

Data Protection Policy

0151 709 4640
www.modetraining.co.uk



Copies of all MTL policy and procedures may be obtained in large print please call 0151 709 4640 for a copy or alternatively e mail admin@modetraining.co.uk

to be read and understood by:

Staff, Students, Employers, Work experience Providers, School Mentors and all relevant partners

Introduction

A Statement of Intent

Mode Training adheres to General Data Protection Regulation (GDPR) EU directive 2018 and Data Protection Act 2018 (Royal Assent 23/05/2018 in preparation for UK leaving EU). GDPR builds on the principles and the themes of the DPA and establishes a framework of duties for Mode Training and rights for individuals, that aim to keep personal information safe. GDPR encourages a balance between the individual's right to privacy and an organisation's need to conduct legitimate and appropriate operations with personal data.

This Policy sets out the obligations of MTL with regard to data protection, and the rights under the DPA/GDPR ("the Act") of people whose personal data are held and processed by MTL. It sets out the procedures to be followed by MTL, its employees, contractors, agents, consultants, partners or other parties working on its behalf, when dealing with personal data.

It is the personal responsibility of all employees (temporary or permanent) contractors, sub contractors, partners, agents, volunteers and anyone else processing information on our behalf to comply with this policy. MTL are fully committed to protecting the privacy of individuals and handles all information in a compliant manner .

Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990, GDPR or the Data Protection Bill. All incidents will be investigated and action may be taken under MTL formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and / or criminal action being taken

In this policy, MTL is the "Data Controller" and its employees, learners, employers, customers, suppliers, contractors and other business contacts are the "Data Subjects".

Every organisation that processes holds and uses information must be registered with Information Commissioner's Office (ICO). MTL registration number is **ZA126347** MTL must comply with seven data protection principles. This Policy aims to ensure compliance with DPA and GDPR. These principles lie at the heart of MTL approach to processing personal data.

Data Protection Principles

GDPR seven key principles

Concerned with the use (processing) of personal data

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Rights of Data Subjects

Under legislation data subjects have the following rights:

- The right to be informed that their personal data is being processed
- The right to access any of their personal data held by MTL (no charge can be made for access request and MTL have one month to process the request)
- The right for individuals to have inaccurate personal data rectified or completed if incomplete
- The right to have personal data erased
- The right to prevent the processing of their personal data in limited circumstances
- The absolute right to stop their data being used for direct marketing

Personal Data

Personal data is defined as data which relates to a living individual who can be identified from that data, or from that data in conjunction with other information which is in the possession of, or is likely to come into the possession of, the data controller. It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Examples of personal data include: names, addresses, dates of birth, photographs, IP addresses, vehicle registration plates and CCTV footage.

The Act further defines “**sensitive personal data**” as personal data relating to:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious (or similar) beliefs
- Trade union membership
- Their physical or mental health condition
- Their sexual life
- The commission or alleged commission by them of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the

sentence of any court in such proceedings.

The data subject must give explicit consent to the collection, storage and processing of sensitive personal data.

MTL only holds personal data which is directly relevant to its employees, learners, customers, contractors, sub-contractors and client contacts. That data will be held and processed in accordance with the data protection principles and with this policy. The following data may be collected, held and processed by MTL:

- Identification information relating to employees and learners including, but not limited to, names and contact details, both personal and organisational
- Equal opportunities monitoring information including age, gender, race, nationality and religion
- Health records including details of sick leave, medical conditions, disabilities and prescribed medication
- Safeguarding records including EHCP plans, case conference notes, social worker reports
- Employment records including, but not limited to, interview notes, CVs, references from previous employers, application forms, assessments including psychometric assessments, performance reviews and similar documents
- Details of salaries including increases, bonuses, commission, overtime, benefits and expenses, whether within MTL or in previous employments, as appropriate
- Records of disciplinary matters including reports and warnings, both formal and informal
- Details of grievances including documentary evidence, notes from interviews, procedures followed and outcomes.

When MTL collects personal information from an individual, we must inform them of what we intend to do with that information once we have it. This is called a **Privacy Notice**. All learners funded will also be issued with funded body (ESFA) privacy notice.

The Privacy Notice must include the following information: -

- Who will own the data – normally MTL
- What the information will be used for
- The legal basis for collecting and using the information
- Who the information will be shared with
- How long the information must be kept for and how it will be stored
- What Rights under GDPR that the data subject has
- How they can complain
- How they can complain to the Information Commissioner's Office
- Whether the data is stored outside of the UK
- Whether any automated decisions are made using the information

Privacy Notice must be given to the data subject as soon as possible when collecting their information and this can be done online, through the post or in the form of a recorded voice message. As long as the Privacy Notice is provided, it can take any form.

