Data Protection Policy

Version Control

1. Full Document Number:	LEGPOL001
2. Version number:	7.0
3. Superseded version number:	6.2
4. Document owner job title:	Senior Data Protection & Information Governance Manager
5. Department / function:	Legal & Governance / Information Governance
6. Approved by:	Information Governance Assurance Committee
7. Date of approval:	10/06/2025
8. Next review date:	30/06/2027
9. Date of Equality Impact Assessment:	01/12/2017
10. Accessibility checked: Yes/no	Yes
11. Does this policy apply to LSTM Group (LSTM and subsidiaries?) Yes / No	Yes, including IVCC and WTC.
12. All policies will be added to the LSTM website unless an exception is provided here	
13. If this policy has been reviewed, has this resulted in a minor or major changes?	Minor
14. Does this policy ensure that there is no modern slavery or human trafficking in our supply chains or in any part of our business?	

This document is uncontrolled if downloaded or printed. Always view the current version of the document via the Knowledge Exchange Policy Hub. Approved documents are valid for use after their approval date.

Modifications from previous version of document

Version	Date of issue	Details of modification
4.0	15/01/2018	Change of title from "Data Protection Act Policy" to "Data Protection Policy". Re-worked entire policy to reflect the new GDPR. Incorporated comments from GOC members.
4.0	21/02/2018	Amendment made to 13.3 Breaches of policy by students
5.0	19/02/2019	Add equality and diversity sections (2 and 3). Clarification on the scope of the responsibilities (including students in 5.4 and 5.5, staff and students to seek advice from DPO 5.5), on frequency of training ("annually" in 5.5). Removed reference to Binding Corporate Rules (14.2). Added reference to information security policy (16.1.9). Minor grammatical corrections. Remove reference to undrafted documents & add links to published documents. Checked and updated all footnotes.
5.1	21/05/2019	Updates following Management Committee (training frequency) and Governance Oversight Committee (typographic corrections).
6.0	10/05/2021	Inclusion of Office for Students, LSTM Group wording, updates after EU exit e.g. to specify UK GDPR with maximum fine in £, clarifying Research section on documentation and pseudonymisation based on feedback, removing duplicated content on international transfers and updating cross references to latest documents and more hyperlinks to improve usability. Simplifying language: "individual" rather than "data subject".
6.1	26/05/2022	Section 15 includes links to anonymisation and DPIA guidance
6.2	08/05/2025	Reviewed and revised slightly by the Senior Data Protection & Information Governance Manager. Roles of SIRO and IAO added, plus incorrections and broken links amended. Brought definitions text into line with ICO.
7.0	10/06/2025	Approved by the Information Governance Assurance Committee after addition of sentence about ICO registrations and Artificial Intelligence

Contents

1. Scope

1.1 This policy applies to all personal data handled by LSTM Group (Liverpool School of Tropical Medicine and all subsidiaries). It covers personal data held electronically and in paper files. So long as the processing of the data is carried out for LSTM Group's business purposes, it also applies regardless of where data is held, regardless of who the data is about, and regardless of who owns the PC/device on which it is stored. It therefore applies to all staff, students and third parties acting on its behalf if they are involved in processing personal data as part of their business.

1.2 Definitions are more widely explained below, but "processing" data is widely defined and includes every plausible form of action that could be taken in relation to the data such as obtaining, storing, adapting, altering, retrieving or using it in any way; sharing or disclosing it; erasing and destroying it.

2. Introduction and Context

2.1 Most business functions need to process information about their dealings with people. This includes information relating to staff, students and other individuals. LSTM Group processes these 'personal data' for a variety of reasons, such as to recruit and pay its staff, to record the academic progress of its students and to comply with statutory obligations (for example, health & safety requirements).

2.2 The legislative framework for this is found and referenced in the UK Data Protection Act 2018. This policy outlines the responsibilities of staff and those working with them, including all students, to ensure compliance with the Act and the UK General Data Protection Regulation. For the remainder of this document these two pieces of legislation will be referred to as Data Protection law.

