LSHTM Information Management and Security Policy Supporting policy: Acceptable Use Policy

Document Type	Policy
Document owner	Phil Rogers, Head of Information Security & IT Compliance
Approved by	Executive Team
Approval date	Feb 2023
Review date	05/11/2022
Version	3.1
Amendments	05/11/2022 Minor changes and correction.
Related Policies & Procedures	https://www.lshtm.ac.uk/aboutus/organisation/information-management-and-security

1 INTRODUCTION

1.1 Purpose

1.1.1 LSHTM depends heavily on its Communications and Information Technology (C&IT) services for its research, teaching and administrative activities. These services are funded on condition they are used for legitimate, authorised purposes, and the School may be required from time to time to demonstrate to external auditing bodies that it has mechanisms in place to manage, regulate and control them. The main purpose of this policy is to define what constitutes acceptable use; to encourage the responsible use of facilities; to maximise the availability of resources (equipment, infrastructure and staff) for legitimate purposes; and to minimise the risk of misuse from inside or outside LSHTM.

1.1.2 This policy incorporates the Janet acceptable use policy. Janet is the name given to an electronic communications network and associated electronic communications networking services and facilities that support the requirements of the UK education and research communities. The full text of their policy can be found at: https://community.jisc.ac.uk/library/acceptable-use-policy

1.1.3 There are also various laws and directives that govern the use of C&IT, and others that make explicit reference to C&IT. These are mentioned in more detail later. LSHTM has a duty to bring these to the attention of its staff and students.

1.1.4 If you are not sure whether something you are planning to do might contravene these regulations, check first with your line manager (in the case of staff) or tutor (in the case of students), or seek help from the IT Services Help Desk before proceeding.

1.2 Scope

This policy covers the use of all C&IT services and facilities provided by LSHTM or by third parties on behalf of the School. For the purposes of clarification, these include, but are not limited to:

a. all computers irrespective of ownership when connected to the School communications network;
b. services run by IT Services which may be used by any member of the School. All users of these services must be registered with IT Services;

c. facilities and systems operated by departments for academic research, teaching and administration. Arrangements for use of these facilities are made through the department concerned and are normally restricted to its own staff and students;

d. content hosted on the School's C&IT facilities which is accessible via the internet by members of the public;

e. services operated by third parties on behalf of the School.

Software obtained under an educational licence agreement may also be subject to the terms of these regulations (see, for example, section 3.1 below). They do not, however, apply to other organisations whose traffic the School relays by formal arrangement, unless the terms of an arrangement stipulate otherwise. In the case of sponsored sites, regulations will be established by agreement.

2 AUTHORISED USE

2.1 In this policy, "authorised use" is defined as:

a. for students, use properly associated with the LSHTM programme of study or course for which a student is registered; and reasonable personal use;

b. for employees, use in the course of or properly and directly associated with their employment; and reasonable personal use;

c. for honorary staff, use properly associated with their appointment; and reasonable personal use;

d. for trades union business, use properly associated with union activities;

e. for users who are neither staff nor students, including visitors, use restricted to those purposes specified in the case made for registration.

2.2 Reasonable personal use is defined as incidental and occasional use which does not:

a. disrupt or distract the individual from the efficient conduct of School business (i.e. due to volume, frequency, time expended or time of day used);

b. involve accessing, downloading, storing or sending offensive or inappropriate material or information, or is such as to amount to a criminal or civil offence examples of which are listed in Regulation 3(d);

c. restrict the use of those systems by other legitimate users;

d. risk bringing the School into disrepute or placing the School in a position of liability;

e. add significantly to running costs; or

f. breach the Regulations set out in paragraph 3.

Any use that falls outside of these definitions is prohibited and may lead to LSHTM disciplinary procedures being invoked and may expose you to court proceedings attracting both criminal and civil liability. You may be held responsible for any claims brought against LSHTM and any legal action to which the School is, or might be, exposed as a result of your unauthorised use.

3 REGULATIONS

3.1 C&IT users **must**:

a) respect the copyright of all materials and software that are made available by LSHTM service providers and third parties for authorised use;

> *Users must not make, run or use unlicensed copies of software or data. They should only download data or datasets where they are explicitly permitted to do so. They must abide by the User Acknowledgement of Third Party Rights (the document is available from this page on the Chest website: https://www.chest.ac.uk/user-obligations/), arrangements by Jisc collections (https://www.jisc.ac.uk/jisc-collections), Copyright Law (Copyright, Designs and Patents Act 1988) and by any specific conditions of use imposed by the owners or suppliers of software or data. In particular users should be aware that, unless otherwise stated, software and datasets provided by LSHTM should only be used for LSHTM educational purposes.*

b) familiarise themselves, and comply, with the requirements of the Data Protection Act and School policy, most especially the obligation to notify LSHTM's Archivist and Records Manager of any relevant data holdings.

