



Information Security Policy

Foreword to the Information Security Policy

As a leading higher education institution committed to both high quality teaching and research, LSE has an ethical, legal and professional duty to ensure that the information it holds conforms to the principles of confidentiality, integrity and availability. We must ensure that the information we are responsible for is safeguarded against inappropriate disclosure; is accurate, timely and attributable; and is available to those who should be able to access it.

The Information Security Policy below provides the framework by which we take account of these principles. It enables the LSE community to understand both their legal *and* ethical responsibilities concerning information, and empower them to collect, use, store and distribute it in appropriate ways.

This policy is the cornerstone of LSE's on-going commitment to enhance and clarify our information security procedures. It has my full support and I encourage all LSE staff and students to read it and abide by it in the course of their work.

Professor Eric Neumayer
President and Vice Chancellor (Interim)

1. Introduction

The confidentiality, integrity and availability of information are critical to the functioning and good governance of LSE. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for LSE to recover.

This information security policy outlines LSE's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the School's information systems, and will be applied to all electronic information assets for which LSE is responsible.

Supporting policies, codes of practice, procedures and guidelines provide further details, and can be found on LSE's [Policies and Procedures](#) page.

LSE is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract.

1.1 Objectives

The objectives of this policy are to:

1. Provide an information security framework covering all LSE information systems (including but not limited to all Cloud environments commissioned or run by LSE, onsite and offsite computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems. It requires that:
 - a. The resources required to manage such systems will be made available, and
 - b. Continuous improvement of LSE's Cyber Security Strategy, systems and tools will be undertaken
2. Provide the principles by which a safe and secure information systems environment can be established for staff, students and any other authorised users.
3. Make users aware of, and enable them to comply with, all current and relevant UK and (*where appropriate*) EU or other legislation.
4. Ensure that all users understand their responsibilities for protecting the confidentiality and integrity of the data that they handle.
5. Protect LSE from liability or damage through the misuse of its IT facilities.
6. Maintain research data and other confidential information provided by suppliers at a level of security commensurate with its classification, including upholding legal and contractual requirements around information security.
7. Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

1.2 Scope

This policy is applicable to all staff, students, other members of the School and third parties who interact with information held by LSE and the information systems used to store and process it.

This includes, but is not limited to:

- Cloud systems developed or commissioned by LSE,
- systems or data attached to LSE networks,
- systems managed by LSE,
- mobile devices used to connect to LSE networks or hold LSE data,

- data over which LSE holds the intellectual property rights,
- data over which LSE is the data controller or data processor (wherever held).

2. Policy

2.1 Information security principles

The following information security principles provide overarching governance for the security and management of information at LSE.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability (see *Section 2.3. Information Classification*) and in accordance with relevant legislative, regulatory and contractual requirements.
2. Users with responsibilities for information (see *Section 3. Responsibilities*) must:
 - a. handle that information in accordance with its classification level;
 - b. abide by LSE policies, procedures, and any contractual requirements.
3. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.
 - a. Access to information will be on the basis of *least privilege* and *need to know*.
4. Information will be protected against unauthorized access and processing.
5. Breaches of this policy must be reported (see *Section 2.7. Incident Handling*).
6. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual external audits and penetration testing.

2.2 Legal & Regulatory Obligations

1. The London School of Economics has a responsibility to abide by and adhere to all current UK and (where appropriate) EU legislation as well as regulatory and contractual requirements.
2. A non-exhaustive summary of the legislation that contributes to the form and content of this policy is provided in *Appendix A*.

2.3 Information Classification

1. The following table provides a summary of the information classification levels that have been adopted by LSE and which underpin LSE's 6 principles of information security.
2. These classification levels explicitly incorporate the UK General Data Protection Regulation's definitions of *Personal Data* and *Special Categories of Personal Data*, as laid out in LSE's [Data Protection Policy](#), and are designed to cover both primary and secondary research data.
3. The [Data Classification Standard](#) provides detailed information on information classification levels and appropriate security controls.
4. Information may change classification levels over its lifetime, or due to its volume – for instance:
 - a. student grades classed as Confidential prior to release become Public after release.
 - b. NHS patient data aggregated to a higher level (so that, for instance, there is one observation for each GP Practice, or Hospital) is considered Confidential if any observations created using 5 or fewer patient-level observations are present,
 - i. but is *not* considered confidential if any such observations are either not present, or are dropped from the dataset
 - c. A dataset of names, addresses and telephone numbers that grows over 1000 records moves from Restricted to Confidential

