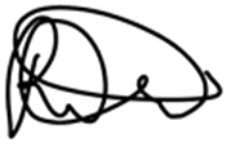
Multi Trades Training

Data Protection & Privacy Policy

Review Date: xxxxxxx

Approved by	**Rob Jones**	**Position**	**CEO**
Signature		**Date**	15/08/2025

Contents

Statement and Purpose 3
The Data Protection Officer 3
Scope 4
Definitions 4
Data Protection Principles 4
Lawful Basis for Processing Personal Data 4
Data Breach 5
Actions Required in the Event of a Personal Data Breach 5
The types of incidents that should be reported. 6
Individual Rights 6
Role and Responsibilities 7
Communication 8
Monitoring and Review arrangements 8
Associated Policies 9
Legal Requirements and external standards 9
Contact Information 9
Document Control 10
Appendix 1- Personal Data Breach Report Form 11

Statement and Purpose

Multi Trades Training ('Multi Trades', 'we', 'our' or 'the provider') 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) and the EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

This Policy sets out our obligations as a company registered in UK under number 11553273, whose registered office is at : Unit 8, Moniton Trading Estate, West Ham Lane, Basingstoke, Hampshire, RG22 6NQ and registered with the Information Commissioners Office (ICO) No: ZA700195.

All Data Users must comply with this Policy when processing Personal Data on behalf of Multi Trades and ensure the highest levels of ethical conduct and integrity apply in all areas of its operation and that all activities are conducted in an honest and transparent manner.

In this Data Protection Policy, references to "we" "our" and "us" shall mean Multi Trades and references to "you" shall mean staff and students that process Personal Data on our behalf.

The Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing this Data Protection Policy.

The position, independence and responsibility of the DPO is defined in Article 39 of UK GDPR to:

- Inform and advise Multi Trades and its employees about their obligations under Data Protection legislation
- Monitor compliance with the UK GDPR
- Advise on Data Protection Impact Assessments (DPIAs)
- Raise awareness of Data Protection legislation
- Co-operate with the supervisory authority, the Information Commissioner's Office, and act as its contact point
- Contact point for the administration of all Data Subject Rights relating to data held by the College; and
- Ensure College policy, guidelines and security measures are appropriate and up to date for the types of data being processed.

Aims of the Policy

- to identify the roles and responsibilities of staff in respect of compliance with this Data Protection Policy
- to make all staff and students that process personal data on our behalf aware of our legal obligations under the Data Protection legislation
- to set out our strategy for ensuring compliance with the Data Protection legislation in respect of processing Personal Data entrusted to Multi Trades
- to minimise the risk of any potential breach of the Data Protection legislation;
- to ensure all individuals (Data Subjects) are aware of their rights under the Data Protection legislation; and
- to encourage valued relationships with stakeholders and trust in our handling of Personal Data.

Scope

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 our its employees, agents, contractors, or other parties working on behalf of Multi Trades.

This Data Protection Policy shall apply to all Personal Data that Multi Trades processes and applies equally to information held in hardcopy or electronic form, which shall include photographic material and video footage.

Personal data may be held or transmitted in paper, physical and electronic formats or communicated verbally in conversation or over the telephone. This Data Protection Policy shall apply regardless of the party that created the Personal Data, where it is held, or the ownership of the equipment used.

Definitions

Data Protection Principles

All processing of Personal Data that you complete on behalf of Multi Tradesmust comply with the seven Data Protection principles contained within the UK GDPR.

In summary, the Data Protection principles require that Personal Data is:

1. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency)
2. Collected only for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes (Purpose Limitation)
3. Adequate, relevant and limited to what is necessary in relation to the purpose(s) for which it is processed (Data Minimisation)
4. Accurate and kept up to date (Accuracy)
5. Not kept in a form which permits identification of individuals for longer than is necessary for the purpose(s) it is processed (Storage Limitation)
6. Processed in a way ensures its security and to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Integrity and Confidentiality) and
7. Responsible for demonstrating compliance with the above listed principles (Accountability).

These seven Data Protection principles are the foundation on which the remainder of the legislation is built and so all staff and students must be mindful to comply with these principles at all times when processing Personal Data.

