LSHTM Data Protection Policy

Document Type	Policy
Document owner	Daniel Scannell - DPO
Approved by	Management Board
Approval date	11 May 2018
Review date	April 2019
Version	1.1 (25 May 2018)
Amendments	Amending for typographical errors, clarity and consistency with other policies
Related Policies & Procedures	a. LSHTM Records Management policy b. LSHTM Information Management & Security policy c. LSHTM Freedom of Information policy

SCOPE

1. The policy applies to anybody whose personal data LSHTM processes, including staff, students, trustees and visitors. It covers all personal data that we process. For these purposes, personal data means any information in any recorded form which, on its own or combined with other data we hold, could be used to identify a living individual. The GDPR expands the definition of personal data so that as well as text, images and location data, it now expressly includes online identifiers. The definition of sensitive personal data (now called “special category data”) now expressly includes genetic and biometric information.

PURPOSE AND OVERVIEW

2. This policy explains the approach of the London School of Hygiene & Tropical Medicine (LSHTM) as a data controller and data processor.

Introduction

3. The London School of Hygiene & Tropical Medicine (LSHTM) has a mission to improve health and health equity in the UK and worldwide. LSHTM does this by working to achieve excellence in public and global health research, education and translation of knowledge into policy and practice. To achieve its mission, the staff, students and other stakeholders of LSHTM use data in many ways. Some of these data are considered personal data belonging to living individuals known as data subjects, including prospective, current and future students, staff, supporters and members of the public. We use a wide variety of personal data from information collected and filed in databases through to photographs and CCTV records.

4. Some of the personal data we process include special categories of data (sometimes called sensitive personal data), such as a data subject's gender, race or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or sexual life.

5. It is every member of LSHTM's responsibility to understand the basic principles of data privacy, and how they must act to enable LSHTM to process people's personal data lawfully.

6. The current Data Protection Act 1998 (DPA) will be replaced on 25 May 2018 with the General Data Protection Regulation (GDPR), which will be enshrined in UK law by a new act of parliament.

7. The School is a data controller as defined in the DPA and the GDPR because it chooses how it collects and processes personal data of staff, students and others.

8. The GDPR applies to data which alone or together with other data can identify living individuals, known as data subjects.

9. LSHTM must only process personal data fairly, lawfully and securely – please see the data protection principles below for further information.

10. LSHTM is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data. Good practice in the field of data privacy is continually evolving, and this policy and its associated documents will be updated to reflect such change.

11. This policy explains in plain language LSHTM's expectations of itself, its staff and students, when LSHTM processes your data, or asks contractors to do so on its behalf.

Principles of data privacy relevant to this policy

12. The GDPR sets out the following six principles of data protection that require personal data to be collected and used fairly, stored safely and not disclosed to any other person unlawfully:

a. Where we process personal data, we must do so lawfully, fairly and transparently (**"lawfulness, fairness and transparency"**);
b. We must only process personal data for clearly pre-specified lawful purposes, and we cannot process personal data for any other reasons (**"purpose limitation"**)[1];
c. We must only collect enough personal data for the stated purpose – the data must be adequate, relevant and only the amount necessary for the purpose for which it is processed (**"data minimisation"**).
d. The personal data we collect must be accurate and where necessary kept up to date (**"accuracy"**).
e. We must not keep personal data for longer than is necessary for its stated purpose (**"storage limitation"**).
f. We must only process personal data in a manner that ensures appropriate security, which includes protecting it against unauthorised or unlawful processing and against accidental

[1] GDPR permits further processing in certain circumstances for archiving, research or statistical purposes.

loss, destruction or damage, using appropriate technical or organisational measures (**"integrity and confidentiality"**).

13. Processing has a very wide definition in law. It includes obtaining or collecting, recording, holding, storing, organising, adapting, reformatting, cleaning, copying, transferring, combining, pseudonymising, anonymising, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

14. LSHTM, where it is a data controller, remains responsible for the control of any personal data it has collected, even if later passed onto another organisation or stored on systems or devices owned by other organisations or individuals (including devices personally owned by members of staff).

15. The new law means that many more data protection breaches must now be reported to the Information Commissioner's Office. Where a report is needed, we must do so no later than 72 hours after the breach is discovered.

POLICY

LSHTM duties as Data Controller and Data Processor

16. LSHTM is legally responsible for demonstrating compliance with the six data protection principles described at paragraph 11 above. LSHTM arranges mandatory training for staff and students to enable them to comply with the law too. If any member of LSHTM is found to have breached this policy deliberately, LSHTM may take disciplinary action against them, including immediate suspension of access to LSHTM facilities. In very serious cases, such people may face criminal investigation.