2.3 LSTM is designated as a "public authority" and therefore is required to appoint a Data Protection Officer[1]. This Data Protection Officer has responsibility across the LSTM Group"?

[1] UK GDPR Article 37.1(a) https://ukgdpr.fieldfisher.com/chapter-4/article-37-gdpr/

2.4 LSTM Group acknowledges its obligations under Data Protection law and is committed to protecting the rights and freedoms of all individuals whose personal data are processed as part of its business and research processes.

2.5 As such, LSTM, IVCC (Innovative Vector Control Consortium) and WTC (Well Travelled Clinics) are all registered with the UK Information Commissioner's Office as Controllers. LSTM and LSTM Kenya are also registered with the Office of the Data Protection Commissioner (ODPC) in Kenya as both Controllers and Processors. For more information on this, please see our Information Governance (IG) Framework.

3. Equity and Diversity

LSTM Group is committed to promoting equity of opportunity, combatting unlawful discrimination and promoting good community relations. We will not tolerate any form of unlawful discrimination or behaviour that undermines this commitment and is contrary to our Equity Diversity Inclusion policy.

This document required an Equity Impact Assessment, which is at the end of this document.

4. Safeguarding

LSTM Group believes that everyone we come into contact with, regardless of age, gender identity, disability, sexual orientation or ethnic origin has the right to be protected from all forms of harm, abuse, neglect and exploitation. LSTM Group will not tolerate abuse and exploitation by staff or associated personnel.

LSTM Group recognises its role in safeguarding and protecting our staff, students, volunteers and other representatives as well as the beneficiaries, research participants, patients and communities with whom we have direct and indirect contact through our work. LSTM Group has a zero-tolerance policy for staff and organisational representatives committing any type of harm, exploitation, abuse or harassment.

Safeguarding principles are integral to our approach to our policies and procedures. This policy document reflects our organisational commitment to keeping children and vulnerable adults safe, including our staff and students.

5. Roles and responsibilities

5.1 The LSTM Group Leadership Executive is ultimately responsible for LSTM Group's compliance with Data Protection law via LSTM Group's Chief Operating Officer who acts as the Senior Information Risk Owner (SIRO), with day-to-day responsibility delegated to the Senior Data Protection & Information Governance Manager who acts as the Data Protection Officer (DPO).

5.2 The Legal & Governance department via its Information Governance (IG) Team is responsible for oversight of Information Governance across all of LSTM Group including Data Protection matters which includes drawing up, reviewing and monitoring policies and related guidelines.

5.3 The Data Protection Officer has the following responsibilities:

a) To inform and advise LSTM Group management and staff about their obligations under Data Protection law.

b) To monitor compliance with Data Protection law, LSTM Group's Data Protection policies and procedures, along with the associated Information Governance Framework.

c) To provide advice regarding Data Protection Impact Assessment (DPIA) process and monitor its performance.

d) To cooperate with the Information Commissioner's Office (ICO).

e) To act as the contact point for the ICO on issues relating to processing, including "prior consultation" as outlined in Data Protection law.

5.4 IVCC (Innovative Vector Control Consortium) is supported by the LSTM Information Governance team and has its own Senior Information Risk Owner who reports to the IVCC Leadership Team.

5.5 Staff with responsibilities for processing personal data will adhere to the Policy and adhere to any other guidance or procedures accompanying it.

5.6 Staff will undertake training at least every two years (annual for those involved in high-risk work), be aware of this Policy's existence, and seek advice and clarification on Data Protection matters from the Data Protection Officer.

6. Definitions

Term	Definition
Biometric data	One of the special categories of data under the Data Protection law, defined as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data[2].
Consent	'Consent' of means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. LSTM Group will act as the Controller in most instances.
Data Protection by Design & Default	The promotion of data protection compliance from the start of, and integral to all projects and processes which involve personal data (term previously used was Privacy By Design).

