DATA PROTECTION POLICY

1) **Purpose**
    a) Engineering Trust Training (ETT) provides apprentice recruitment and training services to the engineering industry. These activities require documents and data to be retained for the time required by law or by the data retention clauses within current and past contracts.
    b) This policy outlines ETT's commitment to compliance with Data Protection Law and sets out the principles and procedures to be followed by all Staff. This policy should be read in conjunction with ETT's Data Retention Policy and Privacy Statement.
2) **Definitions**
    a) **Apprentice**: means an individual employed by the Employer under an Apprenticeship Agreement who is an Apprentice under the DfE Rules.
    b) **Apprentice Personal Data**: means Personal Data about apprentices of the Employer.
    c) **Board of Trustees**: appointed group of individuals that has overall responsibility for the management of ETT.
    d) **Data Controller**: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by Union or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by Union or Member State law.
    e) **Data Discloser**: a Party who discloses Personal Data to the other.
    f) **Data Processor**: means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller.
    g) **Data Protection Law**: means the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and any national laws or regulations constituting a replacement or successor.
    h) **Data Receiver**: a Party who receives Personal Data from the other.
    i) **Data Subject**: means an identified or identifiable natural person about whom Personal Data is processed; an identifiable natural person is one who can be identified, directly or indirectly, by reference to the Personal Data.
    j) **Employer**: means a business who employs an Apprentice.
    k) **Employer Staff Personal Data**: means Personal Data about an individual who works for the Employer of an Apprentice.
    l) **Personal Data**: means information relating to a Data Subject such as a name, an identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person, including opinions about a Data Subject.
    m) **Special Category Personal Data**: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic or biometric data processed for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person\'s sex life or sexual orientation.

n) **Subcontractor:** means a third party who ETT subcontracts specific elements of an Apprentice's programme.
o) **Subcontractor Staff Personal Data**: means Personal Data about an individual who works for the Subcontractor associated to a specific Apprentice.
p) **Processing**: means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
q) **Shared Personal Data**: The Personal Data to be shared between the parties for the Agreed Purpose, including the Apprentice Personal Data, Employer Staff Personal Data and Staff Personal Data and such other Personal Data as agreed from time to time between the parties for the purpose of giving effect to this Agreement.
r) **Staff Personal Data**: Personal Data about ETT employees, consultants, agents or third parties engaged in the delivery of academic learning for apprenticeships.
s) **Staff**: ETT employees, consultants, agents or third parties engaged in the delivery of academic learning for apprenticeships.

3) Data Protection Principles

a) ETT is committed to processing Personal Data in accordance with the following data protection principles as set out in Data Protection Law. Personal Data shall be:
    i) processed lawfully, fairly and in a transparent manner,
    ii) collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purpose,
    iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'),
    iv) accurate and, where necessary, kept up to date,
    v) 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 ('storage limitation'), and
    vi) 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 ('integrity and confidentiality').

4) Lawful Basis for Processing

a) ETT processes Personal Data in accordance with one or more of the lawful bases set out in Article 6 of the UK GDPR. The specific basis relied upon is determined by the purpose of the processing and documented in our Record of Processing Activities.
b) Our primary lawful bases for processing Apprentice, Employer Staff, Subcontractor Staff and Staff Personal Data are:
    i) Contract: Processing necessary for the performance of the apprenticeship training contract with the Employer and Apprentice.
    ii) Legal Obligation: Processing necessary to comply with our legal obligations (e.g. reporting to the Department for Education (DfE), safeguarding, health and safety).
    iii) Legitimate Interests: Processing necessary for the legitimate interests pursued by ETT in administering and improving our training services, ensuring quality and safety, and maintaining effective business operations,

provided such interests are not overridden by the interests or fundamental rights and freedoms of the Data Subject.

c) Where ETT processes Special Category Personal Data (e.g. health information for reasonable adjustments), we will additionally identify and rely on a condition under Article 9 of the UK GDPR, such as explicit consent, or necessity for reasons of substantial public interest, or for the purposes of preventive or occupational medicine.

5) Roles and Responsibilities

a) Board of Trustees: Has ultimate responsibility for ensuring ETT complies with Data Protection Law and for endorsing this policy.

