EDUC8 TRAINING GROUP

Data Protection Policy 2026 - 27

Document version control

Document title:	Data Protection Policy
Document status:	Final
Version number:	1.5
Date:	16/09/2026
Author:	TON
Approved by:	Board
Review date:	September 2027

Educ8 Training Group Data Protection Policy

Contents:

Section	Section Title	Page
1	Introduction	3
2	Scope of Policy	3
3	Interpretations	3
4	Data Protection Principles	5
5	Lawfulness, fairness, transparency	6
6	Purpose limitation	7
7	Data minimisation	7
8	Accuracy	7
9	Storage limitation	7
10	Security integrity and confidentiality	8
11	Transfer limitation	8
12	Data subject's rights and requests	9
13	Accountability	10
14	Direct marketing	11
15	Sharing personal data	12
16	Changes to this privacy standard	12

1. INTRODUCTION

Educ8 Training Group ("ETG") is one of the largest independent training providers in England and Wales. All companies within the ETG group uphold the same company Vision, Mission and Core Values and follow our group policies and procedures.

At the date of this policy these companies are:

- Educ8 Training Group Limited, registered number 10865705.
- Haddon Training Limited, registered number 04773490.
- Aspire and Learn Ltd, registered number 08784755.
- Educ8 Ltd, registered number 05059754.

Any reference to "ETG" throughout this policy includes all the companies named above.

For the purpose of this policy the reference to "Funding Bodies" includes, but is not restricted to, the Welsh Government/Medr, DfE/DWP and local authorities.

1.1 This Policy or "Privacy Standard" sets out how ETG ("we", "our", "us", "the Company") handle the Personal Data of our customers, learners, suppliers, employees, workers and other third parties.

1.2 This Privacy Standard applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Privacy Standard when Processing Personal Data on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Any breach of this Privacy Standard may result in disciplinary action and, where Data Processors and Sub-Processors are concerned, termination of our relationship.

2. SCOPE

2.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Company and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

2.2 The DPO is responsible for overseeing this Privacy Standard DPO@educ8training.co.uk

2.3 Please contact the DPO with any questions about the operation of this Privacy Standard or data protection or if you have any concerns that this Privacy Standard is not being or has not been followed.

3. INTERPRETATION

For those who are not familiar with the terminology used under data protection laws, we have set out below a number of definitions of terms used in this policy.

3.1 **Automated Decision-Making (ADM):** A decision made solely by automated means, including profiling, without meaningful human involvement, which produces legal effects or similarly significant

effects on an individual.

ETG may use automated processing only where permitted by applicable data protection legislation and appropriate safeguards are in place. Where significant automated decisions are made, ETG will ensure individuals are provided with:

- information about the decision-making process;
- an opportunity to make representations;
- access to meaningful human intervention; and
- the right to challenge or contest the decision.

Additional restrictions apply where Special Category Personal Data is involved

3.2 **Automated Processing:** any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

3.3 **Company name:** Educ8 Training Group (ETG)

3.4 **Company Personnel:** all employees, workers, independent contractors, agency workers, consultants, directors, agents and others.

3.5 **Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

3.6 **Controller:** the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the Data Protection Act 2018 and UK GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

3.7 **Criminal Convictions Data:** means personal data relating to criminal convictions and offences.

3.8 **Data Subject:** a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

3.9 **Data Privacy Impact Assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

3.10 **Data Protection Officer (DPO):** the person required to be appointed in specific circumstances under the Data Protection Act 2018 and UK GDPR. This can be an individual or a company. The Company has appointed the Head of HR as the DPO DPO@educ8training.co.uk.

3.11 **Explicit Consent:** consent which requires a very clear and specific statement (that is, not just action).

3.12 **Applicable Data Protection Legislation:** means the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 (DUAA), the Privacy and Electronic Communications Regulations (PECR), and any legislation, statutory instruments, codes of practice or guidance issued by the Information Commissioner's Office (ICO) as amended from time to time. Personal Data is subject to the legal safeguards contained within these laws and regulations.

3.13 **Personal Data:** any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

3.14 **Personal Data Breach:** any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

3.15 **Privacy by Design:** implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the Data Protection Act 2018 UK GDPR.