[2] UK GDPR Article 4 https://ukgdpr.fieldfisher.com/chapter-1/article-4-gdpr/

Data Protection Officer (DPO)	To be appointed by a Data Controller where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the Controller or the Processor consist of processing operations which, by their nature, their scope and/or their purposes, require regular and systematic monitoring of individuals on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to UK GDPR Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
Data Subject	A living individual who is the subject of personal data.
Genetic data	One of the special categories of data in Data Protection law, defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result from an analysis of a biological sample from the natural person in question.
Information Asset Owner (IAO)	IAOs have local responsibility for data protection compliance in their directorates / departments. They are also accountable to the SIRO for the information uses within their areas.
Natural Person	A human being as distinguished from a person (as a corporation) created by operation of law[3].

[3] Merriam-Webster Law Dictionary https://www.merriam-webster.com/legal/natural%20person

Personal Data (also known as Personally Identifiable Information)	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.
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.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller. In most instances LSTM Group will need to draw up Data Processing contract / paperwork with the Processor.
Senior Information Risk Owner (SIRO)	A SIRO is an individual who is a member of the Executive within LSTM Group and therefore someone who can influence the organisation on a corporate level. IVCC has also appointed a SIRO.
Special Category personal data (formerly known as sensitive personal data)	Special categories of data have additional rules and processing restrictions covering: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade Union membership • Genetic data • Biometric data (where used for identification purposes) • Health related data (including disabilities) • Sex-life • Sexual orientation
Supervisory Authority	An independent public authority to regulate Data Protection. In the UK, this is the Information Commissioner's Office (ICO).

Third Country	Any country **other than** a member of the European Economic Area (EEA) i.e. EU Member States together with Iceland, Liechtenstein and Norway.

7. Data Protection Principles

7.1 LSTM Group staff, students and third parties acting on its behalf should be aware of the principles of Data Protection law and ensure that these are addressed when dealing with personal data.

7.2 The first principle is lawfulness, fairness and transparency.

7.2.1 For processing to meet the first principle you need to identify a lawful basis. The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

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

c) **Legal obligation:** the processing is necessary for you 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 you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your 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 if you are a public authority processing data to perform your official tasks.)

7.2.2. For Special Category personal data, an extra condition is needed. These are normally one of the following:

a) Explicit consent
b) Employment, social security and social protection (if authorised by law)
c) Vital interests
d) Not-for-profit bodies
e) Made public by the data subject
f) Legal claims or judicial acts
g) Reasons of substantial public interest (with a basis in law)
h) Health or social care (with a basis in law)
i) Public health (with a basis in law)
j) Archiving, research and statistics (with a basis in law)

7.3 The second principle is purpose limitation. Personal data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

7.4 The third principle is data minimisation. Processing of personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7.5 The fourth principle is accuracy. Processing of personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

7.6 The fifth principle is storage limitation. Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required to safeguard the rights and freedoms of individuals.

7.7 The sixth principle is integrity and confidentiality. Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7.8 The final requirement of the Controller, or "seventh principle" is accountability. The controller shall be responsible for, and be able to demonstrate, compliance with the principles. In practice, sufficient records and documentation need to be retained to demonstrate adequacy in this area.

7.9 In addition, Data Protection law imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, to ensure that the level of protection of personal data is not undermined. See the "Guidance Note for International Transfers of Personal Data" for further information.

8. Data Subject Rights in Data Protection law

8.1 Under the Data Protection law, an individual has certain rights.

8.2 Right to be informed[4]. It is necessary to inform the individual via a "Privacy Notice"; and a Privacy Statement on forms gathering personal data which should point to the Privacy Notice. The information given must be concise, transparent, understandable and easily accessible, communicated in clear and plain language and free of charge. All our current Privacy Notices can be found on our website here.

8.3 Right of access. Under Data Protection law, individuals have the right to obtain confirmation that their data is being processed; access to their personal data, and some supplementary information such as that which should be provided in a privacy notice. This is usually known as a "Data Subject Access Request". Further information is provided in LSTM Group's "Data Subject Access Request Procedures".

8.4 Right to rectification. Individuals are entitled to have their personal data corrected if it is inaccurate or incomplete. Those in charge of processing the personal data need to make arrangements to allow this. Self-service updating is preferred, but if this is not possible, then they should promptly action any requests for changes.

