Information Classification Standard

Introduction

The confidentiality, integrity and availability of LSE's information assets must be appropriately protected against unauthorized access, disclosure or modification.

This standard has been developed to meet the requirements laid out in both the Data Protection Policy (section 2.2) and the Cyber Security Policy (statements 1 and 2)

Data Protection Policy:

- Implementing technical and organisational security measures to keep personal data as secure as possible.
- Ensuring that Special Categories personal data is only processed where absolutely necessary and with the appropriate security measures.

Cyber Security Policy:

- Access to information will be on the basis of least privilege and need to know.
- Information must be classified according to LSE's Information Security Classification Standard, with due regard to relevant legislative, regulatory and contractual requirements. These requirements extend to primary and secondary research data gathered or used under contract.

Different types of information assets require different security measures depending upon their sensitivity and the scale of data they contain. LSE's information classification standards enable everyone to correctly classify and securely use information assets for which they have responsibility.

This standard includes classification criteria and categories. It requires data owners and stewards to classify the information they are responsible for and implement appropriate technical controls to maintain its confidentiality, integrity and availability.

It assists with ensuring that the confidentiality and integrity of intellectual property is appropriately preserved.

It is for use by anyone who is responsible for setting the access boundaries around both unstructured and structured data – who can use it (both access it and change it), where it can be stored and how it must be treated.

Standard

Data controlled by LSE is classified into three categories::

- Confidential
- Restricted
- Public

See the Definitions section for examples of each category.

LSE has no information assets that would require adoption of the Government Security Classifications Policy.

The expected controls required for each level of data are given below.

Use of Confidential Data

Only those who explicitly need access must be granted it, and only to the least degree in order to do their work (the 'need to know' and 'least privilege' principles).

When held outside LSE, on mobile devices such as laptops, tablets or phones, in Cloud storage or in transit, 'Confidential' information must be protected behind an explicit logon challenge that meets LSE's password requirements and by *at least* AES 128-bit encryption at the device, drive or file level, or by other controls that provide equivalent protection for data at rest.

Confidential data held outside the UK or EEA (e.g. in cloud environments) must be held according to UK GDPR requirements and will require an explicit contract. These standards can be enforced via Standard Data Protection Clauses or an explicit Data Processing Agreement (DPA).

Any cloud service holding Confidential data must meet ISO27001 or demonstrate equivalent controls.

Use of Restricted Data

'Restricted' information is open to groups of people within the School.

'Restricted' information must be held in such a manner that prevents unauthorised access i.e. on a system that requires a valid and appropriate user to log in before access is granted. When held locally – i.e. on a laptop or mobile device – it must be encrypted at rest to at least AES-128 standard.

If 'Restricted' information contains personal data and is held outside the UK or EEA (e.g. in cloud environments) it must be held according to UK GDPR requirements and will require an explicit contract. These standards can be enforced via Standard Data Protection Clauses or an explicit Data Processing Agreement (DPA).

Any cloud service holding Restricted data must meet ISO27001 or have equivalent controls.

Use of Public Data

'Public' information can be disclosed or disseminated without any restrictions on content, audience or time of publication.

Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules.

Scope

This standard applies to all information where LSE is the data controller (for personal data) or copyright holder (for non-personal data), irrespective of the location or the type of service or device it resides on.

Any legal or contractual stipulations over information classification (e.g. where LSE is not the data controller) take precedence over this standard.

Definitions

Confidential

'Confidential' information has significant value for LSE, and unauthorized disclosure or dissemination could result in severe financial or reputational damage to LSE, including fines of up to 4% global turnover from the Information Commissioner's Office, the revocation of research contracts and the failure to win future research bids.

Data defined by the UK GDPR as *Special Categories* of Personal Data falls into this category.

Examples include:

- religion, health, criminal convictions, trade union membership, ethnicity for identified or identifiable individuals contained in primary or secondary research data;
- salary information;
- individuals' bank details;
- draft research reports of controversial and / or financially significant subjects;
- passwords;
- large aggregates of GDPR-defined Personal Data (>1000 records) including elements such as name, address, telephone number;
- HR and Student Record System data,
- Interview transcripts,

Restricted

Information defined as *Personal Data* by the UK GDPR falls into this category, such as names, email addresses, phone numbers, photos.

Information you may want to share with the School community, but not the general public at large, would fall into this category, such as the location of refuge points within the School. If information does not fit into the 'Confidential' or 'Public' categories, then it is 'Restricted' information.

Examples include:

- GDPR-defined Personal Data (information that identifies living individuals) including where used as part of primary or secondary research:

- Name, email, work location, work telephone number, photographs (where not deliberately published on any LSE-related website e.g. lse.ac.uk)
- reserved committee business;
- draft reports, papers and minutes;
- internal correspondence;
- final working group papers and minutes;
- information held under license;

Public

Data where there are no restrictions on dissemination. Examples include:

- Annual accounts,
- minutes of statutory or formal committees,
- pay scales,
- Experts' Directory,
- Information available on the LSE website or through the LSE's Publications Scheme programme,
- Course information,
- Information intentionally published on LSE websites including lse.ac.uk

Responsibilities

All users – classify data and treat it according to its classification

System owners – ensure systems can secure data according to its classification

System commissioners – ensure systems, including cloud services, can secure data according to its classification before purchase

Data Protection Officer – reporting appropriate data breaches to the Information Commissioner's Office

Supporting/Relevant documents

The standard has been developed to meet the requirements laid out in both the Data Protection Policy (section 2.2) and the Cyber Security Policy (statements 1 and 2)

Data Protection Policy:

- Implementing technical and organisational security measures to keep personal data as secure as possible.
- Ensuring that Special Categories personal data is only processed where absolutely necessary and with the appropriate security measures.

Cyber Security Policy:

- Access to information will be on the basis of least privilege and need to know.
- Information must be classified according to LSE's Information Security Classification Standard, with due regard to relevant legislative, regulatory and contractual requirements. These requirements extend to primary and secondary research data gathered or used under contract.

Assurance / Compliance

Information Assets must meet the UK's General Data Protection Regulation and Data Protection Act (2018).

Assurance will be provided by regular penetration tests, red team exercises and internal audit activities.

Document Control

Standard owner:	Director of Cyber Security
Standard author:	Jethro Perkins
Responsible office:	DTS
Approving body:	Policy Committee
Effective date:	[11 August 2026
Date of next review:	16 July 2029
Review schedule:	3 years

Version history

Whole numbers should represent significant revisions of the policy, decimals should be used to indicate minor amendments. E.g. version 2 would represent a wholescale review and update, whereas 2.1 would represent minor technical updates that do not change the nature or implementation of the policy.

Version	Date	Approved by	Details of amendments
5	13 July 2026	Policy Committee, subject to minor amendments	Rewrite into new template
5.1	16 July 2026		Incorporating amendments required to v5, and also corrections suggested by the DPO