Security Level	Definition	Examples	FOIA2000 status
1. Confidential	Normally accessible only to specified members of LSE staff. Should be held in an encrypted state outside LSE systems; may have encryption at rest requirements from providers.	<ol style="list-style-type: none"> 1. GDPR-defined <i>Special Categories</i> of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record) including as used as part of primary or secondary research; 2. patient-level observations; 3. aggregated patient data containing observations created using 5 or fewer patient-level observations; 4. passwords; 5. large aggregates of personally identifying data (>1000 records) including elements such as name, address, telephone number. 	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
2. Restricted	Normally accessible only to specified and / or relevant members of LSE staff or the student body	<ol style="list-style-type: none"> 1. GDPR-defined <i>Personal Data</i> (information that identifies living individuals including home / work address, age, telephone number, schools attended, photographs); 2. Name, email, work location, work telephone number; 3. reserved committee business; 4. draft reports, papers and minutes; 5. systems 6. internal correspondence 7. information held under licence 8. company policy and procedures (as appropriate to the subject matter) 	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
3. Public	Accessible to all members of the public	<ol style="list-style-type: none"> 1. Annual accounts, 2. minutes of statutory and other formal committees, 3. pay scales etc. 4. Experts' Directory 5. Course information 6. Information available on the LSE website or through the LSE's Publications Scheme. 7. company policy and procedures (as appropriate to the subject matter) 	Freely available on the website or through the LSE's Publication Scheme.

2.4 Suppliers

All LSE's suppliers will abide by LSE's Information Security Policy, or otherwise be able to demonstrate corporate security policies and / or appropriate information security certifications (e.g. ISO27001, Cyber Essentials Plus) providing equivalent assurance. This includes:

- when accessing or processing LSE assets, whether on site or remotely
- when subcontracting to other suppliers.

2.5 Cloud Providers

Under the UK GDPR, a breach of personal data can lead to a fine of up to 4% of global turnover. Where LSE uses Cloud services, it retains responsibility as the data controller for any data it puts into the service, and can be fined for a data breach, even if this is the fault of the Cloud service provider.

LSE also bears responsibility for contacting the Information Commissioner's Office concerning any breach of its data, as well as any affected individual. LSE must therefore be able to judge the appropriateness of a Cloud service provider's information security provision. This leads to the following stipulations:

1. All providers of Cloud services to LSE must respond to LSE's Cloud Assurance Questionnaire prior to a service being commissioned, in order for LSE to understand the provider's information security provision.
 - a. No cloud services contract will be approved by the Procurement team without either:
 - i. A completed Cloud Assurance Questionnaire, with approval given for use of the service by the Information Security Team; or
 - ii. Written approval from the Information Security Team that the contract can be commissioned.
2. Cloud services used to process personal data will be expected to have ISO27001 certification or equivalent controls, with adherence to the standard considered the best way of a supplier proving that it has met the UK GDPR principle of privacy by design, and that it has considered information security throughout its service model.
3. Any request for exceptions, where the standards of security cannot be demonstrated to meet ISO27001 will be considered by LSE's Risk Manager and the Chief Operating Officer.

2.6 Compliance, Policy Awareness and Disciplinary Procedures

1. Compliance with this policy is mandatory.
2. Mandatory user awareness training will accompany this policy.
3. All current staff, students and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines.
4. Any security breach will be handled in accordance with all relevant School policies, including the [Conditions of Use of IT Facilities at the LSE](#) and the appropriate disciplinary policies.

2.7 Incident Handling

1. If a member of the School is aware of an information security incident then they must report it to the DTS Service Desk at tech.support@lse.ac.uk or telephone 020 7107 5000.
2. Breaches of personal data will be reported to the Information Commissioner's Office by LSE's Data Protection Officer (DPO). The DPO can be contacted at glpd.info.rights@lse.ac.uk.
3. All members of the School Community must report instances of actual or suspected phishing to phishing@lse.ac.uk

2.8 Supporting Policies, Codes of Practice, Procedures and Guidelines

1. Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available on LSE's Policies and Procedures [website](#).