b) Data Protection Officer (DPO): The DPO is responsible for:

i) informing and advising ETT and its Staff on data protection obligations,
ii) monitoring compliance with Data Protection Law and this policy,
iii) providing advice on Data Protection Impact Assessments (DPIAs),
iv) acting as the primary point of contact for the Information Commissioner's Office (ICO) and for Data Subjects,
v) maintaining the Record of Processing Activities, and
vi) adopting a robust approach to data security, including:
(1) ensuring that specific physical and electronic spaces are made available for the storage of Personal Data,
(2) prohibiting the transfer of Personal Data to external devices, unless approved by the DPO under an appropriate data sharing agreement,
(3) ensuring that all Staff report any breaches of data security to the DPO,
(4) ensuring appropriate precautions are taken when using mobile devices, and
(5) ensuring that all requests to share Personal Data with third parties are referred to the DPO for approval,
vii) proviing advice about secure and appropriate methods of sharing data if appropriate,
viii) following a clear Data Retention Policy that outlines what Personal Data is kept, why it is kept, how it is kept and for how long,
ix) publishing a Privacy Statement outlining: the organisation and contact details of the DPO; the basis for collecting Personal Data; how the Personal Data is used; how it is kept secure,
x) respecting, facilitating and appropriately responding to the rights of individuals, and
xi) ensuring that all Staff are fully trained in respect of their data protection responsibilities.

c) All Staff: Are responsible for:

i) completing all required data protection training,
ii) reading, understanding, and complying with this policy and related procedures,
iii) ensuring Personal Data is collected, used, stored, and shared securely and in line with instructions, and
iv) reporting any actual or suspected data breach, security incident, or policy non-compliance immediately to the DPO.

6) Data Subject Rights

a) Data Protection Law provides Data Subjects with specific rights regarding their Personal Data. ETT is committed to respecting, facilitating, and responding appropriately to these rights, which include: the right to be informed; the right of access; the right to rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and rights related to automated decision making.
b) ETT is committed to:
    i) responding to all data subject rights requests with transparency and integrity,
    ii) ensuring that all personal data is processed fairly and lawfully and in accordance with data subjects' rights, and
    iii) ensuring that all Staff comply with this policy when dealing with data subject rights.
c) All requests to exercise data subject rights must be referred immediately to the DPO.
d) The DPO will verify the identity of the requester and will aim to respond to valid requests without undue delay and within one month of receipt. If an extension is needed, the Data Subject will be informed within one month.
e) Responses will be provided free of charge, except in cases of manifestly unfounded or excessive requests.
f) The DPA and UK GDPR set out several exemptions which may apply to data subject rights requests. ETT may be exempt from complying (in full or in part) with a request if, for example:
    i) the information sought is classed as 'third party data',
    ii) disclosure would prejudice the prevention or detection of crime,
    iii) ETT is required by law to retain the data, or
    iv) another applicable exemption applies.
g) The DPO will inform the Data Subject of their right to lodge a complaint with the ICO and of their ability to seek an internal review of ETT's decision.

7) Use of Data and Data Sharing

a) Processing of Personal Data by ETT is for the primary purpose of providing a programme of academic learning for apprenticeships to Apprentices of an Employer.
b) Apprentice Personal Data is processed in connection with ETT providing a programme of academic learning for apprenticeships.
c) Employer Staff Personal Data is processed in connection with ETT providing a programme of academic learning for apprenticeships of the Employer.
d) Staff Personal Data is processed in connection with ETT providing a programme of academic learning for apprenticeships.
e) Shared Personal Data between ETT, the Employer and other third parties involved in providing a programme of academic learning for apprenticeships is necessary to progress, protect and manage an Apprentice.
f) Apprentice Personal Data, Employer\'s Staff Personal Data and Staff Personal Data will be retained in line with the ETT Data Retention Policy.
g) Types of personal data will include but not be limited to Name, Address, Email address, Telephone number, Academic results and progress, Unique Learner Number.
h) Permitted Data Processors will include:

i) any person providing the Training Services on behalf of the ETT,
ii) any Company who recruits for or employs an Apprentice using ETT
iii) IT service providers (for the purpose of hosting, supporting or maintaining the ETT IT systems, including any back-up, disaster recovery systems, learning platforms and operational platforms),
iv) Governing or funding bodies such as the DfE, and
v) End point assessment organisations.

i) A Data Processor will only Process Shared Personal Data for the purposes of providing a programme of academic learning for apprenticeships and will do so in accordance with the lawful bases outlined in this policy.
j) Data Processors shall comply with all applicable requirements of the Data Protection Law with respect to its Processing of the Shared Personal Data.
k) The Data Discloser shall, in respect of Shared Personal Data, ensure that its privacy notices are clear and shall provide sufficient information to the Data Subjects for them to understand what of their Personal Data the Data Discloser is sharing with the Data Receiver, the circumstances in which it will be shared, the purposes for the data sharing and the identity of the Data Receiver.
l) The Data Receiver undertakes to inform the Data Subjects the purposes for which it will Process their Personal Data and provide all the information that it must provide in accordance with Data Protection Law, to ensure that the Data Subjects understands how their Personal Data will be processed by the Data Receiver.
m) ETT may, at its sole discretion, request that the Employer provide evidence in a form acceptable to ETT of compliance with Data Protection Law. Such requests will be reasonable in scope.
n) The Data Receiver will not engage any third-party Data Processor to Process the Shared Personal Data without the prior written consent of the Data Discloser.
o) Where the Data Receiver appoints a third party as Data Processor for the purpose of Processing Shared Personal Data it must ensure that the Data Processor has in place appropriate technical and organisational measures to meet the requirements of Data Protection Law and protect Data Subject rights.