Lawful Basis for Processing Personal Data

In compliance with the first Data Protection principle set out above, Personal Data must be processed fairly, lawfully and in a transparent manner for specified purposes. UK GDPR requires that processing of Personal Data must be for one or more lawful purposes under Article 6 of UK GDPR, known as a “lawful basis”.

At least one of the following "lawful bases" must apply whenever Personal Data is being processed:

- **Consent**: the individual (Data Subject) has provided their informed consent to process their Personal Data for a specific purpose
- **Contract**: the processing is necessary for a contract with the Data Subject or is required to take specific steps before entering into a contract with the Data Subject
- **Legal obligation**: the processing is necessary to comply with the law (not including contractual obligations)
- **Vital interests**: the processing is necessary for the protection of the vital interests of the Data Subject or another person
- **Public task**: the processing is necessary to perform a task in the public interest or for official functions, and
- **Legitimate interests**: the processing is necessary for the legitimate interests of the party processing the Personal Data, unless there is a good reason to protect the Data Subject's Personal Data which overrides such legitimate interests. This lawful basis will not apply if a public authority (such as Multi Trades) is processing Personal Data to perform its public tasks.

You must identify the appropriate lawful basis before you commence to process any Personal Data on behalf of Multi Trades and keep a record of the lawful basis which is being relied upon. Further information which may help you identify the appropriate

Data Breach

Multi Trades is responsible for ensuring appropriate security for the Personal Data entrusted to it, which includes protecting Personal Data against unauthorised or unlawful processing and against accidental loss or destruction.

Actions Required in the Event of a Personal Data Breach

We will make every effort to avoid a Personal Data Breach from occurring, however if one should occur, the Data Protection legislation requires usto notify the Information Commissioner's Office (ICO) without undue delay and no later than 72 hours after having become aware of it. In some circumstances we will also have to notify the Data Subject without undue delay.

To meet the statutory reporting timeframes, we require you to:

- submit a Personal Data Breach Report Form to the Data Protection Officer ('DPO') immediately upon discovery of a Personal Data Breach or suspected breach
- provide all factual information available within the Personal Data Breach Report Form
- co-operate with the Data Protection & Information Compliance Unit with their investigations and response to all queries as a matter of urgency, and
- preserve all evidence relating to the suspected Personal Data Breach.

The Personal Data Breach Report Form can be found in Appendix 1. Once completed, immediately email the Report Form to info@mttraining.co.uk . A member of our staff shall then contact you in confidence to discuss the content of the report.

We shall investigate all incidents of a suspected or actual Personal Data Breach and take appropriate action to mitigate the consequences and prevent similar events occurring in the future.

Should the investigation confirm that a Personal Data Breach has in fact occurred, the Data Protection Officer will notify the ICO, where required, notify the Data Subject and update the Data Breach Register accordingly.

The types of incidents that should be reported.

Any Personal Data Breach or suspected Personal Data Breach including but not limited to any incident that could potentially compromise the security of Personal Data such as:

- theft or loss of a laptop
- loss of mobile phones, flash drives and other data storage devices
- sending an email or letter to the wrong address
- loss of Personal Data resulting from an equipment or systems failure
- loss of hardcopy documents are files which contain Personal Data
- non arrival of sensitive information
- maintenance of unsecured databases
- human error, such as accidental deletion or alteration of Personal Data
- unforeseen circumstances, such as a fire or flood, and
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams.

The above list is not exhaustive and should you be in in any doubt, please simply report the suspected incident to the DPO as a caution. Manage any breaches of data security promptly and appropriately,

This means that we will take all necessary steps to reduce the impact of incidents involving personal data by following the Data Breach Policy and Procedures.

Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Officer will liaise with the UK Information Commissioner's Office and report the breach, in line with regulatory requirements, within 72 hours of discovery. The Data Protection Officer will also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach.