> *Data Protection laws protect individuals against the unauthorised use or disclosure of their data. The school is registered with the UK Data Protection authorities. The processing, misuse or disclosure of an individual's data outside LSHTM's registration may amount to a criminal offence.*

c) comply with the Computer Misuse Act 1990 which makes activities such as hacking or the deliberate introduction of viruses a criminal offence;

> *Hacking is defined here as the unauthorised use of a computer system (locally or through a network), or the use of resources that have not been allocated, with intent to access, modify or damage another's files or system files, or to deny service to legitimate users, or to obtain or alter financial or administrative records, or to facilitate the commission of a crime.*

d) have the written approval of their Head of Department where activities which might be subject to legislation are carried out in pursuit of legitimate, approved academic research (for example, work involving the use of images which may be considered obscene or indecent, or research into computer intrusion techniques)

e) take all reasonable precautions to prevent the introduction of any virus, worm, Trojan Horse or other harmful program to any computer, file or software;

f) abide by all other applicable supporting policies of the Information Management and Security Policy.

3.2 C&IT users **must not**:

a) use material or programs in a way which is unlawful, defamatory or invasive of another's privacy;

b) use the C&IT services and facilities in such a way as to risk or to cause loss, damage or destruction of data or breaches of confidentiality of data;

c) use the C&IT services and facilities in a way which infringes any patent, trademark, trade

secret, copyright, moral right, confidential information or other proprietary right of any third party;

d) jeopardise the provision of services (for example by inappropriate use of bulk e-mail, or by recreational use that deprives other users of resources);

e) publish, create, store, download, distribute or transmit material that is offensive, obscene, indecent or unlawful. Such materials will always include, but at LSHTM's discretion may not be limited to, items deemed to be offensive, obscene, indecent or unlawful under The Obscene Publications Act 1959, Equality Act 2010, Harassment Act 1997, The Protection of Children Act 1978, The Public Order Act 1986, the Criminal Justice and Public Order Act 1994 and the Terrorism Act 2006. Attention is also drawn to The Counter-Terrorism and Security Act 2015 (Commencement No. 1) Regulations 2015 which requires universities and colleges to have "due regard for the need to prevent people being drawn into terrorism".

f) use IT facilities in a way that brings or could bring LSHTM into disrepute. This includes associating the School with external facilities such as Web sites that could bring the School into disrepute by association, for example by embedding LSHTM email addresses in such sites, or by providing hyperlinks from LSHTM web sites to such sites;

g) disclose passwords to others, or use accounts or passwords belonging to others, or otherwise circumvent registration procedures;

> The term "password" is here taken to refer to any authentication credential issued by LSHTM, and includes both hardware tokens and cryptographic keys. Users will be held personally liable and may be subject to disciplinary proceedings for any misuse of their account resulting from the disclosure of passwords to others.

h) access or attempt to access computers or computing services at LSHTM or elsewhere for which permission has not been granted, or facilitate such unauthorised access by others;

i) attempt to circumvent any firewall or software designed to protect systems against harm;

j) interfere, or attempt to interfere, with or destroy systems or software set up on public facilities (this includes loading, or attempting to load, unauthorised software on to any LSHTM C&IT facilities);

k) interfere with, disconnect, damage or remove without authority any equipment made available for use in conjunction with any LSHTM C&IT facilities;

l) set up equipment to provide services that they are not competent to administer, especially if such services result in security vulnerability or exposure to misuse;

m) use mobile phones, smoke, eat or drink (except for bottled water) in LSHTM computer rooms;

n) interrupt teaching sessions when a computer room has been booked for this purpose.

LSHTM does not tolerate discrimination or harassment in any form whatsoever. This principle extends to any information distributed via any LSHTM C&IT system or via the Internet. You may not store on, or transmit from, any system any material which discriminates or encourages discrimination or harassment on racial or ethnic grounds or on grounds of gender, sexual orientation, marital status, age, ethnic origin, colour, nationality, race, religion, belief or disability.

Breaches of this policy will lead to disciplinary action. In the event that you receive or become aware of obscene, indecent, offensive, inflammatory, discriminatory or socially offensive material, you should notify the relevant person set out in paragraph 5.2.

Failure to comply with these regulations may lead to disciplinary action and may expose you to court proceedings attracting both criminal and civil liability. You will be held responsible for any claims brought against LSHTM and any legal action to which the School is, or might be, exposed as a result of your unauthorised use.

4 CONDITIONS OF USE

Use of LSHTM C&IT facilities is subject to the following conditions. Additional conditions may apply to locally managed systems; it is the responsibility of those managing such systems to make their users aware of any local regulations.

4.1 The facilities (including software) are provided entirely at the risk of the user. The School will not be liable for loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), damage (including damage to hardware, software or data) or inconvenience arising directly or indirectly from the use of the facilities, except where statutory health or safety matters are involved.

4.2 Whilst LSHTM's information management and security policy requires providers of computing facilities to employ appropriate security measures to prevent unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data, LSHTM cannot, and does not, give any warranties or undertakings to the user about security, confidentiality or integrity of data, personal or other. The same applies to any other electronic material submitted to or processed on facilities provided or managed by LSHTM or otherwise deposited at, or left on, its premises.

4.3 LSHTM accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or the invalidation of any warranty agreement) to equipment not owned by the School as a consequence of any work carried out on such equipment by members of staff (or students acting in the capacity of members of staff), whether authorised or not.

