Title: **Personal Data Protection Policy** Ref: GDPR-001 (V2)

1 Purpose and Scope

This policy explains the terms 'data', 'personal data' and 'sensitive personal data' and describes how such data must be collected, processed, stored and disposed of to meet the Company's data protection standards and to comply with its legal requirements. Any failures to follow the policy may result in disciplinary proceedings.

In the course of doing business, the MTC needs to gather and use certain information about individuals. These individuals can include students, staff, contractors, applicants, alumni, customers, suppliers, business contacts and any other people the business has a relationship with or may need to contact.

All MTC employees and contractors are responsible for protecting the information that they hold about individuals. This includes contact information such as email addresses and telephone numbers of suppliers and customers as well as the more obvious financial and health information stored by specific departments.

2 Responsibilities

As the legal Data Controller the MTC is responsible for establishing policies and procedures in order to comply with the requirements of the Data Protection Act 2018.

2.1 Governance Team

The Governance Team comprises

- Data Protection Officer
- Departmental Data Controllers
- Legal and Commercial Representation

The Governance Team is responsible for:

- Data Protection registration with the Information Commissioner's Office (ICO). Details of MTC's registration are published on the Information Commissioner's website. Anyone who is, or intends, processing personal data for purposes not included in the notification should seek advice from the Governance Team;
- drawing up guidance, giving advice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information;
- the appropriate compliance with the data subject rights, including ensuring that subject access requests are logged and responded to in a timely manner;
- ensuring that any data protection breaches are resolved, catalogued and reported appropriately in a swift manner and in line with guidance from the Information Commissioner's Office;
- investigating and responding to complaints regarding data protection including requests to cease processing personal data;
- providing appropriate documentation around privacy notices

2.2 The Data Protection Officer (DPO)

The DPO is responsible across the entire company for all data protection issues. The DPO reports to the Head of Commercial and Legal. Their role is:

- to inform and advise the organisation and its employees about their obligations to comply with the data protection laws;
- to monitor compliance with the data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training of staff and ensuring internal audits are carried out;
- to be the first point of contact for supervisory authorities and for individuals whose data is processed.

2.3 Departmental Data Controller

Departmental data controllers are the people who determine the purposes for which, and the manner in which, any personal data is processed. While MTC is the data controller of all personal data used in our business, departmental data controllers are appointed where necessary. If there is no departmental data controller then reference should be made to the Data Protection Officer. Data Controllers have a responsibility to:

- demonstrate control of the data in an auditable way;
- establish practices and policies in line with the data protection legislation;
- retain responsibility for the processing of data, no matter where that data is processed, by informing the processors and data subjects how the data is used and controlled.

2.4 Managers

Managers, including those who employ contractors, short term or voluntary staff, should ensure that:

- all personnel must be appropriately vetted for the personal data that they are processing;
- any personal data collected or processed in the course of work undertaken for MTC is kept securely and confidentially;
- all personal data is returned to MTC on completion of the work, including any copies that may have been made. Alternatively that the data is securely destroyed and the MTC receives notification in this regard from the contractor or short term / voluntary member of staff;
- MTC receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
- any personal data made available by MTC, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from MTC. This includes the use of cloud based accounts and storage;
- all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly;
- Where external companies are used to process personal data on behalf of MTC, responsibility for the security and appropriate use of that data remains with MTC, and the contracting department's Manager. Where a third-party data processor is used:
    - a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
    - reasonable steps must be taken to ensure that such security measures are in place;
    - a written contract establishing what personal data will be processed and for what purpose must be set out;
    - a data processing agreement, available from the Legal Department, must be signed by both parties.

- For further guidance about the use of third-party data processors please contact the Governance Team.

