DATA PROTECTION POLICY

Purpose

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.

1) Definitions

a) Apprentice: means an individual employed by the Employer under an Apprenticeship Agreement who is an Apprentice under the ESFA 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 any national laws or regulations including the Data Protection Act 1998 amended (DPA), the UK General Data Protection Regulation (UK GDPR) 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) 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;

o) 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.
p) Staff Personal Data: Personal Data about ETT employees, consultants, agents or third parties engaged in the delivery of academic learning for apprenticeships.
q) Staff: ETT employees, consultants, agents or third parties engaged in the delivery of academic learning for apprenticeships.

2) Data Security Procedures

a) 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:
      (1) the organisation and contact details of the DPO
      (2) the basis for collecting Personal Data
      (3) how the Personal Data is used
      (4) how it is kept secure
   ix) respects, facilitates and appropriately responds to the rights of individuals by:
      (1) seeking consent from the Data Subject to use their Personal Data (if required), ensuring that this consent is of an “opt in” nature

(2) 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
(3) rectifying any inaccuracies or incomplete Personal Data within a month of a formal request being made
(4) 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
(5) notifying the Data Subject if the security of their Personal Data is compromised within 14 days of a breach occurring
(6) complying with a withdrawal of consent within a month of the request being made disclosing any automated decision making / profiling practices
(7) ensures that all staff are fully trained in respect of their data protection responsibilities
(8) 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:
    (a) report any data breach to the ICO as soon as possible but within 72 hours
    (b) take remedial action to mitigate the situation
    (c) notify Data Subjects affected by the breach
    (d) maintain a log of actual and potential compliance failure.

3) 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 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 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 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 including;
    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 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.

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:
      (1) 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,
      (2) communicate the name and details of the data protection officer or other contact point where more information can be obtained,
      (3) describe the likely consequences of the Personal Data breach; and
      (4) 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 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.

4) Lawful, fair and transparent processing

a) Individuals have the right to access their personal data, and any such requests made to ETT shall be dealt with in a timely manner.

5) Data minimisation

a) ETT shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6) Accuracy

a) ETT shall take reasonable steps to ensure personal data is accurate.

b) Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7) Data Subject Rights

a) Data Protection Law sets out eight rights, which individuals can exercise in terms of their personal information. The legislation gives individuals the following rights:

i) The right to be provided with specified information about the processing of their personal data (‘the right to be informed’).

ii) The right to access their personal data and certain supplementary information (‘the right of access’, sometimes known as ‘Data Subject Access’).

iii) The right to have their personal data rectified, if it is inaccurate or incomplete (‘the right of rectification’).

iv) The right to have, in certain circumstances, their personal data deleted or removed (‘the right of erasure’, sometimes knowns as ‘the right to be forgotten’).

v) The right, in certain circumstances, to restrict the processing of their personal data (‘the right to restrict processing’).

vi) The right, in certain circumstances, to move personal data the individual has provided to another organisation (‘the right of data portability’).

vii) The right, in certain circumstances, to object to the processing of their personal data and, potentially, require the NMC to stop processing that data (‘the right to object’).3.8. The right, in relevant circumstances, to not be subject to decision making based solely on automated processing (‘Rights related to automated decision making, including profiling’).

b) ETT are commitment 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,
iii) ensuring that all Staff comply with this policy when dealing with data subject rights, and
iv) identifying the approach that we will routinely take when responding to requests, including setting out in general terms any exemptions in the DPA we are likely to apply when responding to requests.

