



DATA PROTECTION POLICY

Document control

Audience	Internal colleagues, External colleagues, Customers, External Quality Assurance bodies and regulators
Application	This policy applies to all Achieve+Partners personnel and bodies that work it
Version	2026.1
Published	September 2026
Document status	Published
Responsibility	The Managing Director is accountable for ensuring the implementation of this policy. The Operations Director is responsible for carrying out the requirements of this policy. The Operations Director is the Achieve+Partners Data Protection Officer.

Document change record

Changes to specific sections of the document are listed below:

Page	Section	Change
2		Added definitions
		Updated throughout to reflect new terminology and strengthen policy.



SECTION 1: POLICY AND PRIVACY STANDARD

Introduction

Achieve+Partners takes its responsibilities with regard to the management of the requirements of the Data Protection 1998 Act very seriously. This policy sets out how Achieve+Partners manages those responsibilities.

Purpose

This Policy sets out how Achieve+Partners ("we", "our", "us", "the Company") handle the Personal Data of our learners, customers, suppliers, employees, consultants, workers and other third parties.

This policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees and learners, workers, candidates, clients or supplier contacts, shareholders, website users or any other Data Subject.

Scope

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

All Directors are responsible for ensuring all Company Personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure that compliance.

The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines.

Achieve+Partners Limited is a professional awarding body and end-point assessment organisation and is registered as a data user with the Data Protection Registrar.



Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

- + Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
- + Collected only for specified, explicit and legitimate purposes (Purpose Limitation);
- + Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
- + Accurate and where necessary kept up to date (Accuracy);
- + 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);
- + 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);
- + Not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and
- + Made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

Lawfulness, fairness, transparency

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

We only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The 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.

The GDPR allows Processing for specific purposes, some of which are set out below:

- + The Data Subject has given his or her Consent;
- + The Processing is necessary for the performance of a contract with the Data Subject;
- + To meet our legal compliance obligations;
- + To protect the Data Subject's vital interests;



- + To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices; or
- + You must identify and document the legal ground being relied on for each Processing activity in accordance with the Company's guidelines on Lawful Basis for Processing Personal Data.

Consent

A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

When processing Special Category Data or Criminal Convictions Data, we rely on a legal basis for processing.

Employees and contractors

All Company Personnel must comply with this policy when Processing Personal Data on our behalf and attend training on its requirements.

Arrangements

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. The following arrangements are in place to ensure that the various types of data Achieve+Partners holds is protected.

Applications

Data from all applications made to Achieve+Partners for advertised job roles including directors, employees, consultants, examination markers, question setters, committee members and independent assessors is kept securely and will be kept no longer than necessary. The information is used for Achieve+Partners to create a computer record of the application and to enable the application to be processed and to monitor fair access information.

Employee information

Achieve+Partners holds data in relation to its employees for the period of time that individual is in employment. Data includes personal information, payroll, training records, declarations, performance management records, DBS certificate information and other related information. This information is held



securely with restricted access. The employee can access or request access to this information at any time. Payroll and counts information are held securely on the company online accounts software. Access is restricted to the accountant and senior management team.

Once an employee leaves the business all sensitive personal data will be destroyed. A record of the employee will be held for a period of 5 years.

Contractor information

Achieve+Partners holds data in relation to its contractors for the period of time that individual is contracted. Data includes personal information, training records, performance management records, DBS certificate information, CV, Qualification certificate copies and declarations made to confirm conflicts of interest. This information is held securely with restricted access.

Once a contractor ceases work with the business all sensitive personal data will be destroyed. A record of the contractor will be held for a period of 5 years.

Learner data

Achieve+Partners collects, stores and processes personal data about learners for the purpose of administrating and managing apprenticeship end-point assessment. Achieve+Partners will continue to hold data electronically after a learner has finished the apprenticeship for a period of 10 years. Our Lawful Basis for processing this information is legitimate interest for the purpose of administrating and managing apprenticeship end-point assessment. Paper copies will be electronically scanned before being securely destroyed within 1 month of receipt.

