Policy

Information Security Policy

LONDON CAMPUS OF HIGHER STUDIES

Document Title	Information Security Policy
Document Owner	IT Department
Approved By	Information Steering Committee
Date Approved	02 October 2023
Date of Review	02 October 2024
Document Version	1.1

Contents

1. Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of LCHS. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for LCHS to recover.

This information security policy outlines LCHS's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the Institute's information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.

LCHS is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which the LCHS is responsible.

LCHS 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 in accordance with the requirements of data security standard ISO 27001.

1.1 Objectives

The objectives of this policy are to:

1. Provide a framework for establishing suitable levels of information security for all LCHS information systems (including but not limited to all computers, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

a. This explicitly includes any ISO27001-certified Information Security Management Systems the Institute may run.

b. The resources required to manage such systems will be made available.

c. Continuous improvement of any ISMS will be undertaken in accordance with *Plan Do Check Act* principles

2. Make certain that users are aware of and comply with all current and relevant England legislation.

3. Provide a safe and secure information systems working environment for staff, students and any other authorised users.

4. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle, including satisfying the information security requirements of third party data providers.

5. Protect LCHS from liability or damage through the misuse of its IT facilities.

6. Respond to feedback and update as appropriate, initiating a cycle of continuous improvement.

1.2 Scope

This policy is applicable to, and will be communicated to, all staff, students, other members of the Institute and third parties who interact with information held by the LCHS and the information systems used to store and process it.
This includes, but is not limited to, any systems or data attached to the LCHS data or telephone networks, systems managed by LCHS, mobile devices used to connect to LCHS networks or hold LCHS data, data over which LCHS holds the intellectual property rights, data over which LCHS is the data controller or data processor, communications sent to or from the LCHS.

1.3 Definitions

LCHS Data, for the purposes of this policy, is data owned, processed or held by LCHS, whether primary or secondary, irrespective of storage location. It is used interchangeably with the term 'information'.

2 Policy

2.1 Information security principles

The following information security principles provide overarching governance for the security and management of information at LCHS.
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 and LCHS policy (see *Section 2.2. Legal and Regulatory Obligations*).

2. Staff with particular responsibilities for information (see *Section 3. Responsibilities*) must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.

3. All users covered by the scope of this policy (see *Section 1.2. Scope*) must handle information appropriately and in accordance with its classification level.

4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. a. On this basis, access to information will be on the basis of *least privilege* and *need to know*.

5. Information will be protected against unauthorized access and processing in accordance with its classification level.

6. Breaches of this policy must be reported.

7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits and penetration testing.

8. Any explicit Information Security Management Systems (ISMSs) run within the Institute will be appraised and adjusted through the principles of continuous improvement, as laid out in ISO27001 clause 10.

2.2 Legal & Regulatory Obligations

The London Campus of Higher Studies has a responsibility to abide by and adhere to all current England legislation as well as a variety of regulatory and contractual requirements.
Related policies will detail other applicable legislative requirements or provide further detail on the obligations arising from the legislation summarized below.

2.3 Information Classification

The following table provides a summary of the information classification levels that have been adopted by LCHS and which underpin the 8 principles of information security defined in this policy.
These classification levels explicitly incorporate the Data Protection Act's (DPA) definitions of *Personal Data* and *Sensitive Personal Data*, as laid out in LCHS's *Data Protection Policy*, and are designed to cover both primary and secondary research data.

Detailed information on defining information classification levels and providing appropriate levels of security and access is provided in the *Data Classification Standard*. Information on appropriate encryption techniques for securing Confidential data can be found here.
Information may change classification levels over its lifetime, or due to its volume – for instance:

Security Level	Definition	Examples
1. Confidential	Normally accessible only to specified members of LCHS staff. Should be held in an encrypted state outside LCHS systems; may have encryption at rest requirements from providers.	Exam Candidates records.
2. Restricted	Normally accessible only to specified members of LCHS staff or the student body	HR records
3. Internal Use	Normally accessible only to members of LCHS staff and the student body	Internal correspondence, final working group papers and minutes, committee papers, information held under license
4. Public	Accessible to all members of the public	Minutes of statutory and other formal committees, Information available on the LCHS website or through the LCHS's Publications Scheme.

2.7 Supporting Policies, Codes of Practice, Procedures and Guidelines

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 for viewing on LCHS's website.
All staff, students and any third parties authorized to access LCHS's network or computing facilities are required to familiarize themselves with these supporting documents and to adhere to them in the working environment.

2.8 Review and Development

This policy, and its subsidiaries, shall be reviewed by the Information Security Steering Committee (ISSC) and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organizational policies or contractual obligations.
Additional regulations may be created to cover specific areas.

ISSC comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems

3 Responsibilities

3.1 Members of LCHS:

All members of LCHS, LCHS associates, agency staff working for LCHS, third parties and collaborators on LCHS projects will be users of LCHS information. This carries with it the responsibility to abide by this policy and its principles and relevant legislation, supporting policies, procedures and guidance. 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.

A. Data Owners / Guardians:

Many members of LCHS will have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of information. These include:

B. 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 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.

C. Heads of Departments, Divisions, Centers:

Responsible for the information systems (e.g. HR/ Registry/ Finance) both manual and electronic that support LCHS's work. Responsibilities as above (for *Principal Investigators / Project administrators*).