2.5 Staff

Staff members who process personal data must comply with the requirements of this policy. Staff members must ensure that:

- all personal data that they provide to MTC is up to date and accurate, and that MTC is informed of any changes to that data;
- all information they handle is protected by following our data protection and security policies at all times;
- no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party. This includes the disclosure of email addresses and telephone numbers over the phone;
- personal data is kept in accordance with MTC's retention schedule;
- any queries regarding data protection, including subject access requests and complaints, are directed to the Governance Team within 4 hours of receipt;
- any data protection breaches are swiftly brought to the attention of the Governance Team and that they support the Governance Team in resolving breaches;
- where there is uncertainty around a Data Protection matter advice is sought from the Governance Team.
- Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Governance Team.

3 Definition of data protection terms

Data is information which is stored on a computer, or in paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Personal data means data relating to a living individual who can be identified from that data, or from that data and other information that is likely to come into our possession. Personal data can be factual (such as a name, address or date of birth), an opinion (such as a performance appraisal) or assigned (such as a telephone number or email address).

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

The Data Controller, in our case The Manufacturing Technology Centre Ltd, is the organisation responsible for determining the purposes for which, and the manner in which, any personal data is processed.

Data processors include any organisation or person who processes personal data on behalf of a data controller.

The **Information Commissioner's Office (ICO)** (www.ico.org.uk) is the UK's independent authority for data protection in the UK, and is the "supervisory authority" in terms of the Data Protection Act 2018.

4 Data protection principles

Anyone processing personal data must comply with the enforceable principles of good practice laid out in Article 5 of the GDPR. These require that personal data shall be:"

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) 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."

4.1 Fair and lawful processing

The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The lawful bases for processing are set out in Article 6 of the GDPR, and at least one of these must apply whenever personal data is processed:

1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

4. Vital interests: the processing is necessary to protect someone's life.
5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

4.2 Processing in line with data subject's rights

Data must be processed in line with data subjects' rights. Data subjects have the following rights:

1. The right to be informed about the collection and use of their personal data.
2. The right of access to their personal data and supplementary information. This allows individuals to be aware of and verify the lawfulness of the processing.
3. The right to rectification allows individuals to have inaccurate personal data rectified, or completed if it is incomplete.
4. The right to erasure is not absolute and only applies in certain circumstances.
5. The right to restrict processing is not absolute and only applies in certain circumstances.
6. The right to data portability gives individuals the right to obtain and reuse their personal data for their own purposes across different services. It only applies to data that they have provided in the first instance and is only valid where processing is based on consent of for the performance of a contract and processing is carried out by automated means.
7. The right to object gives individuals the right to object to processing based on legitimate interests, direct marketing and processing for the purposes of scientific research and statistics. If the right to object meets the criteria then MTC will stop processing the data immediately.
8. Rights in relation to automated decision making and profiling

Not all rights are available to individuals as the following table describes:

	Right to Erasure	Right to Portability	Right to Object
Consent	Yes	Yes	No – but they have the right to withdraw consent
Contract	Yes	Yes	No
Legal Obligation	No	No	No
Vital Interest	Yes	No	No
Public Task	No	No	Yes
Legitimate Interest	Yes	No	Yes

4.2.1 Dealing with Subject Requests

A formal request from a data subject around information that we hold about them must be made verbally or in writing to the corporate Data Protection Officer (dpo@the-mtc.org). MTC will comply with the request as quickly as possible, but will ensure that a response is provided within 1 month.

5 Data Protection Breaches

A data protection breach is considered to be anything that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes both accidental and deliberate breaches.

Where a Data Protection breach occurs, or is suspected, it must be reported within 2 hours of detection to the Data Protection Officer (dpo@the-mtc.org). This will trigger an investigation which must include full and accurate details of the incident, including who is reporting the incident and what classification of data is involved.

In the event of a data breach, then the breach will be documented and analysed by the Governance Team and decisions will be taken with regards to notifying the ICO (risk to people's rights and freedoms) and to notifying the affected people (high risk to people's rights and freedoms).

6 Data security

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if the processor agrees to comply with those procedures and policies, or if the processor puts in place adequate measures.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

a. Confidentiality means that only people who are authorised to use the data can access it.
b. Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
c. Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.
d. Non-Repudiation provides proof of the integrity and origin of the data, ensuring that the data is genuine.