17. LSHTM keeps a record of its processing activities. For more information please see www.lshtm.ac.uk/dpo.

Information Management and Security

18. All members of LSHTM who use personal data must ensure that they hold such data securely, and that it is not disclosed to any unauthorised third party in any way, including by accident. In particular:
    a. any mobile devices used for LSHTM work must be encrypted and password protected, whether supplied by LSHTM or personally by the staff member or student;
    b. USB sticks and removable storage used to store personal data must never be used unless they and/or the files on them are encrypted and password protected;
    c. if cloud-based or remote storage is needed, this must be held in an appropriately secure system, such as the School's One Drive for normal personal data, or the secure server for special category data or where required by the NHS IG Toolkit, or a research ethics committee. Please see the LSHTM Data Classification and Handling Policy for more information.

19. The LSHTM Information Management and Security Policy applies to all members of staff and students and all other computer, network or information users authorised by the School or any of its departments thereof, including visitors.

Deletion of personal data

20. The LSHTM Records Retention & Disposal Schedule provides guidance on the retention and disposal of records created and managed by LSHTM, based on legal and regulatory requirements.

21. To comply with the data minimisation principle, LSHTM will only retain personal data for as long as is necessary to meet the purpose for which it was collected, including a short additional time during which we will confirm that the data should be deleted. This will be assessed in accordance with the LSHTM Records Retention & Disposal Schedule. Personal data which are no longer needed must be deleted securely. Paper records must be disposed of in confidential waste bins (for secure destruction off-site) and electronic records must be securely deleted.

22. Data which have been anonymised can be retained indefinitely.

Lawful Conditions for Processing

23. GDPR has clarified that data controllers like LSHTM must take care to choose the most appropriate lawful basis for processing personal data. The potentially lawful reasons for processing data are:

    a. consent by the data subject;
    b. the processing is required due to a contract between the data controller and data subject;
    c. the data controller is obliged by law to process the data;
    d. processing is necessary to protect someone's vital interests (i.e. life or death situation)
    e. the data controller must process the data to perform a task carried out in the public interest;
    f. the data controller needs to process the data in pursuit of its the legitimate interests or the interests of a third party, and the processing does not interfere with the rights and freedoms of the data subject.

24. All processing of personal data carried out by LSHTM must meet one or more of the conditions above. In addition the processing of 'special categories' of personal data requires extra, more stringent, conditions to be met in accordance with Article 9 of the GDPR.

25. Under GDPR, higher education institutions are classified as public authorities and therefore the use of the 'legitimate interests' justification is not possible in terms of LSHTM's core activities (public tasks) such as providing education or doing public health research. LSHTM does rely on legitimate interests for other types of processing such as marketing, development activities and alumni relations.

26. GDPR requires public authorities not to rely upon consent where another basis for lawful processing exists, and particularly for the performance of its core activities. Part of the reasoning behind this is that consent does not reflect the imbalance in the relationship between a data controller and data subject. In these cases it is unlikely that consent could be deemed to be freely given. Therefore where possible LSHTM will identify alternative justifications for processing, and these are recorded in LSHTM's privacy notices for staff, students and alumni. Other privacy notices may be issued in due course.

27. Where LSHTM relies upon consent, it will work to ensure that this meets the definition of a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or other clear affirmative action, signifies agreement to the processing of personal data relating to him or her". LSHTM will not rely upon silence, pre- ticked boxes or inactivity where it relies upon consent as the lawful basis for processing.

28. LSHTM will clarify with those whose consent is relied upon that they can withdraw their consent at any time.

Privacy Notices

29. LSHTM has produced privacy notices for staff, students and alumni, available at www.lshtm.ac.uk/dpo. Processing for purposes not stated in these privacy notices will be performed on the basis of consent, or documented in a further privacy notice.

Record of Processing Activities

30. LSHTM has produced a record of processing activities, available to view at www.lshtm.ac.uk/dpo.

31. LSHTM's Data Protection Officer will work with staff and students seeking to process personal data for activities not listed in the record of processing activities. A Data Protection Impact Assessment may be needed for such activity.

Children

32. The new law has more stringent controls on the processing of personal information relating to children, and particularly the information that must be available to the child or their parent explaining why the data are being collected, and the use to be made of the data.

33. Please contact the Data Protection Officer for further details.

Research

34. Data collected for research purposes are covered by the GDPR. It is important that staff collecting data for the purpose of research or consultancy incorporate an appropriate form of consent on any data collection form. The Research Governance and Integrity Office can advise on this as part of your ethics application.

35. The new law is a little more permissive about the secondary processing of research data. Retention of research data for archive and statistical purposes remains permitted, and the new law expressly permits museums, galleries, archives and libraries to process personal data without consent where necessary for "archiving purposes in the public interest", subject to appropriate safeguards for the rights and freedoms of data subjects. It also exempts archive services from complying with certain of the rights of data subjects (e.g. access, rectification, erasure), where the exercise of those rights would seriously impair or prevent them from fulfilling their objectives.

36. In addition, data which have been appropriately anonymised can be retained indefinitely, as they cease to be personal data when it is no longer possible to use them to identify a living individual. Pseudonymisation, where a data set is anonymised unless combined with a

reidentification key, is highly advised for all studies.

Data Subject Rights

37. Data subjects have express rights to access and correct personal information held about them by LSHTM. Subject access allows individuals to confirm the accuracy of personal data and check the lawfulness of processing, and to exercise rights of correction or objection if necessary. As part of the right to access data, individuals can reasonably request to see information that LSHTM holds about them.

