DATA PROTECTION POLICY

1) Purpose

Engineering Trust Training Ltd (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.

The General Data Protection Regulations ('GDPR') regulates how organisations use the personal data of living individuals. It requires organisations to be accountable and transparent in its handling of such data and gives individuals rights to challenge its use and to access the data held. The GDPR supersede the Data Protection Act 1998 and this policy has been updated to reflect the new regulations.

2) Definitions

a) Apprentice Personal Data: means Personal Data about apprentices of the Employer;
b) Employer Staff Personal Data: means Personal Data about an individual who works for the Employer of an apprentice;
c) Staff Personal Data: Personal Data about ETT employees, consultants, agents or third parties engaged in the delivery of academic learning for apprenticeships.
d) Staff: ETT employees, consultants, agents or third parties engaged in the delivery of academic learning for apprenticeships.
e) 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;
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 Discloser: a Party who discloses Personal Data to the other
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) 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.
k) 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;
l) Data Protection Law: means the European Union Data Protection Directive 95/46/EC, any national laws or regulations implementing that Directive, including the Data Protection Act 1998 (DPA); the General Data Protection Regulation EU 2016/679 (GDPR) (when applicable) and any national laws or regulations constituting a replacement or successor data protection regime to that governed by GDPR;

m) 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;

n) 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.

3) Data Security Procedures

a) GDPR regulations state that ETT is required to put in place comprehensive but proportionate governance measures to minimise the risk of data breaches and to uphold the protection of Personal Data. ETT will ensure that data is:

i) Processed lawfully, fairly and in a transparent manner in relation to individuals;

ii) collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes;

iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed;

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;

vi) Processed in a manner that ensures appropriate security of Personal Data.

b) The ETT Data Protection Officer (DPO) adopts a robust approach to data security, including:

i) ensuring that specific physical and electronic spaces are made available for the storage of Personal Data

ii) prohibiting the transfer of Personal Data to external devices, unless approved by the DPO under an appropriate data sharing agreement

iii) ensuring that all staff report any breaches of data security to the DPO

iv) ensuring appropriate precautions are taken when using mobile devices

v) ensuring that all requests to share Personal Data with third parties are referred to the DPO for approval. The DPO will also provide advice about secure and appropriate methods of sharing data if appropriate

vi) follows a clear Data Retention Policy that outlines what Personal Data is kept, why it is kept, how it is kept and for how long

vii) maintains records of data Processing activities

viii) publishes 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

ix) respects, facilitates and appropriately responds to the rights of individuals by:

- seeking consent from the Data Subject to use their Personal Data (if required), ensuring that this consent is of an “opt in” nature
- providing access to a copy of Personal Data and supplementary information in either hard copy or electronic format, within a month of a formal request being made

- rectifying any inaccuracies or incomplete Personal Data within a month of a formal request being made
- erasing all Personal Data if it is not required to be kept for a legitimate need within a month of a formal request being made
- notifying the Data Subject if the security of their Personal Data is compromised within 14 days of a breach occurring
- complying with a withdrawal of consent within a month of the request being made disclosing any automated decision making / profiling practices

x) ensures that all staff are fully trained in respect of their data protection responsibilities

xi) records and responds to actual or potential data protection compliance failures effectively. Staff are required to report any actual or potential breaches to the DPO who will:

- report any data breach to the ICO as soon as possible but within 72 hours
- take remedial action to mitigate the situation
- notify Data Subjects affected by the breach
- maintain a log of actual and potential compliance failure

4) Use of Data

a) Processing of Personal Data by ETT is to provide 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 in order 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 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 ESFA

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 only with the consent of the Data Subjects.

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 of 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.

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.

p) 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;

q) 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;

r) 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:
   i) the encryption of Personal Data;
   ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   iii) 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
   iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing;

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

t) 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;

i) notifying the Data Controller without undue delay, and not later than 48 hours after having become aware of the Personal Data breach, to enable the Data Controller to fulfil its notification requirements to the ICO; and

ii) the notification described in paragraph t)i) shall at least:

- describe the nature of the Personal Data breach, including where possible: the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
- communicate the name and details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the Personal Data breach; and
- describe the measures taken or proposed to be taken to address the Personal Data breach, including, measures to mitigate its possible adverse effects;

u) 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, or purports to exercise any of their rights under Data Protection Law in respect of Personal Data then:

i) the Data Processor shall inform the Data Controller and the Data Controller may, at its discretion, provide any response to the Data Subject having regard to both the Data Controller's and the Data Processor's obligations under Data Protection Law;

ii) the Data Processor shall not respond to the Data Subject unless instructed to do so by the Data Controller; and

iii) the Data Processor shall promptly provide all information in its possession or control that the Data Controller requires in order to respond to the Data Subject;

v) The Data Controller and Data Processor will take steps to ensure that any natural person acting under the authority of the Data Controller or the Data Processor who has access to Personal Data does not Process them except on instructions from the Data Controller, unless he or she is required to do so by applicable law;

w) The Data Processor shall not engage another Data Processor without first informing the Data Controller of any intended changes concerning the addition or replacement of other Data Processors, thereby giving the Data Controller the opportunity to object to such changes;

x) Where a Data Processor engages another Data Processor for carrying out specific Processing activities on behalf of the Data Controller, the same data protection obligations as set out above will be imposed on that other Data Processor by way of a contract or other legal act under applicable law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of Data Protection Law. 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 that other Data Processor's obligations;

y) 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 laid down in Data Protection Law.

z) 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;

aa) 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.

5) Data Disposal

a) All confidential (hard copy waste) will be shredded and recycled by an approved waste contractor, who will provide a certificate of destruction.

b) All electronic data is currently saved and archived off site. As the volume of archived data increases a policy for review and disposal will be determined and implemented.

6) ESFA

a) Learner data will be shared with the ESFA in order 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

7) Contact

a) The DPO can be contacted using the following details:

i) The Engineering Trust Training Ltd, 2 The Courtyard, Home Farm, Caversfield, Bicester, OX27 8TG. Telephone 01993 882008. Email info@theengineeringtrust.org