8) Data Processor Obligations

a) Where ETT engages a Data Processor, or acts as a Data Processor for another party, the following obligations shall apply as required by Data Protection Law.
i) The Data Processor shall only Process the Shared Personal Data on documented instructions from the Data Controller, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by applicable law to which the Data Processor is subject; in such a case, the Data Processor shall inform the Data Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.
ii) The Data Processor shall ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
iii) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall implement appropriate technical and

organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate including:

(1) the encryption of Personal Data,
(2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
(3) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
(4) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

iv) In assessing the appropriate level of security, account must be taken of the risks that are presented by Processing, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

v) In the event of an actual or suspected Personal Data breach involving the Shared Personal Data, the Data Controller shall take overall responsibility for any Personal Data breach obligations under Data Protection Law. The Data Processor shall conform to the reasonable requirements of the Data Controller in respect of Personal Data breach notification requirements under Data Protection Law, including;

(1) notifying the Data Controller without undue delay to enable the Data Controller to fulfil its notification requirements to the ICO; and
(2) providing a description of the nature of the breach, the likely consequences, and the measures taken or proposed to address it.

vi) Each party shall be responsible for any obligation it has with regards to the rights of Data Subjects, save that if a Data Subject exercises any of their rights in respect of Personal Data then:

(1) the Data Processor shall inform the Data Controller, and the Data Controller may, at its discretion, provide any response to the Data Subject,
(2) the Data Processor shall not respond to the Data Subject unless instructed to do so by the Data Controller; and
(3) the Data Processor shall promptly provide all information in its possession or control that the Data Controller requires to respond to the Data Subject.

vii) The Data Processor shall not engage another Data Processor without first informing the Data Controller of any intended changes, thereby giving the Data Controller the opportunity to object to such changes.

viii) Where a Data Processor engages another Data Processor, the same data protection obligations as set out above will be imposed on that other Data Processor by way of a contract. Where that other Data Processor fails to fulfil its data protection obligations, the initial Data Processor shall remain fully liable to the Data Controller for the performance of those other Data Processor's obligations.

ix) Taking into account the nature of the Processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data

Controller\'s obligation to respond to requests for exercising the Data Subject's rights.

x) At the choice of the Data Controller, the Data Processor shall delete or return all the Personal Data to the Data Controller after the end of the provision of the Agreed Services relating to Processing and delete existing copies unless applicable law requires storage of the Personal Data.

xi) The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down under Data Protection Law and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

9) Data Security

a) ETT shall ensure that personal data is stored securely using modern software that is kept-up to date.
b) Access to personal data shall be limited to personnel who need access and appropriate security is in place to avoid unauthorised sharing of information.
c) When personal data is deleted, this will be done safely such that the data is irrecoverable.
d) Appropriate back-up and disaster recovery solutions are in place.

10) Data Breach Management

a) In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the DPO shall be notified immediately.
b) The DPO will promptly assess the risk to people's rights and freedoms.
c) Where the breach is likely to result in a risk to rights and freedoms, ETT shall report it to the ICO within 72 hours of becoming aware of it, where feasible.
d) If the breach is likely to result in a high risk to affected individuals, ETT shall also notify those individuals without undue delay.
e) All breaches (actual or suspected) shall be recorded in an internal breach log. The DPO will take remedial action to mitigate the situation.

11) Data Retention & Disposal

a) To ensure that personal data is kept for no longer than necessary, ETT maintains a Data Retention Policy for each area in which personal data is processed and reviews this policy annually.
b) The Data Retention Policy shall consider what data should/must be retained, for how long, and why.
c) All confidential (hard copy waste) will be shredded and recycled by an approved waste contractor, who will provide a certificate of destruction.
d) All electronic data is currently saved and archived. As the volume of archived data increases a policy for review and disposal will be determined and implemented.

12) DfE (formerly ESFA)

a) Learner data will be shared with the Department for Education (DfE) (previously body was the Education and Skills Funding Agency (ESFA)) to update them on progress and to claim funding. Information regarding how this data is handled can be found here: https://www.gov.uk/government/publications/esfa-privacy-notice

13) Policy Governance

a) This policy is owned by the Board of Trustees and managed by the DPO. It will be reviewed annually or in response to significant changes in law or practice. All Staff are required to familiarise themselves with this policy.

14) Contact

a) The Data Protection Officer (DPO), Mark Vingoe, is responsible for monitoring compliance with this policy and can be contacted using the following details:
The Engineering Trust Training Ltd, The Engineering Skills Academy. 11 Wedgwood Road, Bicester, Oxon, OX26 4UL. Telephone 01993 882008.
Email info@theengineeringtrust.org