London School of Economics & Political Science

Governance, Legal and Planning Division

Data Protection Policy

Summary	This document outlines the controls from ISO27002 that relate to the LSE's Information Security Policy and Infrastructure that apply to the LSE, across all departments.
Version	Draft 2.3
Date	dd month yyyy2013
Library reference	IC-PY-001

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author

Version history

Date	Version	Comments
11 January 2014	Final	Received Approval from Council

Review control

Reviewer	Section	Comments	Actions agreed

Table of contents

1. PURPOSE

1.1 This document sets out The London School of Economics and Political Science ("the School")'s policy on data protection. It provides an overview of data protection requirements and directs you to more detailed guidance as appropriate.

1.2 If you have any questions relating to this policy please contact the School's Data Protection Officers via glpd.info.rights@lse.ac.uk.

2. BACKGROUND TO THIS POLICY

2.1 The Data Protection Act 1998 ("DPA") establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes with the right of individuals to retain the privacy of their personal details. The legislation is underpinned by a set of eight straightforward principles, which define how data can be legally processed.

2.2 These eight principles are:

2.2.1 Personal data shall be processed fairly and lawfully.

2.2.2 Personal data shall be held only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.

2.2.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.

2.2.4 Personal data shall be accurate and where necessary kept up to date.

2.2.5 Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

2.2.6 Personal data shall be processed in accordance with the rights of data subjects under the DPA.

2.2.7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of the data.

2.2.8 Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2.3 The Act defines both **personal data** and **sensitive personal data**[i]. Personal data is any information that can identify a living individual and can include such items as home and work address, personal email address, age, telephone number and schools attended, and even photographs and other images. Sensitive personal data consists of racial/ethnic origin, political opinion, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and information relating to legal proceedings and convictions.

2.3.1 Personal data comes under the categories of confidential or restricted information in the Information Classification Standard depending on the volume. Sensitive personal data comes under the category of confidential information only in the Information Classification Standard.

[i] See Part One of the Data Protection Act, http://www.legislation.gov.uk/ukpga/1998/29/part/I

2.4 The DPA sets out a number of obligations with which an organisation that holds or uses personal data must comply to safeguard that personal data. In particular, certain conditions specified in the DPA must be satisfied to justify the holding or use of personal data. These conditions are set out in a basic manner in the School's Data Protection register entry. Staff who are unsure what conditions apply to personal data they intend to process should seek advice from the Data Protection Officers.

3. POLICY AND GUIDANCE

3.1 The School is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

3.2 This Policy and the further School guidance it refers to apply to all personal data processed for the School's purposes, regardless of where it is held and, in respect of automatically processed data, the ownership of the equipment used.

3.3 Links to relevant School guidance are set out at the end of this policy. This list is not exhaustive and all relevant guidance can be found at ***http://www2.lse.ac.uk/intranet/LSEServices/legalAndCompliance/dataProtection/Home.aspx*.**

4. APPLICATION OF THIS POLICY

4.1 The School holds personal information about individuals such as employees, students, graduates, research subjects and others, defined as **data subjects** in the DPA. Such data must only be processed in accordance with the DPA. This Policy and the School Guidance are written to ensure such compliance. Any breach of this Policy and/or the School Guidance may result in the School as the **Data Controller** (and in some cases individuals), being in breach of the DPA and therefore liable in law for the consequences of such breach.

4.2 Heads of Department and Service Leaders are responsible for ensuring that the School complies with the DPA. All students and staff must ensure they have read and understand this Policy and the School Guidance.

4.3 It is the responsibility of all users of personal data throughout the School to ensure that personal data is kept securely. Personal data should not be disclosed to any unauthorised third party in any form, either accidentally or otherwise.

4.4 Any breach of or failure to comply with this Policy or the School Guidance, particularly any deliberate release of personal data to an unauthorised third party, may result in disciplinary or other appropriate action.

4.5 The School will continue to perform periodic audits to ensure compliance with this Policy and the DPA and to ensure that all guidance and support is kept up to date.

4.6 Any unauthorised access to or disclosure of personal data or other data security breaches should be reported to the Data Protection Officers and/or the Information Security Manager as soon as possible.

4.7 The School Secretary is responsible for ensuring that the School community remain informed of their obligations under the Data Protection Act, with operational duties of advice and support devolved to the Data Protection Officers.

