LSTM Data Protection Act Policy

Reference Number:	**ISS/POL/002**	**Reviewed by ICT:**	**9/10/2013**
Version number:	**2.0**	**Approved by MC:**	**31/10/2013**
Superseded Version Number:	**[v.1.0] 30/11/2010**	**Effective Date:**	**01/11/2013**
Originator:	**Julia Martin**	**Review Date:**	**01/10/2015**
Comments:			

General Principles

- Under UK law, LSTM is required to comply with DPA legislation;
- All staff and student are expected to be familiar with the Act when handling personal data as defined by the Act;
- Extra security and precautions must be in place when handling sensitive data as defined by the Act;
- A serious breach of the Act could result in a prosecution for LSTM and so contravention must be taken seriously and could result in disciplinary proceedings.

Abbreviations

DPA – Data Protection Act, 1998

1. Scope and Purpose

The purpose of this policy is to ensure that staff and students at the Liverpool School of Tropical Medicine comply with the provisions of the Data Protection Act 1998 when processing personal data.

2. Responsibilities

Responsibilities in compliance with the DPA lie with any member of staff or student processing personal information as defined within the Act.

The Director is ultimately responsible for LSTM's compliance with the Act and day-to-day responsibility for this is delegated to the Head of Information Services (Data Protection Officer).

The Data Protection Officer is responsible for ensuring that LSTM's registration with the Information Commissioner's Office is accurate and up-to-date. Any member of staff who identifies a new requirement for the use of personal data within the organisation must notify the Data Protection Officer who will make the necessary arrangements to update LSTM's

registration information. You can check LSTM's registration details via the Information Commissioner's website at:
http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

3. Main points

As a data user LSTM is legally required to manage personal data in accordance with the Act. Examples of personal data are: name, address, personal e-mail, date of birth.

All staff and students must follow the 8 main principles of the Act which state that personal data of any living person must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary;
- Processed in line with [the individual's] rights;
- Secure;
- Not transferred to other countries without adequate protection.

Within the Act, some data is considered of extra sensitivity and hence requires extra care and security in its handling. Such data includes: racial or ethnic origin, religious beliefs, physical or mental health.[1] Staff and students handling such data must pay particular care to its security. It should be held in a secure environment and its removal or transfer should not occur without due consideration being given to a secure method. For example, carrying such data on an unencrypted laptop or USB drive is not acceptable. Further guidance on general security is available in LSTM's "LSTM IT Security Policy".

It is never acceptable to release personal information unless you are sure that the requestor is who they say they are, so members of staff should be very wary of unsolicited telephone calls even if the person sounds genuine. You should take care not to confirm or deny if someone works at LSTM, but to refer the caller to the Data Protection subject access requests procedure on the LSTM web site and request that they apply for any information in writing. Details of this process are in section 4 below.

All staff and students must familiarise themselves with the contents of the Act if they are handling personal data and must not infringe the Act. Guidance for staff is available on the Staff Intranet under Data protection.

A serious breach of the Act could result in very serious penalties to LSTM including the imposition of a fine as high as £500,000.

4. Subject Access Requests

These may be placed by anyone that LSTM holds personal data on including current or ex staff and students.

[1] A full list is available at:
http://pcwww.liv.ac.uk/lstmintranet/information_services/dataprotection/definitions.htm

The "Release of Information to Prevent or Detect Crime Policy" outlines the procedures which must be followed in the event of such a request from the Police or other enforcement agencies. All general subject access requests must be directed towards the Data Protection Officer and the current procedures are available on the LSTM website.

5. Guidance

This policy cannot cover all DPA issues. Staff are advised that further information can be found on the staff intranet at:
http://pcwww.liv.ac.uk/lstmintranet/information_services/dataprotection/index.htm

Information on DPA matters for students can be found on the student intranet at: [Insert link]

6. Contact

If you are unsure about your responsibilities under the Data Protection Act, or have any other queries, please contact the Head of Information Services (Data Protection Officer):

Julia Martin Tel. Ext. 3191, E-mail: j.martin@liv.ac.uk

7. Linked policies

1. **Data Protection Act: LSTM Policy for Release of Information to Prevent or Detect Crime**:
http://pcwww.liv.ac.uk/lstmintranet/information_services/policies/documents/dpa_crimeprevention.pdf

2. **IT Security Policy**:http://pcwww.liv.ac.uk/lstmintranet/information_services/policies/index.htm

8. Enforcement

A serious violation of this Act would at least result in a loss of reputation for LSTM; but in addition, could result in prosecution and a fine up to £500,000. Therefore, it is imperative that staff and students understand their responsibilities under the Act. An initial breach of the policy may be dealt with in an advisory way and the reasons for non-compliance explained. However, if a breach is considered to be serious in nature and/or you subsequently breach the policy, further action will be initiated, which for staff and students may include formal disciplinary proceedings.

Julia Martin 21st October 2010
(Head of Information Services) Revised 25th July 2013