LSHTM Data Protection Policy

Document Type	Policy
Document owner	Peter Wright – DPO
Approved by	Management Board
Approval date	11 May 2018
Review date	June 2021
Version	1.4 (December 2020)
Amendments	Amending for typographical errors, updates, clarity and consistency with other policies, and to refer to the forthcoming 'UK GDPR'
Related Policies & Procedures	a. LSHTM Records Management policy b. LSHTM Information Management & Security policy and supporting documents c. LSHTM Freedom of Information policy

SCOPE

1. This policy applies to anyone **processing personal data** on behalf of LSHTM, including staff, students, trustees and visitors. It covers all **personal data** that is **processed** by or on behalf of LSHTM. For these purposes, '**personal data**' means any information relating to an identified or identifiable natural person (for the full legal definition, please see the Glossary of Terms contained at Annex 1). In practice, this means that **personal data** encompasses any information in any recorded form which, on its own or when combined with other data, 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 categories of personal data**") now expressly includes genetic and biometric information.

N.B. Terms in **bold** throughout this policy are defined in the Glossary of Terms contained at Annex 1.

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. 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, research participants, 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 personal data** (sometimes called "sensitive **personal data**"), such as a **data subject's** racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, **genetic data**, **biometric data** for the purpose of uniquely identifying a natural person, **data concerning health** or data concerning a natural person's sex life or sexual orientation.

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

6. The Data Protection Act 1998 (DPA1998) was replaced on 25 May 2018 by the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

7. **Important:** Upon the expiry of the Brexit transition period, the GDPR will be retained in UK domestic law as the so-called 'UK GDPR', which will sit alongside an amended Data Protection Act 2018. While there will be some technical amendments to the wording of the EU version of the GDPR to ensure that the legislation works in a solely UK context, the substance of the current data protection regime – including the key principles, obligations and rights, and their implications for universities and their employees, students, research participants, etc. – will remain unchanged, at least for the foreseeable future. This policy will be kept under regular review and will be amended, as necessary, to reflect changes in applicable legislation.

8. Unless the context otherwise dictates, references in this policy to the 'GDPR' should be construed as references to the version of the GDPR in effect in the UK at the relevant time, which from 1 January 2021, will be the UK GDPR.

9. LSHTM is a data **controller** as defined in the GDPR because it chooses why and how it collects and **processes personal data** of staff, students and others.

10. The GDPR applies to data which, alone or together with other data, can identify living individuals, known as **data subjects**, and which relates to those individuals.

11. LSHTM must only **process personal data** in accordance with the key data protection principles – see below for further information.

12. 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 protection and privacy is continually evolving, and this policy and its associated documents will be updated to reflect such change.

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

its behalf.

Principles of data protection relevant to this policy

14. The GDPR sets out the following principles of data protection that require **personal data** to be collected and used fairly and lawfully, 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"**).

15. 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 loss, destruction or damage, using appropriate technical or organisational measures (**"integrity and confidentiality"**);
    a. We are responsible for **processing personal data** in compliance with the above data protection principles and we must have appropriate measures and records in place to demonstrate that we comply ("**accountability**").

16. **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.

17. 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).

18. The GDPR 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.

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

POLICY

LSHTM duties as Data Controller and Data Processor

19. LSHTM is legally responsible for demonstrating compliance with the key data protection principles described at paragraph 12 above. LSHTM arranges mandatory training for staff and students to enable them to comply with the law too. LSHTM is obliged to investigate beaches of this policy and data protection laws, and may take disciplinary action in circumstances where a breach is considered deliberate, including immediate suspension of access to LSHTM facilities. In very serious cases, individuals may face criminal investigation.

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

Information Management and Security

21. 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. Portable devices should not be used to **process personal data** unless this is necessary to meet LSHTM's business requirements;
    b. Any portable devices used for LSHTM work must be encrypted and password protected using a strong password. This applies whether the device is supplied and managed by LSHTM IT Services or personally by the staff member or student (in which case, LSHTM's Bring Your Own Device Policy applies);
    c. USB sticks and removable storage should only be used to store **personal data** in exceptional circumstances (i.e. where no other form of storage is available) and must never be used unless they and/or the files on them are encrypted and password protected with a strong password;
    d. If cloud-based or remote storage is needed, this must be held in an appropriately secure system, which should, wherever feasible, be hosted in the UK or Europe, such as the School's OneDrive for less sensitive **personal data**.
    e. The LSHTM secure server should be used for more sensitive or confidential **personal data** or where required by the NHS Data Security and Protection Toolkit, or a research ethics committee. Please see the LSHTM Data Classification and Handling Policy for more information.

