Apprenticeship Policy

Data Protection Policy

MTD Training

INTRODUCTION

MTD hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes. This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work.

In particular, this policy requires staff to ensure that the Lead Compliance and Policy Officer (LCPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

DEFINITIONS

BUSINESS PURPOSES

The purposes for which personal data may be used by us:

Personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice. For example, our obligations for processing data in relation to staff pension schemes.
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests.
- Ensuring business policies are adhered to (such as policies covering email and internet use). For example, the use of privacy notices and email disclaimers to all.
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting.
- Investigating complaints.
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Improving services

PERSONAL DATA

Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.

Personal data we gather on learners may include:

- Personal details: this includes name, date of birth, address, qualifications, next of kin (and places of work, if relevant), telephone numbers plus a photograph.
- Details concerning health – for instance whether they are diabetic, suffer from asthma etc.
- Details of any disabilities which might have an impact on your academic study e.g. dyslexia.
- Details about academic performance, expected and actual results, references and attendance.
- A copy of the learner contract
- Copies of any other related agreements – e.g. use of IT, permission to use photographic images.
- Details of any change of course taken.
- Details of any certificates/assessments held concerning academic progress, e.g. reports, referrals.

- Personal details required for examination entries and any other communications with examination boards.
- Details of any disciplinary meetings held with members of staff.

The following information is held by MTD on staff:

- Personal details: name, address, date of birth, qualifications, next of kin.
- Details of physical and/or mental health: details about specific conditions individuals may suffer from, such as asthma or diabetes.
- Information about sickness absences and any medical reports we may have received.
- Details about work performance, including notes of observation sessions, appraisals, and staff development.
- Personal information: details about start date, pension and pay details, any current disciplinary or grievance matters, any deductions from salary or any loans.
- Details about any criminal record.
- References produced by MTD.

SENSITIVE PERSONAL DATA

Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

In this document the phrase 'data processing' means almost anything to do with information accordance with the Data Protection Act 2018, MTD ensures that personal information stored by the organisation is fairly and lawfully processed.

SCOPE

This policy applies to all staff who must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Staff will be notified of changes.

THE DATA PROTECTION PRINCIPLES

MTD sets this policy in the spirit of the Data Protection Principles; set out by legislation and expressed below:

1. Data must be processed fairly and lawfully.
2. Data should be obtained only for one or more specified and lawful purposes
3. Personal data held shall be adequate, relevant, and not excessive.
4. Data should be accurate and up to date.
5. Data should be held no longer than for the purpose it was originally collected.
6. Data should be processed in accordance with the data subject's rights under the Act.
7. Data should be secured.
8. Data should only be transferred to other countries if they have suitable or equivalent security measures.

MTD ensures that we process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

WHO IS RESPONSIBLE FOR THIS POLICY?

The Lead Compliance and Policy Officer (LCPO) is responsible for the processing of data. The LCPO must ensure that data processing complies with the Data Protection Act, determine the purposes for which the data will be used and oversee the implementation of this policy.

THE LEAD COMPLIANCE AND POLICY OFFICER'S RESPONSIBILITIES:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and advice for all staff members and those included in this policy.
- Answering questions on data protection from staff, board members and other stakeholders.
- Responding to individuals, such as Parents/Guardians, Learners and employees who wish to know which data is being held on them by the MTD .
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.

RESPONSIBILITIES OF THE IT MANAGER:

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Researching third-party services, such as cloud services the company is considering using to store or process data.

RESPONSIBILITIES OF THE MARKETING MANAGER:

- Approving data protection statements attached to emails and other marketing copy.
- Addressing data protection queries from learners, employers, prospective employees, target audiences or media outlets.
- Coordinating with the LCPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.

MTD PROCEDURE

THE PROCESSING OF ALL DATA:

MTD shall always have a legitimate reason for the collecting and storing of data and will always ensure that the processing of data has no adverse effect on any individual. It will be transparent in processing data and where appropriate inform individuals through a 'privacy notice' that their personal information is being processed.

The processing of all data must be:

- Necessary to deliver our services.
- In our legitimate interests and not unduly prejudice the individual's privacy.
- In most cases this provision will apply to routine company data processing activities.