6.1 Governance

MTC has in place the following agreements, contracts and policies that govern the security and the use of the systems within the business.

a. Non-Disclosure Agreements
b. Contracts
c. Building Access Policy (EST-001)
d. IT Policy (IT-002)
e. Data Protection Policy (this document)

f. Cyber Essentials Plus accreditation

6.2 Physical Security

MTC has put in place the following physical security barriers to protect access to its facilities, equipment and data.

a. Entry controls. Any stranger seen in entry-controlled areas should be reported.
b. Secure lockable desks and cupboards. Desks and cupboards must be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
c. Methods of disposal. Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.
d. Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended.

6.3 Personnel Security

a. Training for departmental managers and other staff classed as controllers
b. Awareness training for all staff in the business
c. BPSS clearances for staff in the business

6.4 Cyber Security

MTC provide the following cyber security measures to ensure the security of its data and systems.

a. Firewalls and external security
b. Encryption, firewalls and antivirus on all endpoints
c. Web and Email logging and monitoring
d. Removable media logging and monitoring
e. Controlled access via Active Directory Groups to all areas of the network
f. Logging and monitoring of file accesses, changes and deletions
g. Tagging of data to pre-determined rules
h. Regular Health Checks by 3rd parties

7 Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by MTC. In particular they should:

a. Not pass out information such as telephone numbers or email addresses without the consent of the individual concerned;
b. Offer to take a message or transfer the call;
c. Refer to their line manager for assistance in difficult situations. No-one should feel that they are being pressurised into disclosing personal information.

8 Retention of Data

In order to comply with legislation, MTC will keep some forms of information for longer than others.

Data retention periods will be defined in the data protection registers held by the Governance Team.

9 Subject Consent

In many cases MTC processes personal data with the consent of the individual. If the data is sensitive, express consent must almost always be obtained. Agreement to MTC processing some specified classes of personal data is a condition of employment for working in certain areas. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974.
All prospective staff will be asked to consent to their data being processed when an offer of employment or a course place is made. A refusal to sign such a form without good reason may result in the offer being withdrawn.

10 Processing

10.1 Processing Personal information

MTC process personal information in line with their legal obligations. Contact information provided by the Company will be shared externally via online federation systems such as Microsoft Teams, through the use of Business Cards, and through the passing of information to the Members of MTC. MTC will share personal information with 3rd parties when necessary to meet their statutory and contractual obligations and these will be recorded in the data protection registers maintained by the Data Controllers. MTC will not share personal information with 3rd parties unless it is required for contractual or legal obligations, or where consent has been given and recorded by the appropriate department.

10.2 Processing Sensitive Personal Information

Sometimes it is necessary to process sensitive personal information. This may be to ensure that MTC is a safe place for everyone, or to operate other MTC policies, such as the sick pay policy or equality policies. MTC may also ask for information about particular health needs, such as allergies to particular forms of medication, or any health conditions or disabilities. Because this information is considered sensitive, subjects will be asked to give express consent for MTC to process this information. MTC will not share this information with 3rd parties unless it is required for contractual or legislative obligations.

11 Compliance

Compliance with the Act is the responsibility of all staff. Any deliberate or negligent breach of the Data Protection Policy may lead to access to MTC facilities being withdrawn, disciplinary action being taken or criminal prosecution in serious cases. It may also result in personal liability for the individual. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

12 Exclusions

Any personal data that is not required for legitimate business purposes that is stored electronically on MTC systems or in paper form in MTC desks or cupboards is considered to be processed by individuals strictly for personal/household activities, and therefore falls outside this policy and the Data Protection Act 2018.

Reasonable amounts of such data should only be stored in the individual's home/workplace folder, is held at the individual's own risk and should be deleted at the earliest opportunity.
In the event of a data breach in these areas, there is no requirement under the Data Protection Act to notify the individuals concerned.