This information may be disclosed to the Office of Qualifications and Examination Regulations (Ofqual), Education & Skills Funding Agency (ESFA) and other government and educational organisations potential employers and other relevant organisations where necessary for the fulfilment of obligations.

Learner assessment materials

Paper versions of Learners' examination answer books and other assessment materials, which have been submitted to and marked by Achieve+Partners, will be kept for a maximum period of 1 year, ideally these will be returned to the learner on completion of marking. This information can only be identified by a unique



learner number. Where this data is stored electronically as part of the learners' record Achieve+Partners will continue to hold data electronically after a learner has finished the apprenticeship for a period of 10 years.

Assessor learner information and assessment materials

Learners' details, assessment outcomes and recordings of assessments (paper, electronic and voice recordings) and any other assessment materials, which have been submitted to and quality assured by Achieve+Partners must be securely deleted/destroyed by the Independent Assessor 10 days after the assessment has been completed. Our Lawful Basis for processing this information is legitimate interest for the purpose of administrating and managing apprenticeship end-point assessment.

Customer information

Customer application information (e.g. signed agreements, staff and qualification approval applications) are kept as electronic copies for the period that a customer is working with Achieve+Partners, they are then archived and stored for a further 3 years. Paper copies will be electronically scanned before being securely destroyed within 1 month of receipt. Our Lawful Basis for processing this information is legitimate interest for the purpose of administrating and managing apprenticeship end-point assessment.

This information may be disclosed to the Office of Qualifications and Examination Regulations (Ofqual), Education & Skills Funding Agency (ESFA) and other government and educational organisations, and other relevant organisations where necessary for the fulfilment of obligations.

Customer personnel

Achieve+Partners collects, stores and processes personal data about customers employees. This is kept as an electronic copy for the period that a customer is working with Achieve+Partners they are then archived and stored for a further 3 years. Paper copies will be electronically scanned before being securely destroyed within 1 month of receipt. The information is kept securely and will be kept no longer than necessary. Our Lawful Basis for processing this information is legitimate interest for the purpose of administrating and managing apprenticeship end-point assessment.

Marketing and communications

Personal data including names, emails, employer and telephones is held by Achieve+Partners for marketing and sales purposes, this includes, for example, electronic newsletters, enquiries and event bookings.



Our Lawful Basis for processing this information is consent.

All marketing contacts are asked to positively opt-in and may withdraw their consent at any time without detriment. Achieve+Partners will review consent bi-annually and will keep records of when and how we received consent.

All sales contacts are asked to positively opt-in and may withdraw their consent at any time without detriment. Achieve+Partners will review consent bi-annually and will keep records of when and how we received consent.

Achieve+Partners has provided details on the terms of use and use of cookies on the website. Both of these documents can be found under the Policies tab at achievepartners.co.uk.

Data security

Personal Data is secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

Achieve+Partners data is held securely electronically with access for those Achieve+Partners employees needing to use the data. When data is no longer required it will be securely deleted or destroyed, as appropriate.

Confidentiality

Achieve+Partners employees are fully aware of the confidential nature of much of their work and confidentiality is an element of the standard contract of employment a breach of which is considered to be gross misconduct.

During the time anyone working with Achieve+Partners or with any of its agencies and stakeholders as part of their duties, may have access to confidential information that can identify a learner, another member of staff and/or business in confidence information about the Company.

This type of information should not be disclosed to any person outside of the normal working environment, particularly non-employees. If there is a need to disclose/share confidential information in pursuit of



working duties, permission will be granted to do this by the Responsible Officer, and this will be done so within legal and regulatory requirements.

Withdrawal of consent

Where consent to hold someone's personal data for marketing or sales purposes is withdrawn the Operations Director is responsible for ensuring that all personal data held for that person is deleted and all Achieve+Partners employees will be asked to do the same. This will be completed within 15 working days of the receipt of the request.

