Data Protection Policy

Version Control

1. Full Document Number:	OPEPOL001
2. Version number:	6.1
3. Superseded version number:	6.0
4. Document owner job title:	Data Protection Officer
5. Department / function:	Strategic Operations
6. Approved by:	Research Governance Oversight Committee
7. Date of approval:	18-5-2021
8. Next review date:	01-05-2023
9. Date of Equality Impact Assessment:	01-12-2017
10. Equality Impact Assessment Reference Number:	EIA - 19458
11. Does this policy apply to LSTM Group (LSTM and subsidiaries?)	Yes
12. Add document to external LSTM website?	Yes

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	15.01.18	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	21.02.18	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 crossreferences 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 Section 13 includes reference to overarching Research DPIA

Contents

1 Scope

1.1 This policy applies to all personal data handled by LSTM Group. It covers data held in paper files and held electronically. 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 in LSTM Group 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, 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 found and referenced in the UK Data Protection Act 2018 ("the Act"). This policy outlines the responsibilities of staff and those working with them, such as certain students, to ensure compliance with the Act and the UK General Data Protection Regulation ("the Regulation").

2.3 LSTM and its wholly owned subsidiaries are designated as a "public authority" and so are required to appoint a Data Protection Officer[1].

2.4 The LSTM Group acknowledges its obligations under the Regulation 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.

3 Equality and Diversity

LSTM is committed to promoting equality of opportunity, combatting unlawful discrimination and promoting good community relations. We will not tolerate any

[1] UK GDPR Article 37.1(a) https://ukgdpr.fieldfisher.com/chapter-4/article-37-gdpr/ (last accessed 27/4/21)

form of unlawful discrimination or behaviour that undermines this commitment and is contrary to our equality policy.

4 Safeguarding

In line with our Safeguarding policy and procedures, LSTM's processes reflect our organisational commitment to keeping children and vulnerable adults safe.

5 Roles and responsibilities

5.1 The LSTM Board is ultimately responsible for LSTM's compliance with the Regulation via the LSTM Director and senior management team, with day-to-day responsibility delegated to the Data Protection Officer.

5.2 The Research Governance Oversight Committee is responsible for oversight of information governance at LSTM including data protection matters which includes reviewing and approving policies and related guidelines.

5.3 The Data Protection Officer has the following responsibilities:

5.3.1 To inform and advise LSTM management and staff about their obligations under the Regulation;

5.3.2 To monitor compliance with the Regulation, the LSTM data protection policies and associated framework;

5.3.3 To provide advice where requested regards the data protection impact assessment and monitor its performance;

5.3.4 To cooperate with the Information Commissioner's Office (ICO);

5.3.5 To act as the contact point for the ICO on issues relating to processing, including "prior consultation" as outlined in Article 36 of the Regulation.

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

5.5 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 Regulation, 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 he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. LSTM will act as the data controller in most instances.
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller. In most instances LSTM will need to draw up a data processing contract with the processor.
Data Protection Impact Assessment	A process designed to describe the processing, assess the necessity and proportionality of processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them). The minimal content is specified in Article 35(7)[3].

[2] UK GDPR Article 4 https://ukgdpr.fieldfisher.com/chapter-1/article-4-gdpr/ (last accessed 27/4/21)
[3] UK GDPR Article 35 https://ukgdpr.fieldfisher.com/chapter-4/article-35-gdpr/ (last accessed 27/4/21)

Data Protection Officer	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 the Regulation, 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.
Natural person	A human being as distinguished from a person (as a corporation) created by operation of law[4].
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.
Privacy by design	The promotion of privacy and data protection compliance from the start of, and integral to all projects which involve personal data.

[4] Merriam-Webster Law Dictionary https://www.merriam-webster.com/legal/natural%20person (Last accessed 27/4/21)

Processing	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.
Special categories (formerly known as sensitive personal data)	Special categories of data have additional rules and processing restrictions covering: • Racial or ethnic origin • Political opinion / affiliation • Religious or political beliefs • Trade Union membership • Genetic / biometric data (for the purpose of uniquely identifying a natural person) • Health related • Sex-life / sexual orientation
Supervisory authority	An independent public authority to regulate data protection. In the UK, this is the Information Commissioner's Office.
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 staff and students should be aware of the principles of the Regulation and ensure that these are addressed when dealing with personal data.

7.2 The first principle is legality, transparency and fairness:

7.2.1 For processing to meet the first principle you need to identify a lawful basis. This can include consent, but where this is the case the individual may have greater rights as a result, e.g. to have their data deleted. LSTM will always identify that legal basis and communicate this to an individual before processing their data. Apart from consent, other possible legal bases are:

• necessary for performance of a contract;
• compliance with a legal obligation;
• to protect the vital interests of the individual or another person;
• for the purposes of legitimate interests or in the exercise of official authority invested in the data controller.

