London School of Economics and Political Science

Data Protection Policy

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 Officer via glpd.info.rights@lse.ac.uk.

2. BACKGROUND TO THIS POLICY

2.1 The General Data Protection Regulation (GDPR), to be incorporated into UK law via a new Data Protection Act (DPA), establishes a framework of rights and duties which are designed to safeguard personal data. These are referred to in this policy as 'Data Protection legislation'. The legislation is underpinned by a set of six straightforward principles, which define how data can be legally processed.

2.2 These six principles are:

2.2.1 Personal data shall be processed fairly, lawfully and transparently.

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. There is an exemption for research data.

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. There is an exemption for research data.

2.2.6 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.

2.3 The GDPR also sets out rights of data subjects relating to their personal data. These rights include:

2.3.1 the right to access

2.3.2 the right to rectification

2.3.3 the right to erasure (in certain circumstances)

2.3.4 the right to stop processing

2.3.5 the right to portability (in certain circumstances)

2.3.6 the right to object to marketing. and

2.3.7 the right to have human intervention with regards to automated processing, including profiling

2.4 The GDPR sets out the conditions under which information can be transferred to countries outside the European Economic Area. These include adequacy, appropriate safeguards, binding corporate contracts and explicit consent, amongst others.

2.5 The Act defines both **personal data** and **special categories personal data**.

2.5.1 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.

2.5.2 Special categories 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.

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

2.6 The GDPR sets out certain lawful bases that must be satisfied to justify the holding or use of personal data. These are set out in Article 6 of the GDPR and include: contract; legal; vital interests, public duty, legitimate interests and consent. Special categories data requires that (an) additional lawful basis as set out in Article 9 of the GDPR. These lawful basis are recorded in the School's Information Asset Register. Staff who are unsure what lawful bases apply to personal data they intend to process should seek advice from the Data Protection Officer.

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 Data Protection legislation. Such data must only be processed in accordance with the Data Protection legislation. 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 Data Protection legislation 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 Data Protection legislation. 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 Data Protection legislation 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 Officer and/or the Information Security Manager as soon as possible, using the Data Breach notification form on the website where possible.

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

4.8 The Data Protection Officer is required by Data Protection legislation to report to the highest levels of management at the School, which will normally be done through the School Secretary.

4.9 Staff procuring cloud based services or mobile apps storing personal data for the School must check with the Information Security team that these meet the security requirements of Data Protection legislation.

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 Officer 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 Officer.

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 Officer 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 and comments.

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

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.

7.2 This does not apply to research related data which can be kept indefinitely.

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.

8.3 No web-based, or 'Cloud' services, storing personal data outside the EEA should be used for storing or sending special categories personal data unless this has been agreed with the Data Protection Officer.

8.4 Any transfers of personal data outside the EEA and/or extraordinary transfers of data should be signed off by the School Secretary, unless to countries that are covered by an EU adequacy decision.

9. CCTV AND PHYSICAL ACCESS CONTROL

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

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

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

9.4 Requests for information held within CCTV and access control systems made by any other individuals or organisations will be handled by the Data Protection Officer.

10. INFORMATION ASSET REGISTER

10.1 The School's Information Asset Register (IAR) will be used to meet the record keeping requirements of Data Protection legislation.

10.2 Information Asset Owners, defined as the staff member with responsibility for the information asset, will ensure that they create and maintain the data held within the Information Asset Register.

10.2.1 This will include an annual review of their information assets.

10.3 The Data Protection Officer will ensure that Information Asset Owners receive the appropriate support to maintain the information asset register.

11. COMPLIANCE, POLICY AWARENESS AND DISCIPLINARY PROCEDURES

11.1 The loss or breach of confidentiality of personal data is an infringement of Data Protection legislation 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

12.1 This Policy has been approved by the Information Governance Committee on 26 March 2018. It is available in the policies and procedures section of the website.

Review schedule

Review interval	Next review due by	Next review start
3 Years	March 2021	November 2020

Version history

Version	Date	Approved by	Notes
V1	11.01.2014	Council	
V2	26.03.2018	Information Governance Committee	

Links

External Reference	Link
General Data Protection Legislation	https://gdpr-info.eu/
Information Commissioner's Office	http://www.ico.gov.uk/
Information Commissioner's Office Guidance on Cloud Computing	https://ico.org.uk/for-the-public/online/cloud-computing/
Register of Data Controllers	https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/
School Guidance	**Link**
Records Management Policy	https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/recManPol.pdf
Guidance on best practice for records management, including personal data	https://info.lse.ac.uk/staff/divisions/Secretarys-Division/Information-Rights-and-Management/Information-and-Records-Management
The School's Retention Schedule	https://info.lse.ac.uk/staff/divisions/Secretarys-Division/Information-Rights-and-Management/Information-and-Records-Management
Information Security Policy	http://www2.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/infSecPol.pdf
Guidance on Cloud based services	http://www.lse.ac.uk/intranet/LSEServices/IMT/guides/softwareGuides/other/usingDropboxCloudStorageServices.aspx

Contacts

Position	Name	Email	Notes
Data Protection Officer	Rachael Maguire	R.E.Maguire@lse.ac.uk	Author