2. All staff, students and any third parties authorised to access LSE's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

2.9 Review and Development

1. This policy will be reviewed annually by the appropriate LSE Management Board and updated regularly to ensure it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.
2. Additional policy may be created to cover specific areas.

3. Responsibilities

Members of LSE:

All members of LSE, LSE associates, agency staff working for LSE, third parties and collaborators on LSE projects will be users of LSE information. This carries with it the responsibility to abide by this policy, supporting policies and relevant legislation. No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so. To report data breaches, please see *Section 2.5: Incident Handling*

Business Led Technology Teams:

Responsible for the information systems (e.g. HR/ Registry/ Finance) both manual and electronic that support LSE's work. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and either mitigated or explicitly accepted, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.

Principal Investigators / Project administrators:

Responsible for the security of information produced, provided or held in the course of carrying out research, consultancy or knowledge transfer activities. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and mitigated, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms.

Professional service leads, Departmental managers / Line managers:

Responsible for specific area of LSE work, including all the supporting information and documentation that may include working documents/ contracts/ staff or student information.

Director of Research and Innovation

Signs off LSE research contracts and is responsible for providing the assurance that any mandated security measures for research data are met.

Procurement Team

Ensuring any requests for purchase of IT service and cloud contracts have been authorised by the Information Security Team.

School Secretary

Responsible for LSE compliance with the UK General Data Protection Regulation

Records Manager / Data Protection Officer

Responsible for data protection and records retention issues. Breach reporting to ICO

DTS:

Responsible for ensuring that the provision of LSE's IT infrastructure, cloud environments and applications is consistent with the demands of this policy and current good practice.

Estates Security Team:

Responsible for physical aspects of security.

Cyber Security Team:

Responsible for assurance activities, pen testing, information security policies and specialist information security advice. Incident response for cyber security issues. User awareness.

Information Governance Management Board

Responsible for approving information security policies

Data and Technology Management Board

Responsible for approving technology policies.

Document control

Last reviewed by DTMB: 16/05/2022

Version History

Date	Version	Comments
12/10/16	3.13	Changed 'Purpose' to 'Objectives'. Made more explicit the commitment to continual improvement, including via internal audits and pen testing. Included explicit reference to NHS patient data in the data classification. Added in commitment to satisfy third party data providers' commitments. Included references to the GDPR. Alterations as per recommendations of LSE ISO27001 certification auditors.
21/02/17	3.14	
22/05/17	3.15	
13/06/17	3.16	Updated Objectives to include 'support for any ISMS, and commitment to continuous improvement of any ISMS. Also added in a clause about suppliers abiding by our information security policy.
23/11/17	3.17	Included a further objective (6) to keep research data and supplier data in a state commensurate with its classification.
07/02/18	3.18	Inclusion of new foreword signed by Director Dame Minouche Shafik.
11/01/19	3.19	Adjusted to more specifically address GDPR requirements. New cloud supplier section incorporated. Submitted to ISAB for annual review. Updated to reflect new information classification standard
18/05/20	3.20	Removal of ISAB (replaced by IGMB). Some tidy-up and correction of out of date references. Updating of URLs.
01/06/20	3.21	Updated 1.1.1, 1.1.2, 2.2, 2.7. Added in COO as Caldicott Guardian.
03/05/22	3.22	Updated references and links. Modernised a number of sections including responsibilities. Reduced the total number of words by removing superfluties and repetition. Removal of whistle blowing policy – not strictly a cyber security issue
13/06/23	3.23	Mended broken links, updated job titles, reviewed content. New foreword from Eric Neumeyer.
09/01/24	3.25	Standard review (v 3.24 was experimental and not used). Procurement Team's role in checking contracts for compliance made explicit in 'Responsibilities' section. Data protection references changed to UK GDPR (to disambiguate from the EU's GDPR as the two start to diverge).

Contacts

Position	Name	Email	Notes
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 – on website.
Will training needs arise from this policy	Yes
The Cyber Security Awareness training must be completed by all staff.	

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.

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]

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 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 the new *Prevent* duty, and seek to ensure that its IT facilities are not used to draw people into terrorism.

General Data Protection Regulation and DPA 2018

The GDPR has applied to the UK from 25 May 2018, and has been passed explicitly into UK law. The UK 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 UK 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]