7.2.2 For special categories of data, an extra condition is needed. To share this information explicit consent is usually required.[5]

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 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 Individuals 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, the Regulation 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.

7 Rights in data protection law

7.1 Under the Regulation, an individual has certain rights.

[5] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/ Last accessed 05/03/2019

7.2 The first of these is the right to be informed. It is necessary to inform the individual via a "privacy notice". The information given must be concise, transparent, understandable and easily accessible; communicated in clear and plain language and free of charge.

7.3 Right of access. Under the Regulation, individuals will 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 "subject access request". Further information is provided in "The Subject Access Request Procedures".

7.4 Right to rectification. Individuals are entitled to have their personal data corrected if it is inaccurate or incomplete. Those in charge of 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.

7.5 Right to erasure (right to be forgotten). Individuals have a right to have their personal data erased and to prevent processing in some specific situations.

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

7.7 Right to data portability. This is a new concept which did not exist in the UK Data Protection Act 1998 and allows individuals to acquire and reuse their personal data for their own purposes, but only in certain circumstances.

7.8 Right to object. Individuals have the right to withdraw their consent. There are certain conditions around the right to object when the processing is being carried out for research purposes[6].

7.9 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 him or her or similarly significantly affects them.

7.10 Any project where the processing could have a high risk of infringing individual rights must complete a Data Protection Impact Assessment (see Guidance on their completion here).

[6] "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 05/03/2019)

8 Data Security and Data Breaches

8.1 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 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"

8.2 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 "privacy by design" principles into any current or planned project, so you should ensure that you are using the most up-to-date guidance available and check with IT Services or the Data Protection Officer if you are unsure.

8.3 One major change to data protection brought in by the Regulation is the 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 staff and students must understand this principle and to follow the procedure when they identify a potential data breach. See the "Procedure for Notification of Security Breaches" for further information.

8.4 International transfers are defined as moving data between countries, with a particular focus on transfers going outside the European Union. Staff must ensure that the method of transfer they use complies with the Regulation. Any breach of the Regulation would automatically result in a higher tier fine. Refer to the "International Transfers of Personal Data Guidance" for further details.

9 Prohibited activities

10.1 The following activities are strictly prohibited:

9.1.1 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);

9.1.2 Disclosing personal data to a third person outside of LSTM without the consent of the data subject;

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

9.2 If you have doubts about an activity not listed above, then please seek advice from the Data Protection Officer.

10 Subject Access Requests

10.1 Under the Regulation, the individual has the right to obtain:

10.1.1 Confirmation that their data is being processed;

10.1.2 Access to their personal data;

10.1.3 Other supplementary information (this mirrors the information provided in the privacy notice i.e. purpose of processing, categories of data being processed etc.)

10.2 This right of access was referred to as a "subject access request" (SAR) under the Data Protection Act 1998. Under the Data Protection Act 2018 the response time has reduced from forty days to one month, and no fee can be charged. Such a request for access must be handled according to the "Subject Access Request Procedure".

10.3 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.

10.4 Freedom of Information requests for the requester's personal data. Any such request which is received by LSTM relating to the requester's personal data should be treated as a SAR.

10.5 If you receive a SAR, notify the Data Protection Officer as soon as possible to ensure it is logged and handled appropriately.

11 Release for Crime and Taxation Purposes

12.1 The legislation includes exemptions for the following purposes:

11.1.1 The prevention or detection of crime;

11.1.2 The capture or prosecution of offenders; and

11.1.3 The assessment or collection of tax or duty[7].

11.2 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.

11.2.1 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 staff named therein.

12 Research data

12.1 LSTM 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).

12.2 There is an overarching Data Protection Impact Assessment for research. Some research projects may be outside of this scope and, if high risk, will need to complete a project-specific Data Protection Impact Assessment. There is guidance available on how to complete a DPIA (see link in Section 14).

12.3 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.

12.4 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.

13 Consequences of breaching this policy

14.1 A contravention of data protection legislation which breaches the rights of a individual can lead to fines of up to £17.5 million, 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

[7] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/ Last accessed 10/05/2021

relevant 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 If you have any concerns that this policy is being breached, please communicate them to the Data Protection Officer without delay.

14 Further information

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

14.1.1 "Acceptable Use of Computer & IT Facilities"

14.1.2 "Guidance Note for International Transfers of Personal Data"

14.1.3 "Information Classification Matrix"

14.1.4 "Procedure for Notification of Security Breaches"

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

14.1.6 "Subject Access Request Procedures"

14.1.7 "Staff disciplinary policy and procedure

14.1.8 "Anonymisation Guidance"

14.1.9 "Completion of Data Protection Impact Assessments Guidance"