c) Apart from requests made on behalf of data subjects by an agent acting for that data subject, this policy does not cover requests for personal data made by third parties under the Freedom of Information Act or, as a Third-Party Disclosure Request.
d) The DPO will monitor compliance with this policy and provide advice on responding to data subject rights requests.
e) All Staff are responsible for:
   i) identifying data subject rights requests
   ii) referring data subject rights requests immediately to the DPO
   iii) co-operating with and assisting the DPO to coordinate responses to requests. ETT will provide staff with appropriate training/guidance so that they are able to comply with their responsibilities under this policy.
f) ETT will publish this document on our website to inform people of their rights and how they can exercise their data subject rights.
g) The DPO will ask applicants to provide written confirmation of their request via email. This is because of the requirement to be satisfied of the applicant's identity and for audit purposes.
h) The DPO can accept data subject rights requests by telephone however, these will be subject to further identity checks. In any circumstance, we reserve the right to make identity checks as deemed necessary.
i) The DPO will progress a subject rights request once the following information has been received from the requester:
   i) full name
   ii) previous name(s) (if applicable)
   iii) address and/or email address
   iv) date of birth (if the requester is a registrant)
j) Depending on the circumstances, the DPO may ask the applicant (or their representative) for further proof of identity or authority to act.
k) Where the DPO is otherwise satisfied as to the identity of the person making the request, it may elect to waive the requirement for the applicant to provide proof of identity.
l) The DPO will log the date that the request was received, and the applicant's identity confirmed. The date that a request becomes active will be the date that a valid request is made (i.e. subject to clarification and identity checks).
m) The DPO will aim to deal with all requests promptly and to respond within one month. Where this is not possible the team must within one month tell the applicant:
   i) that they are extending the response time for up to two months and the reasons why

ii) why they have decided not to respond to the request and that they can complain to the ICO or seek a judicial remedy.

n) The DPO will keep a record of their decision-making and respond to any requests by the applicant for a review of their decision.

o) It is a criminal offence for Staff to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure or accurate response to a person who has made a data subject rights request unless:
   i) the data would have been amended in any event; and/or
   ii) ETT reasonably believe that the individual is not entitled to receive the requested information in line with a valid exemption under the DPA.

p) We will consider the data held at the time a request was received. However, in many cases routine use of the data may result in it being amended while the request is being dealt with. We may therefore consider the information we hold as at the date of the response, even if this is different to that held when the request was received.

q) For some data subject rights requests, ETT may need to alter or erase data to comply with the request itself, this applies to the rights of erasure and rectification.

r) Once the relevant information has been located, the DPO will review the data prior to deciding on whichever data subject right has been exercised and will decide whether any exemptions apply or, if there are legitimate reasons why we are unable to action a request.

s) The subject access right is to information (i.e. personal data) and not to documentation. Accordingly, the DPO may extract the applicant's personal data from documentation or redact information, which is not the applicant's personal data when preparing the response. Where appropriate, the DPO may provide relevant contextual information to assist the applicant.

t) The DPA and UK GDPR set out several exemptions which may apply to data subject rights requests. We may be exempt from complying (in full or in part) with a request if:
   i) The information sought is classed as 'third party data' meaning that it is information about other individuals and not the requester.
   ii) We do not have the consent to release third party information, and it is not reasonable in the circumstances to disclose the data.
   iii) The disclosure of information or, granting an individual's request would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.
   iv) The disclosure of information or, granting an individual's request would prejudice our regulatory functions, or the functions of another regulator.
   v) The information contains legally privileged personal data.
   vi) Disclosure of information or, granting an individual's request would be likely to prejudice our negotiations with the data subject.
   vii) We are asked to erase data which we are required to process to comply with a legal obligation, for the performance a task carried out in the public interest or for reasons of public interest.
   viii) There is another applicable exemption in the DPA or, UK GDPR. Other reasons we may refuse a request.

ix) There are other reasons beyond the above exemptions which may result in us refusing a request in part or in full. In terms of the data subject rights of erasure, rectification, restriction of processing and objection, there are often legitimate reasons why we are unable to action the requested outcome. We're required by law to publish and retain certain personal information; therefore, this can result in us being unable to meet desired outcomes.

x) The DPO will usually respond to requests by email unless this is not possible or, another contact method has been specified by a requester.

xi) The DPO will state the decision as to disclosure or, whether we are granting or refusing a request. Clear reasons for any redactions, exemptions or, our reasons for refusing to grant a request. We will cite relevant sections of the DPA and UK GDPR in these circumstances.

xii) Any information we need to send to comply with a request will be attached.

xiii) Information about how an Internal Review can be requested along with contact details for the Information Commissioners Office (ICO).

xiv) ETT will, where appropriate, voluntarily review responses that applicants are not happy with, to resolve any complaint or dispute in a proportionate manner, this stage is called an Internal Review.

xv) Complaints about responses should be referred to the DPO.

xvi) The DPO will escalate to the Board of Trustees if the complaint cannot be resolved.

8) Archiving / removal

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 review 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.

9) 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) Breach

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, ETT shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

11) ESFA

a) Learner data will be shared with the 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

12) Contact

a) The DPO (Mark Vingoe) 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