8.5 Right to erasure (sometimes known as the right to be forgotten). Individuals have a right to have their personal data erased and to prevent processing in some specific situations. This is especially important where Consent is used as the lawful basis for processing the personal data.

8.6 Right to restrict processing. In certain situations, individuals can limit the way in which their information is used.

[4] The right to be informed | ICO

8.7 Right to data portability. This allows individuals to obtain and reuse their personal data for their own purposes across different services.

8.8 Right to object. Individuals have the right to object to the processing of their personal data in certain circumstances. They can also withdraw their consent if Consent is used as the lawful basis for processing. There are certain conditions around the right to object when the processing is being conducted for research purposes[5].

8.9 Right in relation to automated decision making and profiling. The individual has a right not to be subject to a decision based solely on automated processing including profiling, which produces legal effects concerning them or similarly significantly affects them.

8.10 Any project where the processing could have a high risk of infringing individual rights must complete a Data Protection Impact Assessment (DPIA). This is irrespective of whether any other form of risk assessment has been completed.

9. Data Security and Data Breaches

9.1 The sixth principle "integrity and confidentiality" requires that personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. All staff and students are therefore responsible for compliance with this principle and must follow appropriate guidance and standard operating procedures as laid down by the Data Protection Officer and IT Services. This applies to all personal data held in hard copy or electronic format and from wherever in the world staff are operating. Examples of associated policies and guidance can be found in the list of further information at the end of this policy and include:

- "Acceptable Use of Computer and IT Facilities"
- "Information Classification Matrix"

[5] "Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest" http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Article 21 (Last accessed 05/02/2025)

9.2 Please note that this guidance may change as systems are enhanced or developed or as further advice is obtained from the ICO. It is important that you embed "Data Protection by Design and Default" principles into any current or planned initiative (including new IT systems, Projects and Data Sharing initiatives), so you should ensure that you are using the most up-to-date guidance available and check with IT Services or the Information Governance Team if you are unsure. The way for doing this is by completing a DPIA Screening Questionnaire which in turn will lead (if required) to a Data Protection Impact Assessment (DPIA).

9.3 Reporting of data breaches. A personal data breach should be reported to the supervisory authority "*…without undue delay and, where feasible, not later than 72 hours after having become aware of it…*". The only exception to this is where the personal data breach is "*…unlikely to result in a risk to the rights and freedoms of natural persons*". All LSTM Group staff and students must understand this principle and follow the procedure when they identify a potential data breach. See the "Procedure for Notification of Security Breaches" for further information. All breaches, security incidents and near misses must be reported to the Information Governance (IG) Team who keep a central log of incidents across LSTM Group. Issues should be reported using the Data Breach Report Form although it's important to alert the Team as soon as possible due to the ICO reporting deadline.

9.4 International Data Transfers are defined as moving data between countries, with a particular focus on transfers going outside the European Union / EEA. Staff must ensure that the method of transfer they use complies with the Data Protection law. Any breach of this would automatically result in a higher tier fine. Refer to the "International Transfers of Personal Data Guidance" for further details. All instances of International Data Transfers need to be logged with the IG Team who keep a central register for LSTM Group.

10. Prohibited activities

10.1 The following activities are strictly prohibited:

a) Using data obtained for one purpose for another supplemental purpose (e.g. using personal data obtained from student registration for marketing purposes unless consent was obtained for this in the first instance);

b) Disclosing personal data to a third person outside of LSTM Group without the

consent of the data subject;

c) Carriage of personal data on non-LSTM Group laptops or other devices which are not encrypted to standards set by IT Services.

d) Artificial Intelligence (AI) solutions – these should not be used for processing personal data unless due diligence has been done via the Data Protection Impact Assessment (DPIA) process and IT Services. For more information, please contact the IG Team or the Cyber Security Team.

10.2 If you have doubts about an activity not listed above, then please seek advice from the IG Team.

11. Data Subject Access Requests (DSARs)

11.1 Under Data Protection law, the individual has the right to obtain:

a) Confirmation that their personal data is being processed;

b) Access to their personal data;

c) Other supplementary information (this mirrors the information provided in the Privacy Notice i.e. purpose of processing, categories of data being processed etc.)