Health Records

MTL holds health records on all employees, which are used to assess the health, wellbeing and welfare of employees and highlight any issues which may require further investigation. Such health records will include details of sick leave, medical conditions, disabilities and prescribed medication. Data under this heading will be used by management only and will not be revealed to fellow employees (unless those employees are responsible for health records in the normal course of their duties).

Employees have the right to request MTL does not keep health records on them. All such requests must be made in writing and addressed to the Company Director.

Benefits

In cases where employees are enrolled in benefit schemes which are provided by MTL (including, but not limited to, pensions and healthcare) it may be necessary from time to time for third party organisations to collect personal data from relevant employees.

Prior to collection, employees will be fully informed of the personal data that is to be collected, the reasons for its collection, and the way(s) in which it will be processed. MTL shall not use any such data except insofar as is necessary in the administration of relevant benefits schemes.

Monitoring

MTL may from time to time monitor the activities of employees for specific, legal or organisational purposes. Such monitoring may include, but will not necessarily be limited to, internet and email monitoring. MTL shall use reasonable endeavours to ensure that there is no intrusion upon employees' personal communications or activities. Any employee that is to be monitored shall be informed in advance of such monitoring. Monitoring shall not interfere with an employee's normal duties.

Processing Personal Data

All personal data collected and processed by MTL is collected for the purposes of efficiently managing its employees and business databases, and to conform with its equal opportunities obligations. Personal data shall also be used by MTL in meeting any relevant obligations imposed by law.

Personal data may be disclosed within MTL. Personal data may be passed between employees in accordance with the data protection principles and this policy, as long as it is reasonably required by those employees for legitimate purposes.

MTL shall ensure that:

- All personal data is collected and processed fairly and lawfully
- Data subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s)

- All personal data is accurate at the time of collection and kept accurate and up-to-date while it is being held and/or processed
- No personal data is held for any longer than necessary in light of the stated purpose(s)
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data
- All personal data is transferred using secure means, electronically or otherwise
- No personal data is transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory
- All data subjects may exercise their rights set out above in Section 3.

Disclosing personal information

- Personal information must only be shared when the member of staff receiving the request is satisfied as to the legal basis for sharing the information. Staff must ask appropriate questions to ensure the requester (whether internal or external) has the appropriate legal reason to see the information they are requesting. If in doubt speak to your manager or DPO
- If personal information is given to another organisation the disclosing person must identify their lawful basis for the disclosure and record their decision for sharing along with the written request for information. Which should include:
 - A description of information provided
 - The name of the person and organisation the information was given to
 - The date
 - The reason for the information given
 - The lawful basis

If there is an Information Sharing Agreement in place (ISA) this should be adhered to. All information shared should be via Egress.

Lawful

To use information lawfully MTL must ensure no laws are broken when processing data, MTL must also meet a condition for processing. MTL can use information if one of the following applies:

- The data subject has consented to their information being used
- The personal data is being used to perform a contract with the data subject or undertaking actions necessary to create a contract with the data subject
- The personal data has to be processed due to legislation e.g court order
- The personal data is used in line with vital interests of data subject (safeguarding)

To use sensitive data as above MTL are required to meet one of the above conditions and one below:

- Explicit consent has been granted from the data subject
- The processing is necessary for MTL obligations of employment law or social security

Once MTL have collected information for a specific purpose we can only use that information for purposes compatible with the original aim.

Data Protection Procedures

MTL shall ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of MTL comply with the following when processing and / or transmitting personal data:

- Technical and organisational measures ensuring information is secure and prevented from being lost or put at risk of being seen by people who should not have access to it. This can take a variety of forms such as
 - Firewalls
 - Anti virus software
 - Secure e mails – Egress
 - User guides for staff
 - Staff training
 - Open honest culture towards data protection
- Personal data may be transmitted over secure networks only, names should be anonymized – Mode use Egress to transfer e mails and files other than data files which are shared via “The Hub” a secure ESFA portal
- Emails containing personal data shall be stored securely
- Where personal data is to be transferred in hard copy form it shall be passed directly to the recipient or posted marked “Confidential for the addressee only” via by recorded delivery
- All hard copies of personal data shall be stored securely in a locked box, drawer, cabinet or similar
- All electronic copies of personal data shall be stored securely and be password protected

Individual rights

Individuals have a number of Rights under GDPR and DPA they are able to enact them against any organisation at a time they choose.

