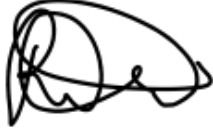




Multi Trades Training

Data Protection Policy

Review Date: July 2024

Approved by	RK Jones	Position	Director
		Date	12th June 2022

Document Control

Date	Review & Revision	By
07.06.23	Inclusion of MTTs Data Breach Policy V(1) Jan 23	Quality Lead

Scope

Mult Trades Training (MTT), the company, is committed to comply with the General Data Protection Regulation (GDPR) which forms part of the Data Protection regime in the U.K. together with the Data Protection Act 2018 (DPA 2018) and the main provisions that apply.

Introduction

This Policy sets out the obligations of Multi Trades Training (MTT) a company registered in UK under number 11553273, whose registered office is at : Shalford Dairy, Wasing Estate, Aldermaston, Berkshire, RG7 4NB regarding data protection and the rights of business contacts and learners in respect of their personal data under The Data Protection Act 1998 (DPA) was introduced to establish a framework for the protection of personal or sensitive data and is underpinned by a set of eight principles, and the EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

This Policy sets the obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by MTT, its employees, agents, contractors, or other parties working on behalf of MTT.

Definition of data

Data refers to information about an individual (referred to as the ‘data subject’) that may be used or processed by MTT (referred to as the ‘data controller’) in order to carry out the training, assessment and certification function. There are two categories:

Personal data

This is information which relates to a data subject who is able to be identified from data or from data with other information, which is already in possession, or likely to come into possession of, the data controller. Facts and opinions about the data subject which can be held electronically or on paper may also be considered as personal data.

Sensitive personal data

This is information about a data subject relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sex life, the commission or alleged commission of any offence, criminal proceedings or convictions.

The Data Protection Principles

This Policy aims to ensure compliance with the DPA and the GDPR by following principles with which any party handling personal data must comply. All personal data must be:

1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
6. 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.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.

Special Category Data such as race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, or sexual orientation data, is only requested where the law allows it and processed in accordance with the data principles. Criminal Offence Data (convictions and offences) is only processed with explicit consent of the data subjects and where we have a lawful basis to do so under Article 6 and Article 10.

Retention of Personal data will be retained for no longer than is necessary for the purpose for which it was collected. Standard retention times are necessary to meet various contractual requirements.

Complying with the data protection principles

To meet the legal obligations of the DPA and the GDPR, MTT follows the Data Protection Policy that NCON has in place to ensure the security of data for all individuals engaged with the delivery, assessment and award of NCON Apprenticeships and qualifications.

[https://www.nocn.org.uk/Data/Support_Downloads/EPADDataProtection\(EPA\).pdf?date=30/06/2022%2013:30:48](https://www.nocn.org.uk/Data/Support_Downloads/EPADDataProtection(EPA).pdf?date=30/06/2022%2013:30:48)

- All members of MTT staff, consultants, advisors, learners and volunteers have access to a copy of this policy, and the policy of NCON.
- All forms which require the collection of sensitive or personal data include a data protection statement to inform the data subject of how their data will be processed
- No data is used for the purposes of marketing, unless the data subject provides written content to confirm that this is acceptable

- No personal data is disclosed, written or verbal, to anybody outside MTT unless written consent from the data subject is provided to confirm that this is acceptable
- Only nominated members of MTT have access to personal data and process this information in accordance with the requirements of the training, assessing and certification function
- All records are electronically stored, with appropriate protection in place to prevent unauthorised access from non-MTT members of staff
- Access to any external database, for example BSKB, is restricted with password protection and access rights made available to nominated members of MTT, with passwords reset regularly
- Learner achievement data will be uploaded to the personal learning record if the data subject has indicated that this is acceptable and a unique learner number has been provided to NCON.
- Access to view information contained within the personal learning record is limited to authorised users, of which they have been vetted prior to authorisation
- Learner achievement data is not used for any other purpose other than those permitted in this policy, including marketing or financial gain
- All records are kept accurate and up to date as far as practicable; NCON relies on the data subject to communicate any changes to personal data as and when applicable
- Should MTT at any point send an email to multiple individuals, those individuals will be blind copied into the correspondence.