5. HANDLING OF PERSONAL DATA BY STUDENTS

5.1 A student should only use personal data for an academic or School-related purpose, with the knowledge and express consent of an appropriate member of staff. The use of personal data by students should be limited to the minimum consistent with the achievement of academic objectives.

5.2 For a postgraduate research student, this appropriate member of staff would be the supervisor. Research students are more likely than other students to be collecting personal

data and creating datasets. They should seek advice from the Data Protection Officers at the earliest stage, and at all times comply with the policy.

5.3 For a postgraduate taught student, the appropriate member of staff would be the supervisor of their dissertation or the course leader of the relevant class/course. As with research students, any personal data collected as part of the dissertation should be kept in accordance with this policy.

5.4 For an undergraduate, responsibility would lie with the course leader of the relevant class/course. Wherever possible, data should be de-personalised so that students are not able to identify the subject.

5.5 Any confidentiality or consent agreements should normally be signed off by the School Secretary or the Head of Research Division. For advice, contact the Data Protection Officers

6. ACCESS TO DATA

6.1 The DPA gives data subjects a right to access to personal data held about them within a set timescale. Therefore it is important that the Data Protection Officers be notified of any request to the School for access to an individual's personal data as soon as they are received.

6.2 There are specific provisions which apply to examination marks.

6.3 If you have any questions relating to access to personal data please contact one of the Data Protection Officers.

7. RETENTION OF DATA

7.1 Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. This applies to both electronic and non-electronic personal data. The School's retention schedule outlines the length of time various classes of records and other data should be kept. This extends to backups and copies made on removable media.

8. DATA TRANSFER

8.1 If data is being sent outside the European Economic Area by the School, the School needs to put in place certain safeguards. Please contact the Data Protection Officer if for any reason related to the School, as part of a supplier contract or for your studies, for example, you may need to send personal data outside the EEA.

8.2 Information published on the web must be considered to be an export of data outside the EEA. No web-based, or 'Cloud' services, should be used for storing or sending sensitive personal data unless this has been agreed with one of the Data Protection Officers.

8.3 Any transfers of personal data outside the EEA and/or extraordinary transfers of data should be signed off by the School Secretary.

10. CCTV AND ACCESS CONTROL

10.1 CCTV at the School will be used in line with the School’s Code of Conduct on CCTV.

10.2 Access control systems are used at the School for the purposes of security, maintenance of IT and building systems and public safety.

10.3 Requests for information held within CCTV and access control systems made by police services under the relevant exemptions in the Data Protection Act will be handled by the School’s Security Office.

10.4 Requests for information held within CCTV and access control systems made by any other individuals or organisations will be handled by the School’s Information Governance Team.

11. COMPLIANCE, POLICY AWARENESS AND DISCIPLINARY PROCEDURES

11.1 The loss or breach of confidentiality of personal data is an infringement of the Data Protection Act 1998 and may result in criminal or civil action against LSE. Therefore all users of personal data at the School's information systems must adhere to the Data Protection Policy and its supporting policies as well as the Information Security Policy.

11.2 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.

11.3 Any breach of this policy 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.

12. STATUS OF THIS POLICY

This Policy has been approved by Council on 11 January 2014. It is available in the policies and procedures section of the website.

Annex A – Further information

External resources

Data Protection Act
http://www.legislation.gov.uk/ukpga/1998/29/contents

Information Commissioner's Office
http://www.ico.gov.uk/

Information Commissioner's Office Guidance on Cloud Computing
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

Register of Data Controllers
http://www.ico.gov.uk/ESDWebPages/search.asp

School Guidance

Records Management Policy:
http://www2.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/recManPol.pdf

Guidance on best practice for records management, including personal data:
http://www2.lse.ac.uk/intranet/LSEServices/legalAndCompliance/recordsManagement/recordsManagementGuidance.aspx

The School's retention schedule:
http://www2.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/retSch.pdf

Information Security Policy:
http://www2.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/infSecPol.pdf

Guidance on cloud based services:
http://www2.lse.ac.uk/intranet/LSEServices/itservices/guides/softwareAndTraining/using-cloud-based-services.aspx

Data Protection Officers

Rachael Maguire, Room TW1 6.01, 020 7849 4622 r.e.maguire@lse.ac.uk

Or email: glpd.info.rights@lse.ac.uk