Data Protection Policy

DOCUMENT CONTROL INFORMATION			
Document type	POL (Policy)	**Full Document Number**	ISTPOL002
Version:	4.0	**Superseded Version:**	3.0
Originator:	Julia Martin	**Job title:**	Head of Information Services
Department / Function:	IST (Information Services)	**Subject category:**	Information Governance
Authorship date:	14-12-2017	**Published date:**	04-04-2018
Management Committee sign off date:	Feb 2018	**Date for Review:**	14-12-2018
Date of Equality Assessment "due regard" form (Equality Act 2010):	01-12-2017	**Equality Assessment reference number:**	EIA - 19458

Please ensure you are viewing the current version of the document.

Target Audience	
People who need a detailed knowledge of the document	All staff involved in processing personal data
People who need a broad understanding of the document	
People who need to know that the Code of Practice exists	All staff

Contents

1 Introduction and Context

1.1 LSTM needs to process certain types of information about the people with whom it deals. This includes information relating to its staff, students and other individuals. It needs to process '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).

1.2 The legislative framework for this has been the Data Protection Act 1998 "the Act", however, from 25 May 2018 this will be replaced by the EU General Data Protection Regulation (GDPR) "the Regulation". The UK Parliament is also preparing a Data Protection Act (currently "Bill") to amend the GDPR for the UK, post-Brexit. This policy outlines the responsibilities of staff, students and other parties connected with LSTM in ensuring compliance with this Regulation.

1.3 As required by Article 37 of the Regulation, LSTM is designated as a "public authority" under the UK Data Protection Bill "the Bill" and is required to appoint a Data Protection Officer[1].

1.4 LSTM acknowledges its obligations under the Regulation and is committed to protecting the rights and freedoms of all individuals whose personal data is processed as part of its business and research processes.

2 Scope

2.1 This policy and the EU General Data Protection Regulation apply to all personal data handled by the School, both that held in paper files and data held electronically. So long as the processing of the data is carried out for LSTM'S business purposes, it also applies regardless of where data is held, (for example, it covers data held on campus and on mobile devices such as on electronic notebooks or laptops) and regardless of who owns the PC/device on which it is stored.

2.2 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.

[1] https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/lbill_2017-20190066_en_2.htm#pt2-ch2-pb1-l1g6 (Viewed 25/10/2017)

3 Roles and Responsibilities

3.1 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.

3.2 The 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.

3.3 The Data Protection Officer has the following responsibilities:

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

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

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

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

3.3.5 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.

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

3.5 All staff will undertake training and be aware of the Policy's existence.

4 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].

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Article 4 (Viewed on 26/10/17)

Consent	'Consent' of the data subject 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.
Data Protection Impact Assessment	A process designed to describe the processing, assess the necessity and proportionality of a 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].
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 virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects 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 Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
Data subject	An 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

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN Article 35

	genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, 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[5];
Privacy by design	The promotion of privacy and data protection compliance from the start of, and integral to all projects which involve personal data.
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)	Article 9 of the GDPR refers to special categories of data, e.g.: • 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)

[4] Merriam-Webster Law Dictionary (accessed 27/10/17)

[5] As defined in the Regulation Art. 4 (12) "Definitions": http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

	• Health related • Sex-life / sexual orientation Special categories have additional rules and processing restrictions.
Supervising authority	An independent public authority which is established by a Member State pursuant to Article 51. 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.

5 General Data Protection Regulation (GDPR) principles

5.1 LSTM staff and students should be aware of the principles of the Regulation and ensure that these are addressed when dealing with personal data.

5.2 The first principle is legality, transparency and fairness:

5.2.1 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 a data subject 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 data subject or another person;
- for the purposes of legitimate interests or in the exercise of official authority invested in the data controller.

5.2.2 For special categories of data, explicit consent is usually required[6].

5.3 The second principle is purpose limitation:

5.3.1 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.

5.4 The third principle is minimisation:

[6] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/

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

5.5 The fourth principle is accuracy:

5.5.1 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.

5.6 The fifth principle is storage limitation:

5.6.1 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 by the GDPR in order to safeguard the rights and freedoms of individuals.

5.7 The sixth principle is integrity and confidentiality:

5.7.1 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.

5.8 The final requirement of the controller, or “seventh principle” is accountability:

5.8.1 Article 5(2) requires that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.” This is sometimes referred to as the “Seventh principle”. In practice, sufficient records and documentation need to be retained to demonstrate adequacy in this area.

5.9 In addition, the Regulation imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Please refer to the “Guidance Note for International Transfers of Personal Data” for further information.

6 Rights under the General Data Protection Regulation (GDPR)

6.1 Under the Regulation, a data subject has certain rights.

6.2 The first of these is the right to be informed:

6.2.1 It is necessary to inform the data subject 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.

6.3 Right of access:

6.3.1 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".