22. 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

23. 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.

24. To comply with the data minimisation and storage limitation principles, 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.

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

Lawful Conditions for Processing

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

    a. Consent: the individual has given clear, valid consent for LSHTM to **process** their **personal data** for a specific purpose.

    b. Contract: the **processing** is necessary for a contract LSHTM has with the individual, or because they have asked LSHTM to take specific steps before entering into a contract.

    c. Legal obligation: the **processing** is necessary for LSHTM to comply with the law (not including contractual obligations).

    d. Vital interests: the **processing** is necessary to protect someone's life.

    e. Public task: the **processing** is necessary for LSHTM to perform a task in the public interest or for LSHTM's official functions, and the task or function has a clear basis in law.

    f. Legitimate interests: the **processing** is necessary for LSHTM's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's **personal data** which overrides those legitimate interests. (This cannot apply in the case of a public authority **processing** data to perform its official tasks.)

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.

27. Under the Data Protection Act 2018, 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.

28. The GDPR and related guidance requires public authorities not to rely upon consent where another basis for lawful **processing** exists, and particularly for the performance of 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.

29. 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**.

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

Privacy Notices

31. LSHTM has produced privacy notices for staff, students, research participants and alumni, among others, available at www.lshtm.ac.uk/aboutus/organisation/data-protection/privacy-notices.

32. **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

33. LSHTM has produced a record of **processing** activities, available upon request from the Data Protection Officer.

34. 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

35. The updated data protection legislation has more stringent controls on the **processing** of **personal data** 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.

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

Research

37. 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 ethics consent on any data collection form, but it is important to

note that consent will not normally be the basis for collecting research data, as explained more fully in the Research Participants Privacy Notice. The Research Governance and Integrity Office can advise on this as part of your ethics application.

38. **Personal data** may be retained indefinitely if they are being held **only** for:
    (a) archiving purposes in the public interest;
    (b) scientific or historical research purposes; or
    (c) statistical purposes.

    Retention of **personal data** for archiving, research or statistical purposes is strictly subject to appropriate safeguards being implemented to protect the rights and freedoms of **data subjects**, including technical and organisational measures to ensure that the retained data is minimised (i.e. adequate, relevant and only the amount necessary for the above purpose(s)). For example, 'pseudonymisation', where the more directly identifying data points in a dataset (such as name, genomic profile, social security or patient number) are removed or replaced with a non-identifiable, preferably random, unique identifier (with the reidentification key being destroyed where possible, or otherwise stored separately and securely) may be appropriate in some cases.
    If **personal data** are retained for any of the above purposes, the data cannot later be used for another purpose - in particular, for any decisions affecting particular individuals. This does not prevent other persons or organisations from accessing public archives, but they must ensure their own collection and use of the **personal data** complies with the relevant data protection legislation.

39. In addition, data which have been properly and genuinely 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 is also highly advised for all studies. Further guidance on pseudonymisation and anonymisation in the context of research can be found at:

    LSHTM-SOP-036: Confidentiality and Anonymisation of Research Data: https://lshtm.sharepoint.com/Research/Research-Governance/Pages/standard-operating-procedures-(sops).aspx;

    or further at:

    https://www.ukdataservice.ac.uk/manage-data/legal-ethical/anonymisation/quantitative.aspx

Data Subject Rights

40. **Data subjects** have express rights to access and correct **personal data** 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.

41. 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.

42. 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.

43. 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 is unlikely to apply as LSHTM does not collect data that would be provided to another higher education provider in an agreed standard form.

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

45. Staff who receive a **data subject** rights request should immediately contact the Data Protection Officer.

Data Sharing

46. 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 business needs;
    d. is necessary for a public task that is core to LSHTM's public functions; or
    e. is based on the **data subject's** consent.

47. LSHTM must also be satisfied that the third party will meet all the requirements of the 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**.

48. Staff who receive requests for **personal data** from third parties such as relatives, police, local councils etc. should consult the guidance on www.lshtm.ac.uk/dpo or immediately contact the Data Protection Officer.

Transfers of Personal Data Outside the UK

49. **Personal data** can only be transferred out of the UK under certain circumstances. These are, in summary: if (a) the transfer is covered by an 'adequacy decision' issued by the UK government; (b) the transfer is covered by 'appropriate safeguards', permitted by the UK GDPR; or (c) one of the limited number of 'exceptions' applies.

