LIVERPOOL MEDICAL INSTITUTION

DATA PROTECTION POLICY

Policy Reference	LMI 016
Current Version	March 2018 (K. Alsop)
Original Version	*January 2015 (K. Alsop)*
Current version accepted by the SMC at its meeting dated	05.08.2018
Signed by the Chair of SMC	Derek Machin

Application: this policy is applicable to all staff, volunteers and Trustees of the LMI.

Review: this policy will be reviewed two years following the current version date or when legislation changes.

1.0 Data Protection Policy Statement

1.1 The Liverpool Medical Institution (LMI) seeks to comply fully with The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), ("the Act") by regulating the use of personal data by those who obtain, hold and process data on living individuals and by providing certain rights, such as, the accessing of personal information, to those living individuals whose data is held by the LMI.

1.2 This policy sets out the principles of the Act and details the duties of staff/ volunteers/Trustees in relation to the processing of personal data and the safeguarding of individuals' rights and freedoms.

2.0 Definitions

2.1 The "Data Controller" for the purposes of the Act is the Strategic Management Council (SMC). The Data Controller shall be responsible for, and be able to demonstrate compliance with GPDR.

2.2 The "Data Protection Officer" for the purposes of the Act is the LMI Manager.

2.3 "Data subjects" are those for whom data is held, for example, employees and members.

2.4 "Personal data" includes any information about an individual where that data identifies an individual, for example, name, address, e-mail address, photograph, posts on social networking websites, or a computer's IP address.

2.5 "Sensitive personal data" is that which could be used to positively identify a data subject and could be used to their detriment, for example, bank account details, medical information, gender, religion, race, sexual orientation, criminal records and proceedings.

3.0 Data Protection Principles

3.1 The Act sets out six Data Protection Principles, which are as follows:

3.1.1 Personal data shall be processed fairly, lawfully and in a transparent manner in relation to the data subject.
3.1.2 Personal data shall be obtained only for specified, explicit and legitimate purposes and shall not further be processed in any manner incompatible with those purposes.
3.1.3 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

3.1.4 Personal data shall be accurate and, where necessary, kept up to date.
3.1.5 Personal data shall 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.
3.1.6 Personal data shall 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.

4.0 Administration of Personal Data

4.1 Acquisition of Personal Data: LMI staff may collect personal data for the following purposes:

- Administration of the membership database and the collection of subscriptions
- Administration of conferencing and meeting facilities, whether held by external bodies or managed internally, such as, the annual sixth form medical conference
- Procurement of, and payment for, goods and services
- Marketing of meetings, conferences and events
- Administration of staff payroll
- Recruitment of staff
- Administration of the Strategic Management Council to comply with the requirements of the Charities Commission, Companies House and the like

When collecting personal data, the data subjects must be informed of the specific purpose or purposes for which their data is being collected by means of a privacy notice. Privacy notices must be accessible and understandable. An example of a privacy notice is included at Appendix A. LMI may not communicate with the data subject without the consent of the data subject.

No more data should be collected than is necessary for the purpose or purposes declared.

4.2 Retention and Disposal of Personal Data: data should not be held for longer than is necessary. The LMI Records Management Policy details how long specific data should be retained for.

Personal data should be reviewed periodically to check that they are accurate and up to date and to determine whether retention is still necessary. The personal data audit should be reviewed every two years

Adequate measures should be taken to safeguard data, so as to prevent loss, destruction or unauthorised disclosure. The more sensitive the data, the greater the measures need to be. Measures include the following:

- Locking away files containing personal data when not in use
- Access to electronic membership data is limited to the admin team and the Finance and Project Manager
- Access to electronic financial data is limited to the Finance and Project Manager and is password protected
- Reports to the SMC, the Membership and Education Committee do not reveal any sensitive personal data.

Where data is to be disposed of, all hard copies must be shredded. Appropriate measures must be taken to ensure that data cannot be reconstructed and utilised by third parties.

4.3 Processing of Personal Data: processing of personal data comprises the editing, amending or querying of data. This shall only be carried out by the staff authorised to do so and with care as to the accuracy of the data.

Members may be contacted when the renewal date for membership is due but if they fail to renew after a reminder, they may not be contacted for the following year's renewal as their consent to be contacted will be considered withdrawn.