3.16 **Privacy Policies or Privacy Notices:** separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or a learner privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

3.17 **Processing or Process:** any activity that involves the use of Personal 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 transmitting or transferring Personal Data to third parties.

3.18 **Pseudonymisation or Pseudonymised:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

3.19 **Special Categories of Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

4. DATA PROTECTION PRINCIPLES

4.1 We adhere to the principles relating to Processing of Personal Data set out in the Data Protection Act 2018 and UK GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).
(b) Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (**Data Minimisation**).
(d) Accurate and where necessary kept up to date (**Data Accuracy**).
(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (**Storage Limitation**).
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).
(g) We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

Lawful and fair processing

5.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The Data Protection Act 2018 and UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.3 The UK GDPR permits processing where one or more of the following lawful bases apply:

(a) the Data Subject has given Consent;
(b) processing is necessary for the performance of a contract with the Data Subject;
(c) processing is necessary to comply with a legal obligation;
(d) processing is necessary to protect the vital interests of an individual;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
(f) processing is necessary for the legitimate interests pursued by ETG or a third party, except where those interests are overridden by the rights and freedoms of the Data Subject.

ETG will identify, document and retain evidence of the lawful basis relied upon for each processing activity.

Consent

5.4 Where Consent is the lawful basis for processing, we recognise that under the Data Protection Act 2018 and GDPR, there are stricter rules about how this is obtained. If we do need to obtain Consent, we will ensure that:-

(a) the Data Subject either by a statement or positive action gives their consent.
(b) consent is not inferred by silence.
(c) pre-ticked boxes are not used as a means of obtaining consent.
(d) consent is separated from other documents such as terms and conditions or contracts.

(e) data subjects are able to withdraw Consent to Processing at any time.

5.5 The above rules ensure that Data Subjects give their Consent freely, understand what they are Consenting to and can change their mind should they wish to do so.

5.6 We will keep appropriate records evidencing how we obtain Consent.

Transparency (notifying data subjects)

5.7 The Data Protection Act 2018 and UK GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6. PURPOSE LIMITATION

6.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

6.2 We will not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

7. DATA MINIMISATION

7.1 We will ensure that the Personal Data which we process is adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. We will achieve this in the following ways: -

a) Personnel will only Process Personal Data when performing job duties which require its use.
b) Personnel will not collect excessive data by only processing data that is necessary to complete a task.
c) When we no longer require the data, we will delete it in accordance with our retention procedures.

8. ACCURACY

8.1 We will take all reasonable steps to ensure that Personal Data that we hold is accurate and, where necessary, kept up to date. Where we identify inaccuracies, we will correct or delete it without delay.

8.2 We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards.

9. STORAGE LIMITATION

9.1 We recognise that Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

9.2 We will maintain retention policies and procedures to ensure Personal Data is deleted after a

reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

9.3 We will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with our records retention schedules and policies.

10. SECURITY INTEGRITY AND CONFIDENTIALITY

Protecting Personal Data

10.1 We recognise that Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

10.2 We will develop, implement and maintain safeguards to ensure that Personal Data which we process is kept secure and confidential. We will evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

10.3 Personnel will follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

10.4 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) **Confidentiality** means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) **Integrity** means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users are able to access the Personal Data when they need it for authorised purposes.

Reporting a personal data breach

10.5 The Data Protection Act 2018 and UK GDPR requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

10.6 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

10.7 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. You must immediately contact the DPO if you suspect a breach. You should preserve all evidence relating to the potential Personal Data Breach.

11. INTERNATIONAL TRANSFERS

11.1 ETG recognises that UK data protection law places restrictions on the transfer of Personal Data

outside the United Kingdom where such transfers may reduce the level of protection afforded to individuals.

11.2 ETG will only transfer Personal Data internationally where one of the following applies:

a) The destination country is covered by UK adequacy regulations;

b) Appropriate safeguards are in place, including:

- the UK International Data Transfer Agreement (IDTA);
- the UK Addendum to the EU Standard Contractual Clauses;
- Binding Corporate Rules (BCRs);
- an approved code of conduct; or
- an approved certification mechanism;

c) A valid exception under applicable data protection legislation applies.