Accuracy of Data - Right to Rectification

Achieve+Partners takes all reasonable steps to ensure accuracy of personal information held. Where this is not the case requests to update personal data must be made in writing to info@achievepartners.co.uk. Achieve+Partners will acknowledge receipt of the request within 5 working days and aims to confirm that the data is accurate and to rectify the data, if necessary, within 28 days.

Request to access personal data Achieve+Partners holds

Requests must be made in writing to info@achievepartners.co.uk. A report on all personal data information that Achieve+Partners holds will be emailed to the requester. Achieve+Partners will acknowledge receipt of the request within 5 working days and aims to complete the request within 28 days.

Maintaining confidentiality of assessment materials

Where confidentiality in:

- a) the contents of assessment materials, or
- b) information about the assessment,

is required in order to ensure that an apprenticeship assessment which an awarding organisation makes available, or proposes to make available, reflects an accurate measure of attainment, Achieve+Partners will take all reasonable steps to ensure that such confidentiality is maintained.

Achieve+Partners will:

- + take all reasonable steps to ensure that such confidentiality is maintained where it (or any person connected or previously connected to Achieve+Partners) provides training or training materials in relation to assessments and qualifications,



- + not provide or endorse any prohibited training, and
- + take all reasonable steps to ensure that any person connected or previously connected to it does not provide or endorse any prohibited training. 'Prohibited training' is training:
 - provided to assessors, coaches, teachers in relation to such a qualification,
 - at which a number of persons are present (whether physically or remotely by means of simultaneous electronic communication),
 - where any one of those persons holds information in relation to the content of assessment materials or information about the assessment for that qualification, and
 - where disclosure of the information to assessors, coaches, teachers would breach such confidentiality.

Achieve+Partners will, in respect of any training it provides to assessors, coaches, teachers in relation to such a qualification (and, in relation to any such training provided by any person connected to Achieve+Partners will take all reasonable steps to) –

- + ensure that the training is reasonably available to all assessors, coaches, teachers preparing Learners, or persons likely to become Learners, for assessments for that qualification,
- + advertise to assessors, coaches, teachers the availability of the training, including in particular by publishing details of the training, and
- + publish the content of any training materials which have been provided to assessors, coaches, teachers in connection with the training, as soon as reasonably practicable after the training has been held.

Achieve+Partners will take all reasonable steps to ensure that no person connected to it, or previously connected to it, offers to disclose information about any assessment or the content of any assessment materials where that information is (or is said or implied to be) confidential.

Where any breach of such confidentiality (including through the loss or theft of confidential assessment materials) is either suspected by Achieve+Partners or alleged by any other person and where there are reasonable grounds for that suspicion or allegation, Achieve+Partners will:

- + investigate that breach,
- + ensure that such an investigation is carried out rigorously, effectively, and by persons of appropriate competence who have no personal interest in its outcome, and
- + so far as possible, establish whether or not a breach of such confidentiality has occurred.



Monitoring and review

This policy is monitored by the Achieve+Partners senior management team to ensure that it remains current with legislative amends and/or changes. The policy is formally reviewed annually and updated accordingly.

The Information Officer is responsible for the update and accuracy of the policy on behalf of the senior management team.



Definitions

Company Personnel:	all employees, workers contractors, agency workers, consultants, directors, members and others.
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.
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 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.
Criminal Convictions Data:	means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.
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.
Data Protection Officer (DPO):	the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.
EEA:	the 28 countries in the EU, and Iceland, Liechtenstein and Norway.
Explicit Consent:	consent which requires a very clear and specific statement (that is, not just action).
General Data Protection Regulation (GDPR):	the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.
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.



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.
Privacy by Design:	implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.
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.
Related Policies:	the Company's policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data.
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, and Personal Data.