Data Protection Policy

(updated August 2018)

INTRODUCTION

LMA keeps information about staff, learners and other parties to allow it to operate as a successful organisation and meet its legal obligations.

To comply with the Data Protection Act 1998, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles in the Act.

DATA PROTECTION PRINCIPLES

In summary, the Principles state that personal data will:

1. Be processed fairly and lawfully.

2. Be obtained for specified and lawful purposes, and will not be processed in a manner incompatible with those purposes.

3. Be adequate, relevant and not excessive for those purposes.

4. Be accurate and up to date.

5. Not be kept for longer than is necessary.

6. Be processed in accordance with the data subject's rights.

7. Be kept safe from unauthorised access, accidental loss or destruction.

8. Not be transferred to a country outside the EEC, unless the country has equivalent protection for personal data.

9. Comply with all aspects of GDPR

PERSONAL DATA AND PROCESSING

Personal data is information relating to a living person who can be identified from the information,

whether stored electronically or in paper-based filing systems or any other medium.

Processing, for the purpose of the Act, is accessing, altering, adding to, using, changing, disclosing or merging data.

REQUIREMENT TO COMPLY

Staff, learners or other parties who process personal data collected in the name of the College must ensure that they follow the above Principles.

Compliance with the Act is the responsibility of all staff and learners who access College systems. A breach of this policy may lead to disciplinary action and/or access to College facilities being withdrawn, or even criminal prosecution.

Questions about the interpretation or operation of this policy should be taken up with the College's designated Data Controllers.

Staff, learners or other parties who believe that the Policy has not been followed in respect of their own personal data should raise the matter with the designated Data Controller initially. If the matter is not resolved it should be raised as a formal complaint or grievance, in accordance with College procedures.

NOTIFICATION OF DATA HELD AND PROCESSED

Staff, learners and other persons about whom the College holds data are entitled to:

Know what information the College holds and processes about them and why.

Know how to gain access to it.

Know how to update it.

Know how the College complies with the Act.

The College will notify staff, learners and other relevant parties of the nature of data that the College holds and processes about them, and the reasons for which it is processed.

LMA will fully comply with Article 5 of the GDPR which requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. 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;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. 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;

e. 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; and
f. 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."

DATA CONTROLLER

The Data Controllers is the person or organisation responsible for ensuring that the requirements of the Act are complied with. LMA, as a corporate body, is the Data Controller under the Act, and the owners are therefore ultimately responsible for implementation of this policy and for compliance with the Act.

The designated Data Controller is the individual appointed by the College to carry out the day to day duties of the Data Controller.

The Data Controller will review the number and nature of requests for rights of access to data and queries raised in connection with this policy annually and, in the light of this review, will propose any necessary changes to this policy or related procedures.

RESPONSIBILITIES OF STAFF AND MANAGERS

Staff are responsible for:

Checking the information that they provide to the College in connection with their employment is accurate and up to date.

Informing the College of changes to information they have provided.

Checking information that the College sends to them, detailing data stored and processed about them.

Informing the College of errors or changes in information stored. The College cannot be responsible for un-notified errors.

If staff collect information about other parties, they must comply with the guidelines for staff, detailed in Appendix 1.

Managers have a responsibility to ensure that their staff are aware of, and comply with, Data Protection Principles.

LEARNER AND TUTOR OBLIGATIONS

Learners must ensure that their personal data provided to the College is accurate and up to date. They should notify changes of personal details to Student Services.

Learners who use College computer facilities may process personal data. If they do so, they must notify their tutor, who must notify the designated Data Controller. A learner who requires further clarification about this should contact the course tutor.

DATA SECURITY

Staff are responsible for ensuring that personal data that they hold on behalf of the College is (a) secure and (b) is not disclosed to an unauthorised third party.

Unauthorised disclosure will be a disciplinary matter, and may be considered gross misconduct.

Personal information should be physically secure and, if it is computerised, it should be password protected or kept only on disk that is stored securely.

RIGHTS TO ACCESS INFORMATION

Staff, learners and persons have the right to access their personal data that is stored by the College. Anyone who wishes to formally exercise this right must complete the "Access to information" form (Appendix 2) and give it to the designated Data Controller.

The College may make a charge of up to £10.00 on each occasion that formal access is requested, although the designated Data Controller has sole discretion to waive this charge, having regard to the circumstances and nature of the request. The charge is to cover administrative costs.

The College aims to comply with requests for access to personal information within 21 working days of the date of receipt of the request by the designated Data Controller. If this timescale cannot be met, the reason for delay will be explained in writing to the person making the request.

PUBLICATION OF INFORMATION

Information already in the public domain is exempt from the Act. The College makes public information concerning its governance, annual accounts, rules, charters, significant policies and media releases, except for confidential matters and personal data, unless consent has been obtained.

Any individual who has good reason for wishing their personal data to remain confidential should contact the designated Data Controller.

DATA SUBJECT CONSENT

In many cases, the College can only process personal data with the consent of the individual concerned. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the College processing specified classes of personal data is a condition of acceptance of a learner onto a course and a condition of employment for staff. This includes information about previous criminal convictions.