50. Information held in cloud storage where the servers are located outside the UK, and/or which are published on the internet must be considered to be an export of data outside the UK.

51. Further guidance on the impact of Brexit on international data transfers out of the UK and to the UK from the EEA will be issued in due course, as the situation evolves.

Data Protection Impact Assessments and Data Protection by Design

52. The GDPR 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**.

53. A Data Protection Impact Assessment (DPIA) is a legal requirement whenever a type of **processing** of **personal data** is 'likely to result in a high risk' to individuals' rights and freedoms. A DPIA screening questionnaire has been integrated into the LSHTM research ethics submission process, with the aim of alerting researchers as to when a DPIA may be required in relation to their proposed study. Further information on DPIAs, and when they are required, can be obtained from the Data Protection Officer.

54. LSHTM will be providing separate guidance on how to ensure that new **processing** activities incorporate "data protection by design and by default", so that data privacy is considered proactively, in line with legal requirements.

Direct Marketing

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

56. While outside the scope of this policy, staff should be aware that other legal requirements and restrictions apply to direct marketing activities under, for example, the Privacy and Electronic Communications (EC Directive) Regulations 2003.

Personal Data Breach

57. LSHTM is responsible for ensuring appropriate and proportionate security for the **personal data** that we hold. This includes protecting the data against **personal data breaches**. LSHTM makes every effort to avoid **personal data breaches**, however, it is possible that mistakes will occur on occasions. Examples of **personal data breaches** 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. cybersecurity incident (e.g. hacking attack).

58. If a **personal data breach** occurs LSHTM is required in many 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.

59. If you become aware of a **personal data breach** you must report it to the Data Protection Officer 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

60. LSHTM could face significant 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.

61. All LSHTM staff and students are required to comply with this Data Protection Policy, its supporting guidance and the requirements specified in the GDPR and Data Protection Act 2018. Any member of staff or student who is found to have made an unauthorised disclosure of **personal data** or breached the terms of this Policy may be subject to disciplinary action. Staff or students may also incur criminal liability if they knowingly or recklessly obtain and/or disclose **personal data** without the consent of LSHTM i.e. for their own purposes, which are outside the legitimate purposes of LSHTM.

Data Protection Office

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

63. This policy will be reviewed regularly, and at least annually 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 Governance Board and the Data Protection Officer.

64. The School's Data Protection Officer is Peter Wright.

65. 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 2708.

Annex 1 – Glossary of Terms Used in this Policy

1. '**personal data**' means any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2. **'processing'** (including '**process**', '**processes**' and '**processed**') means any operation or set of operations which is performed on **personal data** or on sets of **personal data**, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. **'controller'** means the person or organisation which, alone or jointly with others, determines the purposes and means of the **processing** of **personal data**.

4. **'processor'** means a person or organisation which **processes personal data** on behalf of the **controller**.

5. **'special categories of personal data'** means:

    - **personal data** revealing racial or ethnic origin;
    - **personal data** revealing political opinions;
    - **personal data** revealing religious or philosophical beliefs;
    - **personal data** revealing trade union membership;
    - **genetic data**;
    - **biometric data** (where used for identification purposes);
    - **data concerning health**;
    - data concerning a person's sex life; and
    - data concerning a person's sexual orientation.

6. **'data concerning health'** means **personal data** related to the physical or mental health of an individual, including the provision of health care services, which reveal information about their health status.

7. **'genetic data'** means **personal data** relating to the inherited or acquired genetic characteristics of an individual which give unique information about the physiology or the health of that individual and which result, in particular, from an analysis of a biological sample from the individual in question.

8. **'biometric data'** means **personal data** resulting from specific technical **processing** relating to the physical, physiological or behavioural characteristics of an individual which allow or confirm the unique identification of that individual, such as facial images or dactyloscopic (i.e. fingerprint) data.

9. **'online identifiers'** means information relating to the device that an individual is using, applications, tools or protocols such as internet protocol (IP) addresses, cookie identifiers and other identifiers such as radio frequency identification (RFID) tags. Other examples of **online identifiers** that may be **personal data** include: MAC

addresses, advertising IDs, pixel tags, account handles and device fingerprints. The use of these may leave traces which, when combined with unique identifiers and other information received by servers, may be used to create profiles of individuals and identify them.

10. **'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data** transmitted, stored or otherwise **processed**.