PRIVACY NOTICE

MTD 's terms of business contains a Privacy Notice to learners, staff, contractors and all other individuals dealing with the company on data protection.

The notice:

- Sets out the purposes for which we hold personal data on learners and employees
- Highlights that our work may require us to give information to third parties such as professional advisers and external agencies.
- Provides that learners have a right of access to the personal data that we hold about them.

The privacy notice can be found on MTD 's website.

SENSITIVE PERSONAL DATA

In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work/ Safeguarding etc). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Sometimes it is necessary to process information about a person's criminal convictions, race and gender and family details. This may be to ensure that MTD is a safe place for everyone, or to operate other policies, such as the Equality and Diversity Policy and Safeguarding.

MTD will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes or disabilities. The MTD will only use the information for the protection of the health and safety of the individual, but will need consent to process this information, for example in the event of a medical emergency. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and learners will be asked to give express consent for the MTD to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this without good reason.

CONDITIONS FOR PROCESSING PERSONAL DATA

Before data may be processed one of the following conditions must be met:

1. the individual (data subject) has given their consent
2. the processing is necessary in relation to a contract
3. the processing is necessary because of a legal obligation
4. the processing is necessary to protect the individual's vital interests
5. the processing is necessary for the administration of justice or other statutory functions
6. any other legitimate interest

CONDITIONS FOR PROCESSING SENSITIVE PERSONAL DATA

Because such information might be used in a discriminatory way, these are more stringent and must include one of the following conditions:

1. the individual has given consent
2. the processing is required by employment law
3. the processing is necessary to protect the vital interests of the individual or third part
4. the individual has made the information public
5. the processing is necessary for statutory reasons
6. the processing is carried out with a third party who is bound by a professional code of conduct (a doctor for example)
7. the processing is required to monitor equal opportunities
8. the processing is necessary to prevent crime or protect the public.

EXEMPTIONS

Generally all personal data collected and processed will be subject to the Data Protection Act. However, some exemptions may apply. For example, MTD on occasions will ask for references (a confidential reference given by the MTD to a third party regarding education, employment/training, appointment to a public office, a service being provided by the data subject etc) that will remain confidential and are exempt from the requirements of the Act. References we have received and kept on file are not exempt. We must, however, ensure that the rights of the referee are considered. Information about the individual referee should not be disclosed without explicit consent (anonymising the information is acceptable).

MTD cannot refuse to disclose confidential references without providing reasons. Crime and taxation – personal data may have to be disclosed to government departments or the Police. Data will only be released on the basis of properly drawn up requests. Vital interests – personal data may be released if it is in the vital interests of the individual e.g. a medical emergency. Under 19 learners – the MTD will normally release information about a learner's progress and attendance to parents or guardians of learners under 19 years of age on the previous 31st August**.**

ACCURACY AND RELEVANCE

MTD will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the LCPO.

YOUR PERSONAL DATA

Employees and learners must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the LCPO so that they can update your records. Examples of the type of data MTD may process are set out above in the section titled 'Definitions, Personal Data'.

DATA SECURITY

All members of the MTD community must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the LCPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations. For example, payment of pensions and salaries are outsourced to third parties.

STORING DATA SECURELY

In cases when data is stored on printed paper, it is kept in a secure place where unauthorised personnel cannot access it. Printed data is shredded when it is no longer needed. Data stored on a computer is protected by strong passwords that are changed regularly. All staff and learners use a password manager to create and store their passwords.

Data stored on CDs or memory sticks must be locked away securely when they are not being used. The LCPO must approve any cloud used to store data.

Servers containing personal data must be kept in a secure location, away from general office space. Data should be regularly backed up in line with MTD 's backup procedures. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
All servers containing sensitive data must be approved and protected by security software and strong firewall. We store all sensitive personal information securely either in locked filing cabinets or in computer files which are password protected.

Our computer network system is protected by a robust firewall which is monitored by both our premises manager as well as an external supplier, BTA.