The College has a legal obligation to ensure that staff are suitable for the duties and responsibilities of their role, and learners for the course offered. The College also has a duty of care to all staff and learners and must therefore make sure that employees and those who use College facilities do not pose a threat or danger to themselves or others.

The College also asks for certain information about the health of staff and learners, which it will only use in connection with the health and safety of the individual and others, but needs consent to process.

PROCESSING SENSITIVE INFORMATION

It is sometimes necessary to process sensitive information, such as about a person's health, criminal convictions, race, gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College procedures, such as for sick pay or equal opportunities. Because this information is sensitive, and it is recognised that processing may cause concern, staff and learners are asked to give express consent for the College to do this. Offers of employment or course places may be withdrawn if consent is withheld without good reason. More information about this is available from the designated Data Controller.

EXAMINATION RESULTS

Learners are entitled to information about their results for coursework and examinations. However, this may take longer than other information to provide, if third parties such as examining bodies have to be contacted.

RETENTION OF DATA

The College keeps some types of information for longer than others. Information about learners cannot be kept indefinitely. Generally, key information about learners that could be subject to audit may be kept for up to seven years but other information will be destroyed within three years after the learner leaves the College.

The College needs to retain information about staff, generally for two years after staff leave the College. Some information will be kept longer, including information for pensions, taxation or for legal or audit reasons.

A list of information with retention times is available from the designated Data Controller.

STAFF GUIDELINES FOR DATA PROTECTION

1. Most staff process data about learners, e.g. when marking registers, or College work, writing reports or references, or as part of pastoral or academic supervisory roles. The College will ensure that all learners give their consent to this sort of processing, and are notified of the categories of processing, as required by the Act. This information that staff deal with on a day-to-day basis will be "standard" and covers categories such as: General personal details e.g. name and address. Details about class attendance, coursework marks, grades and associated comments. Notes of personal supervision, including matters about behaviour and discipline.

2. Information about a learner's physical or mental health, sexual life, political or religious views, trade union membership, ethnicity or race is sensitive and can only be collected and processed with the learner's consent. If staff need to record this information, they should use the College's standard form for this.

3. All staff have a duty to make sure they comply with the Data Protection Principles in the Data

Protection Policy. In particular, staff must ensure that records are:

Accurate

Up-to-date

Fair

Stored and disposed of securely, and in accordance with College policy.

4. Staff must not disclose personal data to any learner or third party, other than the person whom the data is about, unless for normal academic or pastoral purposes, in accordance with College policy, or as required by law.

5. Staff should not disclose personal data about other staff except in accordance with College policy or if the requesting employee needs the information to perform their duties. Seek advice from Personnel Department if you are asked to provide a reference.

6. Personal data must not be given to someone you do not know unless you can confirm the identity of the person requesting the information and satisfy yourself that you can legally comply with the request. Particular care should be taken with telephone requests and alleged relatives of learners and staff. Refer all difficult situations to the designated Data Controller.

7. Police or similar legal requests for disclosure of personal data should be referred to the designated Data Controller. If the officer will not wait because the matter is urgent, the officer must issue a DP1 form. This will detail the required information and must be signed by a Superintendent. You should make a note the officer's identification number, the information released and the date and time.

8. Personal data collected for a specified purpose should not be used for another purpose (e.g. unsolicited direct marketing.

9. Particular care should be taken with the use of E-mail or fax to transmit personal data. You will need to be certain that it has only been sent to the intended recipient. If you are the recipient, you will need to ensure that the data is retained for the appropriate length of time, remains accurate and can be retrieved when required.

10. Staff have screen-based access through the Corporate Intranet to a considerable amount of personal data that is held within the College's central Information Systems. Paper-based reports are also produced from these Information Systems. Users should ensure that only authorised persons are able to see this information.

10. Before processing personal data, consider the following checklist:

Do you really need to record the information?

Is the information “standard” or “sensitive”?

If it is sensitive, has the data subject’s express permission been obtained?

Does the data subject know why this data will be processed?

Has the data subject confirmed that the data is accurate?

11. When you process data, simple security measures are:

File personal data away from sight of unauthorised persons.

Lock personal data away and/or lock the room if it is being left empty.

Do not leave personal data (paper based or on other media such as USB sticks) in bags or cases in situations where it may be mislaid, damaged or stolen. If possible, avoid taking such information off site.

Seal personal data transmitted by post (internal as well as external) in envelopes or packages.

Ensure your computer password is secure and not disclosed to anyone else.

Log out before you leave your computer unattended.

Position computer screens away from unauthorised view.

Set your computer screen saver to come on after a short interval.

Have back-ups for personal data stored on computer.

Ensure that personal data being disposed of cannot fall into the wrong hands before it is finally destroyed. Shredding is more secure.

12. Use of USB and other storage devices: Corporate data should not be copied onto any USB or storage device (including laptops) without permission from a designated Data Controller.

All such data should be in password protected files and wherever possible should be encrypted.

All such data (even part of) should not be passed onto third parties without the consent of a designated Data Controller.

Data should not be kept on storage devices longer than is necessary and permanently removed/deleted at the earliest possible opportunity.