4.4 LSHTM accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or invalidation of any warranty agreement) to equipment not owned by the School as a consequence of direct or indirect connection, whether authorised or not, to the School's networks. The user shall indemnify LSHTM for any loss or damage, whether direct or indirect, malicious or inadvertent, suffered or incurred as a consequence of the interconnection of any hardware or software not owned by or under the control of LSHTM with any IT system, hardware, software or data owned or controlled by LSHTM.

4.5 LSHTM reserves the right to inspect, monitor, copy and/or remove user data in order to investigate operational problems or for the detection and investigation of suspected misuse. This includes the authorised interception and monitoring of communications as provided for by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under the Regulation of Investigatory Powers Act 2000.

Any monitoring of systems or networks may be carried out **only** in accordance with the LSHTM Policy on Monitoring Computer and Network Use.

For the avoidance of doubt, this does not preclude third parties who operate services on behalf of LSHTM from carrying out lawful monitoring and disclosure on their systems and networks.

It is important to be aware that communications on or through LSHTM's computer systems may be monitored or recorded to secure effective system operation and for other lawful practices. For example, monitoring of user accounts might occur if LSHTM has reason to believe that its computer facilities were being misused to send unsolicited commercial email.

4.6 LSHTM reserves the right to check for insecure and vulnerable systems and to block access to systems and/or services (ports) which place at risk the integrity of its network or services, or which may pose a threat to third parties.

4.7 LSHTM reserves the right to disconnect poorly managed equipment from the departmental LAN or, in extreme cases, disconnect the departmental LAN from the LSHTM core network until the offending machine is disconnected or shown to be configured correctly.

4.8 Any form of electronic communication may be construed in law as a publication and LSHTM Code of Practice will apply. Users must be aware of the implications with respect to Intellectual Property Rights of publishing information in any electronic form.

5 PROCEDURES FOR DEALING WITH MISUSE OR SUSPECTED SECURITY VIOLATIONS

5.1 In the event of suspected misuse of C&IT facilities, LSHTM reserves the right to suspend user accounts and to inspect, monitor, copy or remove users' files if necessary. LSHTM may also disconnect network services and prevent access to the facilities without notice while investigations proceed.

5.2 Cases of misuse or abuse should be reported to, and will be taken up in the first instance by, the appropriate authority shown below:

Misuse by:	Report in the first instance to:
Students	Registry; CSIRT must also be informed. For distance learning students, report also to Distance Learning Team of Division of Education
Staff	Head of Department; CSIRT must also be informed.
Other (e.g. external attack or contractor misuse)	CSIRT

5.3 The Head of Department and LSHTM authorities, including the Registrar where appropriate, may be informed and will deal with the incident under the appropriate disciplinary procedures for students and staff. In some cases legal action may be taken and the Police informed. LSHTM reserves the right to disclose data or information about an individual's use of the School's computing facilities to any appropriate or authorised third party (including the police) to assist in any further investigation.

5.4 If websites containing material that may be illegal are discovered, particularly material

relating to children or the exploitation of children, LSHTM encourages its staff and students to make a report to the authorities named above or to the Internet Watch Foundation (IWF) hotline (http://www.iwf.org.uk). The normal course of events is that the IWF will request that the Internet Service Providers (ISPs) in the UK will block that site. If this does not happen the IWF will inform the Police who may investigate the matter further.

5.5 Actual or suspected security violations should be reported immediately to the LSHTM computer security staff (email csirt@lshtm.ac.uk). No attempt should be made to investigate security vulnerabilities unless or until appropriate authority has been obtained.

6 FURTHER INFORMATION

6.1 Status of this document

This document has been approved by LSHTM's Information Security Working Group and endorsed by the Senior Leadership Team/Academic Affairs Committee. It is subject to regular review by the LSHTM Information Security Working Group.

The enrolment form signed by students explicitly binds them to abide by LSHTM Regulations for use of Networked Computing Services which will be superseded by this AUP and the overarching Information Management and Security Policy. LSHTM staff are also obliged to abide by this AUP as a condition of employment. Users of C&IT services who are neither staff nor students are also bound by the Information Management and Security Policy.

In all cases, the act of registering as a user of the Information Systems facilities or making use of any of the C&IT facilities implies acceptance of conditions of use and compliance with regulations, relevant Acts of Parliament and other applicable laws and directives.

From time to time LSHTM may issue good practice guidelines and reserves the right to withdraw network services to systems or services that are not operated in accordance with those guidelines.

6.2 LSHTM policy on connecting equipment to the LSHTM network

Additional regulations covering the connecting of equipment to the LSHTM network are given in other policies. Links to those policies are available from the following page: https://www.lshtm.ac.uk/aboutus/organisation/information-management-and-security

7. VERSION CONTROL

Version Number	Author/Reviewed by	Approved by	Purpose/Change	Date
1.0	IT Services	Management Board	Initial policy	November 2016
2.0	Jim Nicholas	Management Board	Policy review	04/03/2020
2.1	Abu Hossain (Information Security Manager)		Policy review	24/06/2021
3.0		Management Board		30/06/2021