6.4 Right to rectification:

6.4.1 Data subjects 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.

6.5 Right to erasure (right to be forgotten)

6.5.1 Individuals have a right to have their personal data erased and to prevent processing in some specific situations.

6.6 Right to restrict processing

6.6.1 In certain situations, the data subject has a right to restrict processing.

6.7 Right to data portability

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

6.8 Right to object

6.8.1 Data subjects 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[7].

6.9 Right in relation to automated decision making and profiling

6.9.1 The data subject 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] "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 [Accessed 3/11/2017]

7 Data security and data breaches

7.1 The sixth principle "integrity and confidentiality" stipulates 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"

7.2 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.

7.3 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*". LSTM will put in place suitable procedures to enable this requirement to be met, but it is incumbent on all staff and students to understand this principle and to follow the procedure in the event of their identifying a potential data breach. See the "Procedure for Notification of Security Breaches" for further information.

7.4 International transfers are defined as moving data outside of the EU. LSTM staff and students 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 "Guidance Note for International Transfers of Personal Data" for further details of how to comply with this requirement.

8 Prohibited activities

8.1 The following activities are strictly prohibited:

8.1.1 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);

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

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

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

9 Subject access requests

9.1 Under the GDPR, the data subject has the right to obtain:

9.1.1 Confirmation that their data is being processed;

9.1.2 Access to their personal data;

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

9.2 This right of access was previously referred to as a "subject access request" under the Data Protection Act 1998. The GDPR has brought some changes to this, most notably that the response time is reduced from forty days to one month and that no fee may be charged. Such a request for access must be handled according to the "Subject access procedures" which accompany this policy.

9.3 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.

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

9.5 When an SAR involves 3rd party information you need to seek the other individuals' consent.

9.6 Exemptions may be allowed to SARs in certain circumstances which include the prevention of crime and assessment of taxes (see below). These exemptions apply where the release of the information is "likely to prejudice" the function of the organisation to which the request is made. The advice given by the ICO is that this must constitute a "substantial chance" and not a mere risk that complying with the SAR would noticeably damage the discharge of the function concerned [8].

[8] https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf [Viewed on 2/11/2017]

10 Release for crime and taxation

10.1 The legislation includes exemptions for the following purposes:

10.1.1 The prevention or detection of crime;

10.1.2 The capture or prosecution of offenders; and

10.1.3 The assessment or collection of tax or duty[9].

10.2 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.

10.2.1 A set of 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.

11 Research data

11.1 LSTM staff or students embarking on research which involves personal data should ensure that they have understood this policy and associated guidance and have documented (as per privacy by design guidance) how they will comply. Personal data obtained or used for research should be limited to the minimum amount which is reasonably required to achieve the designed academic objectives. Anonymisation techniques should be applied where possible so that the data subjects cannot be identified.

11.2 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.

12 International transfers

12.1 Personal data can only be transferred outside the European Union in compliance with the conditions for transfer set out in Chapter V of the Regulation. The "Guidance Note for the International Transfers of Personal Data" outlines how transfers can be made in accordance with the Regulation.

12.2 LSTM undertakes to only transfer personal data where the organisation receiving the personal data has provided adequate safeguards. These include legally binding

[9] https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/lbill_2017-20190066_en_14.htm#sch2

agreements between public authorities or bodies; binding corporate rules and standard data protection clauses. Further detail is available in: “Guidance Note for International Transfers of Personal Data”.

13 Risks and implications of breaching this policy

13.1 A serious contravention of data protection legislation which breaches the rights of a data subject can lead to fines of up to Euros 20 million (or 4% of annual global turnover) whichever is the greater and possible litigation against the individual or individuals responsible for the breach. Apart from the fine, such a contravention would be seriously damage to LSTM’s reputation which, in turn, could have negative impact on relationships with our funders and regulatory authorities. As a result, LSTM takes its responsibilities very seriously and expects its staff and students to comply with this policy, and the training and guidance which has been provided.

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

13.3 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 Related documents and 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 “Guide to anonymization in clinical studies”

14.1.3 “Guidance Note for International Transfers of Personal Data”

14.1.4 “Information Classification Matrix”

14.1.5 “Procedure for Notification of Security Breaches”.

14.1.6 “Procedure for the Release of Information to Prevent or Detect Crime”

14.1.7 “Subject Access Request Procedures”

14.1.8 Staff disciplinary procedures

N.B. At the time of writing, the Data Protection Bill is going through the UK Parliament. Advice and guidance may change and the latest guidance will be available on the LSTM Knowledge Exchange (staff intranet).

Annex of Modifications		
Version	**Date of issue**	**Details of modification from previous version**
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