Network, and hence to the internet, is in a position to “publish” material. This could take the form of sending an e-mail or contributing to a website or Social media. As this can be identified as coming from the LSTM network the individual is responsible for any for the content of the publication.

Staff are advised to ensure that nothing published should contravene statutory legislation, LSTM or JANET acceptable use policies.

Anyone publishing an item has “editorial responsibility”; issues such as when an opinion is that of the individual and not LSTM’s should be clearly expressed.

Attention is drawn to the need to comply with the Copyright, Design and Patents Act 1988.

19 Use of Wireless Networking Facilities

Wireless networking is now provided across most of LSTM. It is prohibited to attach private wireless networks to the main LSTM network, and hence to JANET and the internet and these will be removed by IT Services staff if identified.

Guest wireless accounts for visitors are available from reception, and are valid for one week.

20 Use of Licensed Software

All software installed on LSTM / University hardware and infrastructure must be legally compliant.

21 Legal framework

LSTM has a duty to abide by and adhere to relevant UK legislation. Of particular relevance to this policy are the Computer Misuses Act 1990 and the Data Protection Act 1998. Other relevant legislation in this area that you should be aware of includes:

- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Copyright, Design and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- The Terrorism Act 2000
- The Anti-Terrorism, Crime and Security Act 2001
- Official Secrets Acts 1911-1989
- Counter-Terrorism and Security Act (Feb 2015) Including the PREVENT duty for HEIs.
- Obscene Publications Act 1994

22 Enforcement

An initial breach of the policy may be dealt with in an advisory way and the reasons for non-compliance explained. However, if a breach is considered to be serious in nature and/or you subsequently breach the policy, further action will be initiated, which for staff and students may include formal disciplinary action including dismissal.

23 Help & support

Help and support is available via the IT Services Help desk which can be accessed via Knowledge eXchange or telephone x 3250.

For Data Protection Act support please contact Julia Martin or telephone x 3191.

Annex of Modifications		
Version	**Date of issue**	**Details of modification from previous version**
1.0	01.06.09	
2.0	01.11.13	
3.0	01.11.15	
4.0	28.06.16	**Updates from 3.0 to 4.0 to include provision of the HEFCE PREVENT agenda.**
5.0	28.06.16	**Updates from 4.0 to 5.0 to include guidelines from Universities and Colleges Information Systems Association (UCISA)**