THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Technical

Information Classification Standard

1. Introduction

1.1 Purpose

In order to preserve the appropriate confidentiality, integrity and availability of LSE's information assets, the School must make sure they are protected against unauthorized access, disclosure or modification. This is not just critical for assets covered by the General Data Protection Regulation, and the primary and secondary data used for research purposes, but also for all business conducted across the school.

Different types of information require different security measures depending upon their sensitivity. LSE's information classification standards are designed to provide information owners with guidance on how to classify information assets properly and then use them accordingly.

This guidance — developed in accordance with the LSE's Information Security and Data Protection Policies — includes classification criteria and categories.

1.2 Scope

This standard applies to all LSE information, irrespective of the location or the type of service or device it resides on. It should consequently be used by all staff, students, other members of the School and third parties who interact with information held by and on behalf of the LSE.

Any legal or contractual stipulations over information classification take precedence over this standard.

1.3 Assumptions

The definitions of personal data and protected characteristics laid out in the General Data Protection Regulation continue to be relevant and require the currently understood levels of protection.

The mechanisms offered as recommendations in this proposal continue to exist and are available to those that need them.

The reader has sufficient technical knowledge to implement the controls as laid out.

2. Information Classification

2.1 Information Classification Definitions

The following table provides a summary of the information classification levels that have been adopted by LSE and which underpin the principles of information security defined in the Information Security Policy (Section 2.1). These classification levels explicitly incorporate the General Data Protection Regulation's (GDPR) definitions of *Personal Data* and *Special Categories*, as laid out in LSE's Data Protection Policy, and are designed to cover both primary and secondary research data. Examples are provided in Section 2.2 below.

1. 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 GDPR as *Special Categories* of Personal Data falls into this category.

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, or in transit, 'Confidential' information must be protected behind an explicit logon and by AES 256-bit encryption at the device, drive or file level, or by other controls that provide equivalent protection..

2. Restricted

'Restricted' information is open to groups of people within the School. It is subject to controls on access, such as only allowing valid logons from groups of staff or students, but it does not have the stricter controls required by 'Confidential' information.

'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.

Information defined as *Personal Data* by the 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.

Public disclosure or dissemination of this information is not intended, and may incur fines from the ICO and negative publicity for LSE.

3. Public

'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. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system.

2.2 Examples

Security Level	Definition	Examples	FOIA2000 status
Confidential	Normally accessible only to specified and / or relevant members of LSE staff	1. GDPR-defined Special Categories of personal data: • racial/ethnic origin, • political opinion, • religious beliefs, • trade union membership, • physical/mental health condition, • sexual life, • criminal record including when used as part of primary or secondary research data; 2. salary information; 3. individuals' bank details; 4. draft research reports of controversial and / or financially significant subjects; 5. passwords; 6. large aggregates of GDPR-defined Personal Data (>1000 records) including elements such as name, address, telephone number. 7. HR system data, SITS data, LSE Central data 8. Interview transcripts, research databases or other research records involving individually identifiable Special Categories of personal data.	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
Restricted	Normally accessible only to specified and / or relevant members of LSE staff or the student body	1. GDPR-defined Personal Data (information that identifies living individuals) including where used as part of primary or secondary research, contained in research databases, transcripts or other records: 2. Name, email, work location, work telephone number, photographs Other information: 3. reserved committee business; 4. draft reports, papers and minutes; 5. systems; 6. internal correspondence; 7. final working group papers and minutes; 8. information held under license; 9. company policy and procedures (as appropriate to the subject matter)	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
Public	Accessible to all members of the public	1. Annual accounts, 2. minutes of statutory or formal committees, 3. pay scales 4. Experts' Directory	Freely available on the website or through the LSE's Publication Scheme.

		5. information available on the LSE website or through the LSE's Publications Scheme programme 6. course information. 7. company policy and procedures (as appropriate to the subject matter)	

2.3 Data Breaches

Any data breach must be immediately reported to LSE's Data Protection Officer (glpd.info.rights@lse.ac.uk) or Information Security Team (imt.infosec@lse.ac.uk).

2.4 Data controllers, processors and information asset owners

For LSE-owned data, the School is defined as the Data Controller, whereas individuals are Information Asset Owners, and must record the personal information under their responsibility in the Information Asset Register

If information is transferred outside the School – for example, to be processed in a software as a service application, or to be translated or transcribed by a third party – a data processing agreement must be established with this third party. Please contact LSE's Legal Team for further information.

2.5 Granularity of classification

The sets of information being classified should, in general, be large rather than small. Smaller units require more administrative effort, involve more decisions and add to complexity, thus decreasing the overall security.

2.6 Information Retention

There may be minimum or maximum timescales for which information has to be kept. These may be mandated in a research or commercial contract. Other forms of information retention may be covered by environmental or financial regulations: see LSE's Retention Schedules for guidance.

3. Responsibilities

Members of LSE
All members of the LSE community, LSE associates, agency staff working for LSE, third parties and collaborators on LSE projects are users of LSE information. They are responsible for assessing and classifying the information they work with, and applying the appropriate controls.

LSE community members must respect the security classification of any information as defined, and must report any data breaches to the Information Security Manager or Data Protection Officer as quickly as possible.

Information Asset Owners
Information Asset Owners within the School are responsible for assessing information, classifying its sensitivity and stipulating how it can be used. They should then specify the appropriate controls to protect that information. They must record the information classification in the Information Asset Register.

Data Processors

Data Processors are responsible for ensuring the right controls are maintained, in order to ensure data can be stored and used appropriately. There must be a contract between LSE as the data controller and any data processors.

Records Manager / Data Protection Officer:
Responsible for reporting any breaches to the Information Commissioner's Office.

Information Governance Committee
Responsible for approving information security and governance policies.

Document control

Distribution list

External document references

Title	Version	Date	Author
Data Protection Policy Information Security Policy General Data Protection Regulation	3.0 3.18	02/02/18 07/02/18 2016	Rachael Maguire Jethro Perkins

Version history

Date	Version	Comments
07/01/13	2.0	Update from previously released version
08/01/13	2.1	Incorporating updates
12/02/13	2.2	Included reference to the information retention schedule
13/02/13	2.3	Section 3.2 updated
15/02/13	2.4	Inclusion of research data made more specific
12/03/13	3.0	Updated section 3.3 to include rights of access and to suggest that areas may want to appoint explicit data owners. Released version
23/02/18	3.1	Updated to incorporate the GDPR and its terminology
23/11/18	4.2	Removal of Internal Use, leaving 3 classification levels. Updated in light of ISAB comments to provide more concrete examples. Policies may be publically available as well as restricted.
03/12/18	4.3	

Contacts

Position	Name	Email	Notes
Assistant Director of Cyber Security and Risk	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**
If Yes, please give details Change in the levels at which information can be classified. LSE's information security awareness training course, plus other materials (such as the Cloud Assurance Questionnaire) will be updated to reflect the new classification levels.	