GDPR Policy

Policy statement for Multi Trades Training LTD (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 new Data Protection Act 2018 (DPA 2018) and the main provisions that apply, such as GDPR from the 25th May 2018.

We are required to retain certain information about its employees, learners and third parties to monitor:

- **Performance**
- **Achievement**
- **Health and Safety**
- **Safeguarding safer recruitment**
- **Pay salaries.**

It is necessary to collect and process information to enrol learners onto courses, organise training and ensure that legal obligations to funding bodies and Government agencies are complied with.

Information may be shared with third parties for education, training, employment and well-being related purposes including research. This will only take place where the law allows it and the sharing is in compliance with Data Protection legislation. Consent can be withdrawn at any time by contacting The Data Protection Officer using the details provided at the end of this Policy.

Authorised processing of information takes place as part of the day-to-day business however, we will ensure that employees who process personal information follow the key principles at all times. In summary, we will ensure that personal data shall:

- be processed in a lawful, fair and transparent manner (Lawfulness, Fairness and Transparency)
- be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Purpose Limitation)
- kept adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Data Minimisation)
- kept accurate and, where necessary, kept up to date (Accuracy)
- kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data is processed (Storage limitation)

• processed in a manner that ensures appropriate security of personal data (Integrity and confidentiality – Security)

• take responsibility for what we do with personal data and how we comply with the other data principles (Accountability)

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. A privacy impact assessment will be completed for this special category data.

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. Refer to the Document Retention Policy for further information.

Notification of Data Held and Processed:

All employees, learners and other users are entitled to know:

• what information the company processes about them any why

• how to gain access to it

• how to keep it up to date

• what we are doing to comply with its obligations under the act

Data Security:

All employees are responsible for ensuring that:

• Any personal data, which they hold, is kept securely

• Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party Unauthorised disclosure will be deemed a disciplinary matter, and may in serious cases be considered as gross misconduct.

Personal information will be:

• Secured in a locked filing cabinet, or drawer

• If it is computerised, be password protected

• Kept only on a memory stick or disc if encrypted and kept securely

Employees should ensure that casual disclosure doesn't not take place; by, for example:-

- leaving computer printouts uncovered on desktops or by allowing unauthorised users to view computer screens.
- Printouts containing any confidential information must be kept securely, and destroyed in a confidential manner.
- Extreme care must be taken to ensure that emails are sent securely and passwords to attachments are not sent by email but provided over the telephone or by text.
- Offices where staff are employed to process personal data should be locked when not occupied.
- Employees working from home or outside the office are responsible for taking extreme care with personal data to ensure this is keep secure.

Refer to the following policies for further information:

• Data Information and Security Policy

• Password Policy

• Email Policy

• Network Access and Authentication Policy

Employees :

Employees are responsible for checking that any information that they provide in connection with their employment is accurate and kept up to date.

Where an employee, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter to The Data Protection Officer.

Right to Access Rights to Information

All employees, learners and other third parties have individual rights to access personal data that is being held about them either on computer or in manual files. Any person who wishes to exercise this right is required to submit a subject access request in writing. Subject access requests should be made in writing to The Data Protection Officer. This request is free of charge and you will receive a response within one month of receipt. You have the right to:

• be informed about information we collect and share (The right to be informed)

• access your personal data (The right of access)

• rectification of inaccurate personal data (The right to rectification)

• erasure of personal data, this right is not absolute and only applies in certain circumstances (The right of erasure)

• request the restriction or suspension of your personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we are permitted to store the personal data, but not use it. (The right to restrict processing)

• receive personal data provided to a controller in a structured, commonly used and machine readable format. It also gives the right to request that a controller transmits this data directly to another controller. (The right to data portability)

• object to the processing of personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. (The right to object)

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.

Data Protection

Submit Data Protection queries and subject access requests in writing to:

Email: craig.barwick@mttraining.co.uk

Writing: Craig Barwick, 12 Enbourne Way, Brimpton, Berkshire, RG74TP

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