D. Departmental managers / Line managers:

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

E. Head of Research Division

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

F. Institute Secretary

Responsible for LCHS compliance with the ISO27001.

G. Records Manager

Responsible for LCHS's Data Protection Policy, data protection and records retention issues.

H. IMT, Library IT and STICERD IT Staff:

Responsible for ensuring that the provision of LCHS's IT infrastructure is consistent with the demands of this policy and current good practice.

I. Head of Security:

Responsible for physical aspects of security and will provide specialist advice throughout the LCHS on physical security issues.

J. Information Security Manager:

Responsible for this and subsequent information security policies and will provide specialist advice throughout the Institute on information security issues.

K. Information Security Steering Committee:

Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks. Responsible for approving information security policies.

L. Outsourcing and Third Party Access:

External suppliers who are contracted to supply goods or services to the Institute should, where appropriate, be informed of the Institute's Information Security Policy and Data Protection Policy, and may be required to agree to adhere to the policy, and to protect its information assets.
Any third party used for external disposal of the Institute's obsolete information-bearing equipment or hardcopy material must be able to demonstrate compliance with the Institute's information security policy.

M. Operations:

Areas and offices where sensitive information is processed shall be given an appropriate level of physical security and access control to prevent unauthorized access, damage and interference.
Software malfunctions and faults should be reported, logged and monitored via established procedures to ensure timely corrective action is taken.
To ensure the correct and secure operation of information processing facilities, changes to operational procedures are controlled and, where appropriate, have management approval.
Development and testing facilities for business critical corporate information systems are separated from 'live' operational instances, and the migration of software from development to operational status is subject to agreed change control procedures.
User acceptance criteria for corporate information systems upgrades and new versions are required, and suitable tests of the systems carried out, prior to migration to 'live' operational status.

N. Information Handling:

The Institute has established a simple and pragmatic classification dividing information into two types: sensitive and non-sensitive.
The removal or transfer of all sensitive information should be authorised by the appropriate line manager. In addition, sensitive information held on laptops, tablets, USB devices or other storage media must be encrypted using Institute prescribed software in accordance with the Information Handling Guidance.
The Institute encourages a clear desk and screen policy, and screens on which sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorized persons.
Sensitive information should not rely upon the availability of systems or integrity of data files, and should normally be self-contained. Hard copies of sensitive information must be protected and handled according to the distribution and authorization levels specified for those documents.
Backup of the Institute's information assets and the ability to recover them is an important priority. Information owners, custodians and system administrators must ensure that appropriate backup and system recovery procedures are in place to meet the needs of the business, typically in liaison with IT Services staff.
The archiving of information and documents must take place with due consideration for legal, regulatory and business issues, with liaison between IT Services staff and information owners, custodians and system administrators.
All users of corporate information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the

confidentiality, integrity and availability of such files.
Appropriate measures should be taken when permanently disposing of sensitive information, be it paper-based or electronic, including the disposal of IT equipment or storage media containing sensitive information.
Sensitive information may only be transferred across networks, transmitted by post or other similar means, or copied to other media, when the confidentiality and integrity of the data can reasonably be assured.
All users must be aware of the risks of breaching confidentiality associated with the printing, photocopying or other duplication of sensitive information. All information used for, or by the Institute, must be stored, accessed and disposed of appropriately.

O. User Management:

Established procedures for the registration and de-registration of users, and for managing access to corporate information systems, ensure that users' access rights match their authorisations.
Users shall have a unique identifier (user ID) for their personal and sole use for access to Institute information services. The user ID must not be used by anyone in LCHS and associated passwords shall not be shared with any other person for any reason as defined within the Institute's IT Acceptable Use Policy.
System password management criteria and access control standards are established to minimize information security risks and yet allow the Institute's business activities to be Carried out without undue hindrance.
User access to corporate information systems must be authorised by the relevant line-manager, Including the appropriate access rights or privileges granted. Users' access rights must be adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff leave the Institute.

P. Use of Computers:

The Institute's IT Acceptable Use Policy (AUP) defines in detail the appropriate use of Institute computers. The AUP is applicable to, and will be communicated to staff, students and other relevant parties.
IT equipment, mobile devices and storage media must be safeguarded appropriately - especially when left unattended.
Central Institute systems and file stores should be used for the storage of digital information, where it will be protected by a regular automated backup service. The local storage of information on the hard drive of PCs and laptops, or on USB devices, is discouraged and should be reduced as far as possible.
All sensitive information stored on a laptop or USB device must be encrypted. It is the responsibility of the user to ensure that this takes place, and that the information is backed up appropriately.
Utmost care must be used when transporting data on removable devices or media. Sensitive information must be encrypted, and should only be accessed from equipment in secure locations.
Email should only be used to communicate sensitive information where appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed, and that the recipients are authorised to receive it.
Users are not permitted to load unapproved software on to the Institute's PCs, workstations, laptops or other IT devices.

Hamzah Tariq Khan *Hamza Khan*	Muhammad Saqib Sohail *Saqib Sohail*
Director Admin / Operation	**Director Academic Affairs**
02 October 2024	02 October 2024