Standard

Information Security - Information Classification

Jethro Perkins
Information Security Manager

Document control

Distribution list

Name	Title	Department
Nick Deyes	Director of Information Management Technology	IT Services
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Data Protection Policy Information Security Policy Data Protection Act	Draft 3.0	04/12/12 12/03/13 1998	Dan Bennett Jethro Perkins

Version history

Date	Version	Comments
07/01/13	2.0	Update from previously released version
08/01/13	2.1	Incorporating updates as a result of comments from Dan Bennett
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

Review control

Reviewer	Section	Comments	Actions agreed
ISAB	3.2.	Explicit examples of research data need to be included	Research Data examples will be incorporated

ISAB	3.2	Replace “specified members of staff” with “specified and / or relevant members of staff”	Phrase replaced.
ISAB	3.2	Provide under Confidential and Restricted examples explicitly pertaining to research.	Examples of possible research data usage included
ITC	3.3	The mandating of actions of responsibility on data owners is impossible to enforce, so can it be changed to guidelines concerning rights of access, which is more appropriate.	Section updated.

Table of contents

Introduction

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 Data Protection Act, 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, as well as rules for the delegation of classification tasks.

Scope

This standard applies to all LSE information, irrespective of the data location or the type of 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.

Assumptions

The legal definitions laid out in the Data Protection Act 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.

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 the inappropriate situation of information to the Information Security Manager or Head of Security as quickly as possible.

Information Owners
Information Owners are responsible for assessing information and classifying its sensitivity. They should then apply the appropriate controls to protect that information. Information ownership can be delegated: see *Section 3.3*.

IT Services, Library IT and STICERD IT Staff:
Responsible for providing the mechanisms or instructions for protecting electronic information while it is resident on any LSE-owned or controlled system.

Records Management Staff:
Responsible for providing the instructions for the protection and preservation of records, whether physical or electronic.

Information Security Advisory Board
Responsible for the advising on and recommending information security standards on data classification.

Information Classification

Information Classification Definitions

The following table provides a summary of the information classification levels that have been adopted by LSE and which underpin the 8 principles of information security defined in the Information Security Policy (Section 3.1). These classification levels explicitly incorporate the Data Protection Act's (DPA) definitions of *Personal Data* and *Sensitive Personal Data*, as laid out in LSE's Data Protection Policy, and are designed to cover both primary and secondary research data.

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 £500,000 from the Information Commissioner's Office, the revocation of research contracts and the failure to win future research bids. Data that is defined by the Data Protection Act as *Sensitive Personal Data* falls into this category. Only those who need 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.

2. **Restricted**
   'Restricted' information is subject to controls on access, such as only allowing valid logons from a small group of staff. '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 Data Protection Act falls into this category. Disclosure or dissemination of this information is not intended, and may incur some negative publicity, but is unlikely to cause severe financial or reputational damage to LSE. Note that under the Data Protection Act large datasets (>1000 records) of 'Restricted' information may become classified as Confidential, thereby requiring a higher level of access control.

3. **Internal Use**
   'Internal use' information can be disclosed or disseminated by its owner to appropriate members of LSE, partners and other individuals, as appropriate by information owners without any restrictions on content or time of publication.

4. **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.

Designating information as 'Confidential' involves significant costs in terms of implementation, hardware and ongoing resources, and makes data less mobile. For this reason, information

owners making classification decisions must balance the *risk* of damage that could result from unauthorized access to, or disclosure of, the information against the cost of additional hardware, software or services required to protect it.

Examples

Security Level	Definition	Examples	FOIA2000 / DPA1998 status
1. Confidential	Normally accessible only to specified and / or relevant members of LSE staff	1. DPA-defined *Sensitive 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 DPA-defined *Personal Data* (>1000 records) including elements such as name, address, telephone number. 7. HR system data, 8. SITS data 9. LSE Central data 10. Interview transcripts, research databases or other research records involving individually	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.

		identifiable *sensitive personal data*.	
2. Restricted	Normally accessible only to specified and / or relevant members of LSE staff or the student body	1. DPA-defined *Personal Data* (information that identifies living individuals including: • home / work address, • age, • telephone number, • schools attended, • photographs including where used as part of primary or secondary research, contained in research databases, transcripts or other records 2. reserved committee business; 3. draft reports, papers and minutes; 4. systems.	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
3. Internal Use	Normally accessible only to members of the LSE staff or the student body	1. Internal correspondence, 2. final working group papers and minutes, 3. committee papers, 4. information held under license 5. company policy and procedures	Subject to scrutiny in relation to appropriate exemptions/ public interest and legal considerations
4. Public	Accessible to all members of the public	1. Annual accounts, 2. minutes of statutory and other formal committees, 3. pay scales 4. Experts' Directory 5. information available on the LSE website or through the LSE's Publications Scheme programme	Freely available on the website or through the LSE's Publication Scheme.

		6. course information.	

Explicit information ownership and other rights of access to information

IMT recommends that departments, functions and research projects explicitly designate information owners.

Other users may have rights of access to data according to the terms of engagement under which the data was gained or created.

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.

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 Schedule for guidance.