Individual Rights

In accordance with the GDPR and the Data Protection Act 2018 every Data Subject has the following rights:

1. The right to be informed about how their Personal Data is to be used.
2. The right of access to their Personal Data held by the College and other information.
3. The right to rectification if their Personal Data is inaccurate or incomplete.
4. The right to request the deletion or removal of Personal Data where there is no compelling reason for its continued processing.
5. The right to restrict processing in certain circumstances.

6. The right to data portability which allows individuals to obtain and reuse their Personal Data for their own purposes across different services.
7. The right to object to processing in certain circumstances.
8. Rights in relation to automated decision making and profiling.

Role and Responsibilities

Anyone who processes Personal Data for Multi Trades, be that staff or students who process data on behalf of us, are required to adhere to this Data Protection Policy and the Related Policies and commit to ensuring that they:

- Read and comply with this Data Protection Policy and the Related Policies, as may be updated from time to time
- Seek advice from the DPO when unsure about how to comply with this Data Protection Policy and the Related Policies to ensure compliance with the Data Protection legislation
- Ensure that all Personal Data is obtained for specified, explicit and legitimate purpose and is only processed for those purposes
- Ensure that all Personal Data is processed lawfully, fairly and transparently with a "legal basis" for processing
- They only use the minimum amount of Personal Data necessary to fulfil the purpose and which is relevant to such purpose
- Do not disclose Personal Data to unauthorised persons, whether within or outside the College and at all times ensure access is restricted to authorised persons
- Keep and store the Personal Data securely with the level of security appropriate to the sensitivity of the Personal Data and in accordance with the Retention of Records Policy
- Ensure that the use of, and access to, computers, laptops and other portable electronic data processing/storage dev devices are compliant with our guidance
- Only retain the Personal Data for as long as strictly necessary to fulfil the purpose of its processing and in accordance with Records Retention Policy
- Ensure the Personal Data provided is accurate and where applicable, notify us immediately of any changes or errors so that the record can be updated or erased as appropriate
- Immediately report any suspected Personal Data Breaches and follow all recommended next steps as advised by the DPO
- Inform staff immediately of incidents where persons without proper authorisation are found in areas where Personal Data is held or processed, and
- Avoid disclosing Personal Data by telephone unless you are certain the caller is the person they claim to be and is authorised to receive the Personal Data in question.

In addition, all staff must also:

- Complete the compulsory Data Protection training programme together with any further training as specified by us periodically
- Respond promptly to any requests from the DPO in connection with any Subject Access Requests, Data Subject rights-based requests or complaints and immediately forward any such requests if received directly to the Data Protection Officer, so that we can comply with the statutory timeframe for response

- Where staff are responsible for supervising learners or students involved in work which requires the processing of Personal Data, that the staff are required to ensure that the students are fully aware of the Data Protection principles, the requirements of this Data Protection Policy and Related Policies and the need to obtain the informed consent of any Data Subjects involved as appropriate; and
- Avoid, in so far as possible, recording personal opinions not based on fact about a Data Subject. These comments will be disclosable.

Communication

This policy is communicated and implemented through development, implementation, monitoring and review of activities. These will require:

- The Data Protection Officer to liaise with managers to review and update information risk assessments and records of processing activities and take necessary actions to identify and protect personal data and systems used to process the data
- Coordination of effort between relevant Directors and professional specialists to integrate IT, physical security, people, information management, risk management and business continuity to deliver effective and proportionate information security controls
- Review and refresh of all relevant policies and procedures
- Generic and role specific training and awareness
- Embedding data protection by design and default and related information governance requirements into procurement, project management and the implementation of software applications or process enhancements
- Information security incident management policies and procedures
- Business continuity management
- Monitoring compliance and reviewing controls to meet business needs.

Monitoring and Review arrangements

The Data Protection Officer will monitor new and on-going data protection risks and update the Multi Trades risk register, reporting this promptly as required

The Data Protection Officer will liaise with all managers, to ensure that IT security risks related to data protection are captured on the register.

The Data Protection Officer will make regular reports to the Board of Governors on data protection compliance.

We will review the policy annually as part of our annual self-evaluation and assessment reporting (SAR) arrangements and revise as and when necessary, in response to actions from the qualifications regulators, legislation or internal practices, operational feedback from external agencies, customer and learner feedback as identified.