How we use your information

Personal data collected will solely serve the purpose of enabling MTT to carry out the requested activity. By submitting information to us, you are authorising MTT to process your data accordingly. Should contact information be provided, you consent to receiving information relating to the requested activity by email, post or telephone unless stated otherwise.

Security of data

MTT has in place appropriate measures to ensure the safety of stored data to prevent unauthorised use or disclosure. In the event of a breach of security (i.e. theft, deliberate attack on systems, unauthorised use of personal data by a member of staff, accidental loss or equipment failure), a recovery plan will be implemented. This will include procedures for assessing the risk associated with the breach, reviewing and updating security measures and notifying those individuals affected.

The Rights of Data Subjects

The DPA and the GDPR sets out the following rights applicable to data subjects

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the 'right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object
- Rights with respect to automated decision-making and profiling

Retention of Records

Learner Data: 5 Years. Registration details including:

This information may include:

- Date learners started their qualification (e.g. course / cohort start date)
- Learner name, ULN (where applicable) and date of birth
- Learner contact details
- Evidence of Learner eligibility
- Evidence of Learner pre-requisites (if applicable)
- Date Learners were registered with NOCN or other awarding organisations
- Date certificates were claimed by MTT
- Learner Outcomes

Staff/ Workforce Data -5 Years following learner registrations

This information may include:

- Name of all individuals involved in the teaching, learning, assessment and internal verification of the Learners
- Role they undertook (e.g. Coach, Tutor and / or Assessor or IV)
- Evidence of any appropriate / required qualifications
- Evidence of any appropriate licenses or professional memberships

Learner Samples

- A minimum sample of one complete Learner portfolio for each standard MTT delivers each year. The portfolio be in a digital format.

Assessment Evidence

Must be retained and made available to NOCN or the Regulators for up to one year following registration.

This information may include:

- A copy of the Assessment Task versions used (including references to how they are mapped to Learning Outcomes / Assessment Criteria)
- Summary of assessment decisions to include formative and summative decisions and when and by whom the decisions were made

Learner Portfolios

Learner work is the property of the Learner and therefore cannot be retained indefinitely.

However, access may be required by the MTT, NOCN and / or our Regulators (ESFA or Ofsted) for purposes of appeal, audit or on-going monitoring.

Internal Quality Assurance Records

- Must be retained and made available to NOCN and / or the Regulators for up to one year following registration.

This information may include:

- Internal Verification / Quality Assurance Sampling Plans
- Internal Verification sign-off of Assessment Tasks (if applicable)
- Internal Verification reports
- Standardisation activities

Data Breach

Employees are responsible for keeping personal information secure to prevent a data breach.

‘A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data’.

Personal Data Breach includes:

- access 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

Reporting a Data Breach

A notifiable Data breach must be reported to The Data Protection Officer immediately. The Data Protection Officer will investigate the breach and report the matter to the relevant supervisory authority within 72 hours of becoming aware of it.

This policy does not form part of the formal Contract of Employment, but employees are required to abide by the rules and principles of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018) failure to do so can therefore, result in disciplinary proceedings.

Please refer to MTTs Data Breach Policy V(1) Jan 23

Policy responsibility and review

This policy and its procedures will be reviewed annually, to ensure it continues to meet our needs and those of our Regulators i.e., Awarding Organisations (NOCN Cskills Awards) , ESFA (Education & Skills Funding Agency) and external stakeholders.

The contact point for further advice is:

email: craig.barwick@mttraining.co.uk

Or in writing to

Attn: Craig Barwick
Multi Trades Training Ltd
Shalford Dairy
Wasing Estate
Aldermaston
Berkshire
RG7 4NB

Tel: +44 (0) 2034 883801
E: info@mttraining.co.uk