Technical

Conditions of Use of the Residences Network

Overview

Any user of provided network facilities in LSE Halls of Residence must still abide by:

- LSE's Information Security Policy
- The Conditions of Use of IT Facilities at LSE
- Jisc's Acceptable Use Policy

In particular, you must not distribute offensive material, illegally copy software, breach copyright or send mass unsolicited email messages.

In addition, the following conditions of use also apply. Your attention is drawn to the fact that a failure to adhere to these conditions may result in the withdrawal of your access rights.

Scope

Network connections in LSE-run Halls of Residence

Out of Scope

Non-LSE Halls of Residence

Policy

Connections

Wireless

- The primary means of connection is wireless via eduroam.
- Users without LSE accounts must use The Cloud for wireless connections.
- Non-LSE Halls may have 3rd party wireless providers, who will supply their own terms and conditions.

Wired

- LSE Halls also have one wired socket per room.
- Residents can register devices to use this via a self-service portal.

- Registration requires an LSE account.
- Wired provision provides a connection out to the Internet.

Use

1. The registrant is responsible for all network traffic to and from the registered network device.
2. When using LSE-supplied networks, residents shall not alter any network configuration parameters assigned by or notified to LSE systems for their device unless specifically instructed to do so by a member of DTS.
3. The default provision from LSE-supplied networks is Internet access only.

Service

DTS will endeavour to provide a reliable and robust connection to the School network and the Internet, however, this cannot be guaranteed and acceptance of these terms and conditions in no way constitutes a guarantee of uninterrupted service.

Security and Monitoring

In order to detect and prevent potential or exploited network vulnerabilities, DTS may perform regular monitoring, scanning, or probing of devices connected to the network. In using the network connection you are giving your consent to this activity and to the remedial actions described below.

Residents are responsible for the security of their own network devices. Security guidelines are available from LSE's Information Security pages. DTS reserves the right to disconnect a network device if it is deemed to be a threat to security or in breach of policy.

Installation or connection of any type of port scanner or packet sniffing technology to the LSE network for any reason is forbidden.

Remedial Action

DTS may take remedial action as a result of any of the following:

- Regular monitoring of the volume of network traffic and other factors that may have an impact on network performance and reliability indicate that further investigation is necessary.
- Receiving a complaint from an individual or organisation.
- Receiving notification that an account or a device account is compromised, or otherwise poses a security risk to the network and/or other network users.

Action(s) taken as a result of monitoring, scanning or probing could be any one or more of the following:

- Notifying the user of a problem and requesting action to be taken within a stated period of time.
- Further analysis of the source of network traffic to determine the nature of the suspected problem (e.g. high volume of network traffic being caused by file sharing programs and associated copyright infringement).
- Disabling the network connection associated with the equipment.
- Disabling the user's LSE account

Document control

Version: 2.1

Distribution list

Name	Title	Department
Laura Dawson	Director of Data and Technology Services	DTS
Information Governance Management Board		

External document references

Title	Version	Date	Author
Information Security Policy	3.20	05/07/19	Jethro Perkins
Conditions of Use of IT Facilities at LSE	3.4	11/11/2019	Jethro Perkins
Jisc Acceptable Use Policy (https://community.jisc.ac.uk/library/acceptable-use-policy)	12	May 2016	Jeremy Sharp

Version History

Date	Version	Comments
unknown	1	Legacy version on website. Predates existing staff
06/01/20	2	Initial attempt at update.
08/01/20	2.1	Incorporating changes after meeting with the Network Manager

Contacts

Position	Name	Email	Notes
Assistant Director of Cyber Security & Risk Management	Jethro Perkins	j.a.perkins@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	**Yes**
Will training needs arise from this policy	**Yes**
Annual awareness-raising activities from comms – e.g. via newsletters, maildrops, posters. Principles incorporated into LSE's user awareness training.	

Appendix A: Summary of relevant legislation

The Computer Misuse Act 1990

Defines offences in relation to the misuse of computers as:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

The Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA2000) is a general right of public access to all types of recorded information held by public authorities in order to promote a culture of openness and accountability.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use of communications data and can be invoked in the cases of national security, and for the purposes of detecting crime, preventing disorder, public safety and protecting public health.

Defamation Act 1996

"Defamation is a false accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation's reputation from harm.[1]"

Obscene Publications Act 1959 and 1964

The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape or torture.[2]

Protection of Children Act 1978, Criminal Justice Act 1988, Criminal Justice and Immigration Act 2008

The Protection of Children Act 1978 *prevents the exploitation of children by making indecent photographs of them and penalises the distribution and showing of such indecent photographs.* Organisations must take appropriate steps to prevent such illegal activities by their workers using their digital systems and networks.

The definition of 'photographs' include data stored on a computer disc or by other electronic means which is capable of conversion into an image.

It is an offence for a person to […] distribute or show such indecent photographs; or to possess such indecent photographs, with a view to their being distributed or shown by himself or others.

Section 160 of the Criminal Justice Act 1988 made the simple possession of indecent photographs of children an offence. Making an indecent image of a child is a serious arrestable offence carrying

---

[1] "Defamation", *Paradigm*, (2008) http://www.paradigm.ac.uk/workbook/legal-issues/defamation.html [accessed 01/05/15]

[2] "Obscene Publications Act 1959 and 1964", *Internet Watch Foundation*, https://www.iwf.org.uk/hotline/the-laws/criminally-obscene-adult-content/obscene-publications-act-1959-and-1964 [accessed 01/05/15]

a maximum sentence of 10 years imprisonment. Note: The term "make" includes downloading images from the Internet and storing or printing them out.[3]

Terrorism Act 2006

The Terrorism Act 2006 makes it an offence to write, publish or circulate any material that could be seen by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism.

It also prohibits the writing, publication or circulation of information which is likely to be useful to any one or more persons in the commission or preparation of terrorist acts or is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the purpose of being so useful.

In addition, it prohibits the glorification of the commission or preparation (whether in the past, in the future or generally) of terrorist acts or such offences; and the suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances.

Counter-Terrorism and Security Act 2015 – Statutory Guidance

The statutory guidance accompanying the Counter-Terrorism and Security Act 2015 (Prevent duty guidance for higher education institutions in England and Wales https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance_For_Higher_Education__England__Wales_.pdf) requires LSE to have “due regard to the need to prevent people from being drawn into terrorism.” The Act imposes certain duties under the *Prevent* programme, which is aimed at responding to “the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views.” The Prevent programme also aims to provide “practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support”. LSE must balance its existing legal commitments to uphold academic freedom and (under the Education (No. 2) Act 1986) freedom of speech within the law against its Prevent duty, and seek to ensure that its IT facilities are not used to draw people into terrorism.

General Data Protection Regulation

The GDPR has applied in the UK from 25 May 2018, and is incorporated into the UK Data Protection Act 2018. The GDPR reinforces and extends data subjects’ rights as laid out in the Data Protection Act (1998), and provides additional stipulations around accountability and governance, breach notification and transfer of data. It also extends the maximum penalties liable due to a data breach, from £500,000 to 4% global turnover.

The GDPR requires LSE to maintain an Information Asset Register, to ensure where personal data is voluntarily gathered people are required to explicitly opt in, and can also easily opt out. It requires data breaches to be reported to the Information Commissioner’s Office within 72hrs of LSE becoming aware of their existence.

[3] “Protection of Children Act 1978 (and 1999)”, *EURadar* (2011), http://eradar.eu/protection-of-children-act-1978/ [accessed 01/05/15]