Associated Policies

This policy should be read in conjunction with:

- Data Privacy Policy
- Data Breach Policy & Procedure
- Complaints
- Quality Assurance
- Terms and Conditions

Legal Requirements and external standards

Effective data protection and information governance controls are essential for compliance with U.K. law and other relevant legislation in all jurisdictions in which the College operates:

- UK GDPR
- UK Data Protection Act 2018
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
- The EU GDPR, Regulation (EU) 2016/679

All current UK Legislation is published at http://www.legislation.gov.

- UK Information Commissioner's Office (ICO) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
- Guidance on the UK GDPR
- Privacy and Electronic Communications Regulations
- Age Appropriate Design Code
- Data Sharing Code
- Data Protection Guidance
- Joint Information Systems Committee (Jisc)
- Guidance on Data Protection for universities and colleges

Contact Information

By email to The Data Protection Officer: Rob Jones at rob.jones@mttraining.co.uk or info@mttraining.co.uk

Or by post to

Multi Trades Training Ltd
Unit 8
Moniton Trading Estate,
West Ham Lane,
Basingstoke,
Hampshire,
RG22 6NQ

Tel: +44 (0) 2034 883801

Document Control

Date	Review & Revision	Owner	Version
07.06.23	Inclusion of MTTs Data Breach Policy V(1) Jan 23	Quality Lead	V1.1 2023
22.04.24	Renamed to include Privacy and updated with ICO complaint information	Quality Lead	V1 2024
15.07.24	Updated trading address	Quality Lead	V1.1 2024
29.07.2025	General formatting – inclusion of the data principles and additional material changes	Quality Lead	V1 2025

Appendix 1- Personal Data Breach Report Form

To be completed by reporter			
Date incident occurred	Click or tap to enter a date.	**Date Reported**	Click or tap to enter a date.
Location of incident? (Remote, onsite, offsite, own PC, public PC, etc)			
Does the breach involve personal data?	Choose an item.		
Type of data breach: (Indicate what form the data was in when the incident occurred)	**Digital** (e.g., hacking, virus, ransomware, file corruption, mis-addressed email etc) ☐ **Electronic** (e.g., lost laptop, phone, USB device) ☐ **Verbal** (e.g., wrong information given in person) ☐ **Physical** (e.g., lost or misplaced file, letters, certs etc) ☐		
Details of incident: (State facts only and not opinions. Include details of staff involved and any contributing factors)			
What identifying details relating to individuals were disclosed? (select all that apply)	Data subject identity (name, surname, birth date) ☐ Contact details ☐ Identification data (passports, licence, data etc.) ☐ Economic or financial data ☐ Location Data ☐ Criminal convictions, offences or security measures ☐		
Were Special Categories of Data Involved?	Choose an item.		
If 'Yes' is selected above, what types of special categories of data were involved? (select all that apply)	Data revealing racial or ethnic origin ☐ Health and Mental Health data ☐ Religious or philosophical beliefs ☐ Sex life data ☐ Genetic data ☐ Biometric data ☐		
Number of individuals involved?		**Number of records lost, stolen, or accidentally disclosed?**	
What are the potential consequences and adverse effects on those individuals?			
Do you have back up of lost or stolen records?	Choose an item.		
Measures in Place What organisational measures were in place prior to the breach			
Follow Up Action Describe follow up action taken to prevent repetition of the incident:			
Reported By:		**Position**	
Signature			

To be completed by the Data Protection Officer			
What are the potential consequences and adverse effects on the organisation?			
Can the organisation recover back up of lost or stolen records?	Choose an item.		
Measures in Place What organisational measures were in place prior to the Breach and should they be revised? (If so, how?)			
Follow Up Action Describe follow up action taken to prevent repetition of the incident: (i.e., training, review of processes, etc)			
Has the ICO been informed within 72 hours? Only in the instance that an individual's rights or freedoms are likely to be at risk.	Choose an item.		
Has the data subject been informed? Only in the instance that their rights or freedoms are likely to be at risk.	Choose an item.		
Data Protection Officer		Date	Click or tap to enter a date.
Signature			