38. LSHTM will respond within one month to all requests by data subjects for access to their personal data, which will normally be provided free of charge.

39. LSHTM is not required to disclose examinations scripts. Students are entitled to their marks for both coursework and examinations. Unpublished marks must be disclosed within 5 months of a subject access request.

40. In addition to accessing their personal data held by LSHTM, data subjects have the following rights (some of which are not absolute rights):

    a. Right to Object – the right to object to specific types of processing;
    b. Right to be forgotten (erasure) – the right to have their data erased in certain situations e.g. the data are no longer required for the stated purpose. Some exemptions apply. Individuals can ask the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved.
    c. Right to challenge the basis for automated decision making and profiling – in practice this right is unlikely to apply because LSHTM does not automate decisions and profiling is restricted to what is lawfully necessary, e.g. to comply with immigration law.
    d. Right to Rectification – data subjects may ask LSHTM to rectify inaccuracies in personal data held about them.
    e. Right to Portability – in practice, this right will not apply as LSHTM does not collect data that would be provided to another higher education provider in an agreed standard form.

41. Please see www.lshtm.ac.uk/dpo for further information, and for the forms to be used to make a data subject rights request.

Data Sharing

42. LSHTM will only share personal data with a third party or external data processor where lawfully permitted to do so. In particular, LSHTM will ensure that such data sharing:
    a. is lawful and fair to the data subjects concerned;
    b. fulfils a legal requirement or a contractual commitment with the data subject;
    c. is necessary to meet LSHTM's legitimate interests;
    d. is necessary for a public task that is core to LSHTM's public functions; or
    e. is based on the data subject's informed consent.

43. LSHTM must also be satisfied that the third party will meet all the requirements of GDPR particularly in terms of holding the information securely. It will ensure that other legal requirements are in place, including a written contract with the party receiving the personal data.

44. Staff who receive requests for personal information from third parties such as relatives, police, local councils etc. should consult the guidance on www.lshtm.ac.uk/dpo or speak to the Data Protection Officer.

Transfers of Personal Data Outside the EEA

45. Personal data can only be transferred out of the European Union under certain circumstances. The GDPR lists the factors that should be considered to ensure an adequate level of protection for the data and some exemptions under which the data can be exported. In many cases LSHTM will require consent of data subjects before personal information can be transferred out of the EEA.

46. Information held in cloud storage where the servers are located outside the EEA, and/or which are published on the internet must be considered to be an export of data outside the EEA. LSHTM's main cloud storage on One Drive is safe for storing normal personal data for the purposes of GDPR. The School's secure servers should be used for special category data, or where required by the NHS IG Toolkit or a research ethics committee.

Data Protection Impact Assessments and Data Protection by Design

47. The new law requires LSHTM to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data.

48. LSHTM will be providing separate guidance on how to ensure that new processing activities incorporate "privacy by default" and "privacy by design", so that data privacy is considered proactively.

Direct Marketing

49. Please see the privacy notice for alumni for more information on how LSHTM collects and uses data for direct marketing and fundraising purposes.

Personal Data Breach

50. LSHTM is responsible for ensuring appropriate and proportionate security for the personal data that we hold. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. LSHTM makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions. Examples of personal data breaches leading to loss of personal data include:
    a. loss or theft of data or equipment;
    b. inappropriate access controls allowing unauthorised use or deletion;
    c. equipment failure;
    d. unauthorised disclosure (e.g. email sent to the incorrect recipient);
    e. human error; and/or
    f. hacking attack.

51. If a data protection breach occurs LSHTM is required in most circumstances to report this as soon as possible to the Information Commissioner's Office, and not later than 72 hours after becoming aware of it.

52. If you become aware of a personal data breach you must report it immediately. Details of how to report a breach and the information that will be required are available at

www.lshtm.ac.uk/dpo.

Sanctions for non-compliance

53. LSHTM could face fines for non-compliance with the GDPR. There are two tiers of fines depending on the type of infringement, to maximum sums of €10m or €20m depending on the nature of the breach.

54. All LSHTM staff and students are required to comply with this Data Protection Policy, its supporting guidance and the requirements specified in the GDPR. Any member of staff or student who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary action. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of LSHTM i.e. for their own purposes, which are outside the legitimate purposes of LSHTM.

Data Protection Office

55. The person at the School with overall responsibility for compliance with data protection laws is the Secretary and Registrar, assisted and advised by the School's nominated Data Protection Officer.

56. This policy will be reviewed regularly, and at least annually for the first two years in recognition of the developing law, guidance and good practice in the area of data protection. It will be reviewed through the Management Board, with recommendations from the Information Security Working Group and the Data Protection Officer.

57. The School's interim Data Protection Officer is Daniel Scannell, head of the Legal Services Office.

58. In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed to the Data Protection Office: email: dpo@lshtm.ac.uk tel: +44 (0)20 7927 2335.