Processing of personal data must be carried out on LMI premises and data must not be taken off site, whether in hard copy or electronically.

4.4 Accuracy of Personal Data: LMI shall seek to ensure the accuracy of all personal data held in relation to data subjects. Data subjects have a duty to notify the data processor of any changes to information held about them.

4.5 Disclosure of Personal Data: LMI staff must exercise discretion under the Act to protect the confidentiality of those who persona data it holds. In particular,

- LMI staff must not disclose any information about members, volunteers, staff, applicants for events or applicants for LMI jobs unless they are clear that the Data Protection Officer has given authority for them to do so. Particular care should be given to the posting of personal information on the Internet.
- LMI staff must not provide references to prospective employers or landlords or others without the consent of the data subject concerned.
- LMI staff must not disclose personal data to the police or any other public authority unless the disclosure has been authorised by the Data Protection Officer.

4.6 Exemptions: data which is exempted from the provisions of GDPR includes:

- Data pertaining to national security and the prevention/detection of crime
- The assessment of any tax or duty
- Where processing is necessary to exercise a right or obligation conferred or imposed by law, including safeguarding and the prevention of terrorism and radicalisation.

4.7 Right of Access to Personal Data by Data Subjects: if a data subject wants to see their personal data held by the LMI, they must put their request in writing supported by documentary evidence of their identity. All data subject access requests are to be for the attention of the Data Protection Officer. Such request is subject to a fee of £10. Requests will be processed within 21 days of receipt.

4.8 Donor Right to be Forgotten: data subjects who make donations to LMI have the right to be forgotten, that is, to retain their anonymity. Staff who deal with donations shall respect this right and not disclose this information to others.

5.0 Protecting Sensitive Personal Data

5.1 Generally: all sensitive personal data stored and/or handled by LMI must be securely protected against unauthorised use at all times. Any sensitive data that is no longer required for business reasons must be discarded in a secure and irrecoverable manner, for example, by cross cut shredding.

5.2 Bank Details: whenever data subjects provide their bank details to enable payments to be taken from or made to their accounts, this data shall only be held as long as is necessary to make the transaction(s) and to verify the transactions for the year end accounts. Such data shall be held securely and shall not be transferred to any electronic records with multiple staff access.

5.3 Debit and Credit Card Payments: where card payments are made in person, there is no need for the data subject to reveal their personal security information. Where card payments are taken over the telephone, the details may only be entered directly into the card machine and must not be written down or stored electronically. The merchant receipt is printed with the full digits of the card number and its expiry date: the payee's name and the reason for the payment are written on the receipt. The receipt must be recorded in the cash receipt book and the receipt filed without delay. The merchant receipts shall be held no longer than 18 months: this period allows for a transaction to be refunded, if necessary, and enables the verification of the transactions for the year end accounts.

6.0 Data Breaches

6.1 Examples of data breaches include:

- access to data by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

6.2 If there is any breach of the Act by staff/volunteers/Trustees, this must reported to the Data Protection Officer immediately. The Data Protection Officer shall

investigate the breach and report it to the Data Controller within eight hours. The Data Controller must assess the breach and report significant data breaches (where the severity of the breach results in risk to people's rights and freedoms) to the Information Controller's Office within 72 hours of the breach being identified. Failure to do this may result in a significant monetary fine.

6.3 All data breaches will be logged, detailing the breach, the steps taken to investigate the breach and the follow-up action.

6.4 Those whose personal data has been affected need to informed of the data breach in writing, describing, in clear and plain language, the nature of the personal data breach and, including:

- the name and contact details of the Data Protection Officer or other contact point where more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

6.5 All data breaches will be treated seriously by the Data Controller and may lead to disciplinary action up to and including dismissal or expulsion of staff, volunteers or Trustees.

Appendix A

Sample Privacy Notice

Here at Liverpool Medical Institution we take your privacy seriously and will only use your personal information to administer your account and to provide the services you have requested from us.

However, from time to time we would like to contact you with details of lectures, workshops and conferences you may be interested in. If you consent to us contacting you for this purpose, please tick the boxes below to say how you would like us to contact you:

- Post
- E-mail
- Telephone
- Text message

This consent will remain valid for up to three years from the date of signing unless you contact us in writing, by post or by e-mail, to the contrary.

We will not provide your details to any other companies or organisations.