11.3 Where required, ETG will complete and document an International Transfer Risk Assessment or equivalent assessment before transferring Personal Data internationally.

11.4 All international transfers must be approved in accordance with ETG's Data Protection and Information Governance arrangements.

12. DATA SUBJECT'S RIGHTS AND REQUESTS

12.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;
(b) receive certain information about the Data Controller's Processing activities;
(c) request access to their Personal Data that we hold;
(d) prevent our use of their Personal Data for direct marketing purposes;
(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
(f) restrict Processing in specific circumstances;
(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
(i) object to decisions based solely on Automated Processing, including profiling (ADM);
(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
(l) make a complaint to the supervisory authority; and
(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

12.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

12.3 You must immediately forward any Data Subject request you receive to the DPO.

12A. Data Protection Complaints

12A.1 Individuals have the right to raise concerns or complaints regarding the way ETG collects, uses, stores, shares or otherwise processes Personal Data.

12A.2 Complaints may be submitted through any reasonable communication channel, including email, written correspondence, telephone, website forms or directly to ETG personnel.

12A.3 ETG will:

- acknowledge complaints within 30 days of receipt;
- investigate complaints appropriately and without undue delay;
- keep complainants informed of progress where appropriate;
- communicate the outcome of the complaint without undue delay; and
- maintain records of complaints and actions taken.

12A.4 Individuals retain the right to complain to the Information Commissioner's Office (ICO) at any stage.

12A.5 All employees must immediately forward any data protection complaint to the Data Protection Officer.

13. ACCOUNTABILITY

Processing of Special Category and Criminal Offence Data

ETG recognises that Special Category Personal Data and Criminal Offence Data require additional protection.

Where such information is processed ETG will ensure:

- a valid Article 6 lawful basis exists;
- an appropriate Article 9 condition is identified where Special Category Data is processed;
- an appropriate legal condition exists where Criminal Offence Data is processed;
- access is restricted on a need-to-know basis;
- retention periods are defined and documented;
- additional security measures are implemented where appropriate.

Processing activities involving Special Category Data or Criminal Offence Data may require a Data Protection Impact Assessment before processing begins

13.1 The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

13.2 The Company must have adequate resources and controls in place to ensure and to document Data Protection Act 2018 and UK GDPR compliance including:

(a) appointing a suitably qualified DPO or data protection manager;
(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Privacy Standard, or Privacy Policies;
(d) regularly training Company Personnel on the Data Protection Act 2018 and UK GDPR, and
(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement efforts.

13.3 The Data Protection Act 2018 and UK GDPR requires us to keep full and accurate records of all our data Processing activities.

13.4 These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

Training

13.5 We will provide Personnel with appropriate and relevant training to enable them to comply with data privacy laws.

Privacy by design and data protection impact assessment (DPIA)

13.6 We will implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with the data protection principles.

13.7 We will conduct DPIAs in respect of high risk Processing. In particular, we will conduct a DPIA when implementing a major system or change programs involving the Processing of Personal Data.

13.8 The DPO will be consulted when carrying out a DPIA. The DPIA will include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate.
(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose.
(c) an assessment of the risk to individuals; and
(d) the risk mitigation measures in place and demonstration of compliance.

14. DIRECT MARKETING

14.1 We are subject to certain rules and privacy laws when marketing to our customers and clients.

14.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

14.3 The right to object to direct marketing will be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

14.4 A Data Subject's objection to direct marketing will be promptly honoured. If a customer opts out at any time, their details will be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

15. SHARING PERSONAL DATA

15.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

15.2 You may only share the Personal Data we hold with another employee, agent or representative of our Company if the recipient has a job-related need to know.

15.3 You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;
(b) sharing the Personal Data complies with the Privacy Policy provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
(d) the transfer complies with any applicable cross border transfer restrictions; and
(e) a fully executed written contract that contains Data Protection Act 2018 and UK GDPR approved third party clauses has been obtained.

16. CHANGES TO THIS PRIVACY STANDARD

We reserve the right to change this Privacy Standard at any time and will communicate any changes to you accordingly.