**Data Protection Policy**

**INTRODUCTION**

This Data Protection Policy outlines the principles and procedures of ATS in handling personal data in compliance with relevant data protection laws, including the UK Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR).

As an independent training provider, we are committed to safeguarding the privacy and rights of individuals whose personal data we collect and process, including our learners, employees, and partners.

**SCOPE**

This policy applies to all personal data processed by the Provider in relation to:

* Learners (prospective, current, and former)
* Employees, contractors, and freelance trainers
* External partners, suppliers, and stakeholders
* Website visitors and users of online training platforms

All staff, contractors, and stakeholders who have access to personal data must comply with this policy.

**KEY DEFINITIONS**

* **Personal Data**: Any information that relates to an identified or identifiable individual.
* **Processing**: Any action taken in relation to personal data, including collecting, storing, altering, using, disclosing, or erasing data.
* **Data Subject**: An individual whose personal data is processed.
* **Data Controller**: The entity that determines the purposes and means of processing personal data. The Provider acts as the Data Controller for all personal data processed.
* **Data Processor**: An entity that processes personal data on behalf of the Data Controller.

**PRINCIPLES OF DATA PROTECTION**

ATS follows the core principles of data protection outlined in the GDPR:

1. **Lawfulness, Fairness, and Transparency**: Personal data will be processed lawfully, fairly, and in a transparent manner.
2. **Purpose Limitation**: Personal data will only be collected for specified, explicit, and legitimate purposes.
3. **Data Minimisation**: Personal data will be adequate, relevant, and limited to what is necessary for processing.
4. **Accuracy**: Personal data will be accurate and kept up to date.
5. **Storage Limitation**: Personal data will not be kept for longer than is necessary.
6. **Integrity and Confidentiality**: Personal data will be processed securely, ensuring protection against unauthorised or unlawful access, processing, loss, destruction, or damage.

**LEGAL BASIS FOR PROCESSING**

The Provider ensures that it has a valid legal basis for processing personal data. The following are the primary lawful bases used:

* **Consent**: Where the data subject has given clear consent for processing.
* **Contractual Necessity**: Where processing is necessary for the performance of a contract.
* **Legal Obligation**: Where processing is required by law.
* **Legitimate Interests**: Where processing is necessary for the legitimate interests of the Provider or a third party, provided that those interests are not overridden by the individual’s rights.

**DATA COLLECTION AND USAGE**

**LEARNERS**

Personal data collected may include contact details, identification information, course enrolment details, attendance records, assessments, and certification results. This data will be used for:

* Course administration and delivery
* Attendance monitoring
* Assessment and grading
* Issuing certificates
* Communicating with learners

**EMPLOYEES AND CONTRACTORS**

We collect and process personal data related to employment and contractual relationships, including contact details, payroll information, performance evaluations, and disciplinary records. This data is processed for:

* Employment administration (e.g., payroll, benefits)
* Contract management
* Legal compliance (e.g., tax and employment law)
* Staff performance and professional development

**SUPPLIERS AND PARTNERS**

Personal data from external partners and suppliers, such as contact information and financial details, may be processed for contract management, invoicing, and legal compliance.

**WEBSITE VISITORS**

We collect data such as cookies and IP addresses from website visitors to improve user experience and for analytics purposes, in compliance with applicable laws.

**DATA SHARING**

ATS may share personal data with third parties only under the following circumstances:

* **With Consent**: When we have obtained explicit consent from the data subject.
* **Legal Requirements**: When required by law, such as regulatory reporting or responding to legal requests.
* **Service Providers**: With third-party service providers who process data on our behalf, ensuring they follow strict data protection standards.
* **Partners**: In some cases, we may share learner data with external accreditation bodies or funding organisations.

**DATA SECURITY**

We implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. These include:

* Password-protected systems and encrypted devices
* Regular data protection training for staff
* Secure storage of physical documents
* Regular audits of our data protection processes

**DATA RETENTION**

ATS will not retain personal data for longer than necessary. Retention periods depend on the purpose of data collection and legal requirements. For example:

* Learner data will be retained for a minimum of 7 years post-completion of the course for regulatory reasons.
* Employee data will be retained for the duration of employment and 7 years afterward.

**DATA SUBJECT RIGHTS**

Data subjects have the following rights concerning their personal data:

* **Right of Access**: To request access to their personal data.
* **Right to Rectification**: To request correction of inaccurate data.
* **Right to Erasure**: To request deletion of their personal data under certain conditions.
* **Right to Restrict Processing**: To request limitation of processing in certain cases.
* **Right to Data Portability**: To request the transfer of their personal data to another service provider.
* **Right to Object**: To object to processing based on legitimate interests or direct marketing.
* **Right to Withdraw Consent**: To withdraw consent at any time when consent is the basis for processing.

Data subject requests can be made by contacting our Data Protection Officer (DPO).

**DATA BREACHES**

In the event of a data breach, we will take immediate steps to contain the breach and mitigate its impact. If the breach poses a high risk to data subjects’ rights and freedoms, we will notify the Information Commissioner’s Office (ICO) within 72 hours and affected individuals without undue delay.

**DATA PROTECTION OFFICER (DPO)**

James Trowman has been appointed as the Data Protection Officer for the Provider and is responsible for overseeing compliance with this policy and data protection laws. The DPO can be contacted at:

info@aaeg.co.uk

**TRAINING AND AWARENESS**

All employees, contractors, and relevant third parties will receive regular training on data protection practices to ensure understanding of their responsibilities under this policy.

**MONITORING AND REVIEW**

This policy will be reviewed regularly, at least annually, and updated in line with changes in the law or our operational practices. Changes will be communicated to all relevant parties.

**Signed**:
James Trowman

Director
October 2024

This policy ensures that ATS upholds the highest standards of data protection and complies with all relevant legal obligations.