All admin and teaching staff are trained about the proper use of personal data. For example, they only communicate with clients and persons related to clients through authorised channels. They must properly annotate and store all such communication. They must report all breaches of data security to the LCPO. They are aware that they may be subject to criminal proceedings should they deliberately try to access or disclose without authority. They are aware of the threat posed by 'phishing' emails and hackers.
Although rarely used we ensure that fax transmissions of sensitive data are double checked to ensure the correct telephone number. We should ensure that we are confident of the receiver's identity and that the receiver is standing by their fax machine.

Before we dispose of any computer equipment we ensure that there is no data stored within the equipment.

The MTD is committed to keeping our security systems and security software systems up-to-date and has suffered no major incidents at the time of writing this policy.

All staff are aware of the importance of checking credentials.

The premises manager is responsible for maintaining security of access, maintaining security of data and physical protection of data on our premises.

This includes:

- The proper training of all staff about authorised entry to the building
- Maintenance of our keypad security entry systems
- The proper admission procedure for all guests to the MTD
- The maintenance of our CCTV system
- Fire Safety

BREACHES OF SECURITY

MTD takes breaches of security seriously. Examples of potential breaches of security can be caused by a number of factors. Some examples are:

- Loss or theft of pupil, staff data and/ or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment Failure
- Human Error
- Unforeseen circumstances such as fire or flood
- Hacking
- 'Blagging' offences where information is obtained by deception.

MTD aims to carry out the following procedure to mitigate such circumstances:

a. have a data recovery plan
b. proper assessment of risks
c. notify all related parties such as the ICO, relevant data subjects, the police, banks
d. institute a proper procedure of evaluation and response
e. protocol in relation to breach of security is regularly updated.
f. the computer databases are password-protected.

DATA RETENTION

MTD retains personal data for no longer than is necessary for the purpose for which it was collected. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

SUBJECT ACCESS REQUESTS

MTD is aware under the Data Protection Act 2018, individuals are entitled, subject to certain exceptions, to request access to information held about them. Staff who receive a subject access request should refer that request immediately to the LCPO whom may ask you to help us comply with those requests. Staff and Learners may contact the LCPO if they would like to correct or request information that MTD hold about them. There are also restrictions on the information to which individuals are entitled under applicable law.

PROCESSING DATA IN ACCORDANCE WITH THE INDIVIDUAL'S RIGHTS

Information must be processed consistent with the rights of individuals with regard to processing personal data. These rights include:

a. A right to a copy of all processed information; in this case the individual will make a 'subject access request'. We understand that information about our learners belongs to them so any request for information by a related third party may only be granted with the consent of the learner.

This provision is subject to:

- The learner's maturity
- The nature of the personal data
- Any court orders
- The consequences of disclosing the information especially in cases of suspected abuse
- Any detriment to the learner should the third party not have access to the information
- The views of the learner.

A request for information which involves others may be declined unless we have the other's consent.

b. A right to object to the processing of information. Any such objection must be provided in proper written form and, depending on circumstances defined by the Act, may not always be granted**.**

c. In certain circumstances a right to have inaccurate information rectified, blocked, erased or destroyed.

d. Right to claim compensation.

e. A right not to participate in any direct marketing.

f. Secure.

MARKETING

MTD will not send direct marketing material to someone electronically (e.g. via email) unless we have an existing business relationship with them in relation to the services being marketed or an understanding that parties have given consent. All members of the MTD community will contact the LCPO for advice on direct marketing before starting any new direct marketing activity.

TRAINING

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis. It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

It is our policy to develop an understanding of the rights of individuals under the Data Protection Act through internal programmes as well as with training of all teachers and admin staff. Topics would include: What is personal data? How may personal data be used? How should you keep personal data safe? What rights do you have with regard to processing personal data?

MONITORING

All Learners and staff must observe this policy. The LCPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

All staff and learners are responsible for the following:

- Checking that any information that they provide to the MTD in connection with their employment is accurate and up to date informing the MTD of any changes to or errors in information, which they have provided, i.e. changes of address.
- They must ensure that changes of address, etc are notified to the admin staff. The MTD cannot be held responsible for any such errors unless the staff member or student has informed the MTD of them.
- If and when, as part of their responsibilities, staff collect information about other people, for example, about learners' coursework, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with this policy.

CONSEQUENCES OF FAILING TO COMPLY

MTD takes compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.