11.2 Under law, DSARs need to be responded to within one calendar month, and no fee can be charged. Such a request for access must be handled according to the "Data Subject Access Request Procedure".

11.3 Third Party access – this could be a party acting on behalf of the data subject. This may be allowed, but the appropriate procedures must be followed in ascertaining the right of the third party to make the request.

11.4 Freedom of Information (FOI) requests for the requester's personal data. Any such request received by LSTM Group relating to the requester's personal data must be treated as a DSAR rather than an FOI request. Access to personal data is an exemption under FOI.

11.5 If you receive a DSAR, notify the IG Team as soon as possible to ensure it is logged and handled appropriately.

12. Release for Crime and Taxation Purposes

12.1 Legislation includes exemptions for the following purposes:

a) The prevention or detection of crime;

b) The capture or prosecution of offenders; and

c) The assessment or collection of tax or duty[6].

12.2 However, the exemption applies, only to the extent that complying with a SAR would be likely to prejudice the crime and taxation purposes set out above.

12.2.1 Procedures exist which must be invoked in the event of an approach by an enforcement agency (e.g. Police, UK Border Force). The member of staff receiving the request must immediately invoke these procedures and the release of information can only be authorised by the senior members of LSTM Group's staff named therein.

13. Research data

13.1 LSTM Group staff embarking on research which involves personal data should ensure that they have understood this policy and associated guidance, have documented how they will comply, and have communicated instructions to ensure research group members and collaborators understand how to protect the data. This documentation will include, at the very least, completing Data Management Plan as required in the Research Data Management Policy (section 3.3).

13.2 There is an specific Data Protection Impact Assessment for research projects, and this is available from the IG Team along with more guidance and assistance with their completion.

13.3 Personal data obtained or used for research should be limited to the minimum amount which is reasonably required to achieve the designed academic objectives. Pseudonymisation and other techniques should be applied wherever possible to protect the privacy of participants.

13.4 There are some exemptions in the legislation regarding data obtained for "…archiving, research and statistical purposes", for example, allowing personal data to be held for longer than the original purpose it was obtained.

[6] What other exemptions are there? | ICO (Last accessed 05/02/2025)

14. Consequences of breaching this policy

14.1 A contravention of Data Protection legislation which breaches the rights of an individual can lead to fines. There are two levels of fines, but the maximum fine for the higher tier (serious breaches) is up to £17.5 million or 4% of total annual worldwide turnover (whichever is higher), and possible litigation against the individual or individuals responsible for the breach. Some Data Protection offences can also bring a criminal conviction and prison sentence for individuals at fault. Any contravention could seriously damage LSTM Group's reputation which, in turn, could have negative impact on relationships with our funders, partners and regulatory authorities. Responsibilities are therefore taken very seriously, and all staff and students are expected to comply with this policy, and the training and guidance which has been provided.

14.2 Breaches of this policy by staff will be investigated, and where appropriate, formal disciplinary action may be taken up to and including dismissal.

14.3 Breaches of this policy by students will be investigated, and where appropriate, formal disciplinary action may be taken up to and including termination of studies.

14.4 Breaches by consultants or other third parties acting on behalf of LSTM Group may lead to the termination of their contract.

14.5 If you have any concerns that this policy is being breached, please contact the IG Team without delay. If you wish to remain anonymous then you may also use the Whistleblowing Policy.

15. Further information

15.1 Related documents including policies, guidance and procedures are listed here:

a) "Acceptable Use of Computer & IT Facilities"

b) "Anonymisation Guidance"

c) "Completion of Data Protection Impact Assessments Guidance"

d) "Data Subject Access Request Procedures"

e) "Disciplinary Policy"

f) "Freedom of Information Policy"

g) "Guidance Note for International Transfers of Personal Data"

h) "Information Classification Matrix"

i) "Procedure for Notification of Security Breaches"

j) "Procedure for the Release of Information to Prevent or Detect Crime"

k) "Research Data Management Policy"

l) "Whistleblowing Policy"