The Rights include: -

- **The Right of Subject Access** – the right to request a copy of data held about them by an organisation and find out how it is used
- **The Right of Rectification** – the right to ask for inaccurate or incorrect information to be corrected or removed
- **The Right of Data Portability** – the right to move data from one organisation to another. This could apply when moving bank accounts or energy suppliers
- **The Right to Be Forgotten (Erasure)** – the right to ask for data to be removed by the organisation that holds it
- **The Right of Restriction** – the right to stop information being used whilst a complaint is made
- **The Right of Objection** – the right to ask an organisation to stop using their data. This is particularly used with regards to direct marketing

MTL has 30 days (one month) to respond to an individual’s request to enact their Rights. This is provided the applicant has put their request in writing and suitable identification has been supplied.

A request for information should be put in writing to the

**Data Protection Officer
Mode Training Limited
The Secret Warehouse
Syren Street Liverpool
L20 8HN**

or alternatively

E mail to admin@modetraining.co.uk with Subject Access Request in the subject header

The following information will be provided to the data subject:

- Whether or not MTL holds any personal data about the person
- A description of any personal data held about the person
- Details of what that personal data is used for
- Details of any third-party organisations that personal data is passed to
- Details of any technical terminology used.

Employee Records and Retention

MTL shall retain all employee records following the end of employment for the following periods:

- Personnel and Payroll records 3 years
- Pension records 6 years

Learner records and retention

- Learner records As determined by funding bodies
- Portfolios and certificates As determined by awarding bodies

Further information listed in MTL retention schedule

Notification to the Information Commissioner's Office

As a data controller, MTL is required to notify the Information Commissioner's Office that it is processing personal data. MTL is registered in the register of data controllers.

Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

Organisational Measures

Overall responsibility for overseeing data protection and ensuring compliance rests with the Company Director.

Company Director shall ensure that:

- ICO are provided with the necessary documentation relating to data protection at MTL on an annual basis
- A suitably experienced DPO Data Protection Officer is appointed
- DPO is given training to exercise their duties effectively
- Resources are made available complying with all relevant legislation including Data Protection Act (DPA) 2018 and General Data Protection Regulation (GDPR) 2018

Data Protection Officer shall:

- Inform and advise MTL and their employees regarding their obligations to comply with ALL data legislation
- Monitor MTL compliance with legislation including managing internal data protection activities, advise on data protection impact assessments, conduct internal audits and provide staff training
- Review this policy on an annual basis in conjunction with the Director
- Encourage good information handling practice across the whole organisation
- Act as contact for ICO and individuals whose data MTL process
- Ensure all employees, contractors, agents, consultants, partners or other parties working on behalf of MTL are made fully aware of both their individual rights and responsibilities and MTL's responsibilities under legislation, and are given a copy of this Policy
- Ensure all employees, contractors, agents, consultants, partners or other parties working on behalf of MTL handling personal data are given training and guidance to ensure their understanding of this policy
- Ensure all employees, contractors, agents, consultants, partners or other parties working on behalf of MTL handling personal data are appropriately supervised
- Ensure methods of collecting, holding and processing personal data are regularly reviewed
- Ensure all personal data are kept up-to-date
- Ensure all personal data which is out-of-date or no longer required is deleted or confidentially destroyed
- Ensure performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of MTL handling personal data is regularly reviewed
- Report any breaches of data handling to ICO in a timely manner

All MTL Staff shall:

- When processing personal data regarding learners, colleagues and/or contractors/employers comply with data protection principles
- Inform the Director if their personal data changes (e.g. change of address or marital status)
- Ensure as far as is possible all personal data received and processed is accurate and up to date. Personal information held should be checked at regular intervals it is up to date and accurate. If information held is incorrect it should be updated on all systems as soon as is practical

- When inputting data or updating information ensure it is adequate, relevant, clear and professionally worded
- When responsible for the security of data they process ensure it is not disclosed to anyone who does not have the relevant authorisation to gain such information
- Ensure all equipment including iPads, Laptops, USB are handled securely
- Staff are also data subjects. They should ensure that any information they supply to MTL in connection with their employment is accurate and up to date. MTL cannot be held responsible for errors from changes about which they have not been informed
- Follow the principles set out in MTL Data Protection Staff Guide

Non Compliance

- Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence
- Failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Policy shall constitute a breach of contract
- In all cases, failure to comply with the principles or this Policy may also constitute a criminal offence under the Act
- All contractors, agents, consultants, partners or other parties working on behalf of MTL handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of MTL arising out of this Policy and the Act
- Where any contractor, agent, consultant, partner or other party working on behalf of MTL handling personal data fails in their obligations under this policy that party shall indemnify MTL against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Review of policy and procedures

This policy will be reviewed by Debbie Tagoe – Company Director in conjunction with Amanda Clarke named Data Protection Officer annually, sooner if advised by ICO or change of law

Signatures

This policy was produced by Debbie Tagoe and Amanda Clarke on behalf of Mode Training Limited.

Debbie Tagoe
Signature

Amanda Clarke
Signature