Data Protection Policy

1. Purpose

The purpose of this policy is to set out the relevant legislation and to describe the steps the Association of Apprentices (AoA) is taking to ensure that it complies with it.

2. Scope of this policy

This policy applies to all systems, people and data processing activities that constitute AoA's information systems, including staff or contractors, who have access to AoA's systems.

3. Data Protection legislation

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (2018) are the most significant pieces of legislation affecting the way that AoA carries out its information processing activities. Significant fines can be imposed by the Information Commissioner's Office (ICO) if a breach is deemed to have occurred under the UK GDPR, which is designed to protect the personal data of citizens of the United Kingdom. It is AoA's policy to ensure compliance with all UK Data Protection legislation, is clear and demonstrable at all times.

4. Data Protection objectives

AoA places emphasis and priority on the protection of personal data, held under its auspices, at all times. It is our objective to implement all reasonable measures to ensure our processes and systems are robust and secure and that any staff or contractors working on behalf of the company are adequately trained and aware of our data protection standards and information security requirements in general.

AoA is committed to being transparent about how it collects and uses the personal data of individuals, and in meeting its data protection obligations.

5. Definitions

There is a total of 26 definitions listed within the UK GDPR and it is not appropriate to reproduce them all here. The most fundamental definitions with respect to this policy are as follows:

5.1 'Personal data' is defined as:

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an*

online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

5.2 'Special categories of personal data' means:

information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

5.3 '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.

5.4 '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.

6. Principles relating to processing of personal data

There are six fundamental principles upon which the UK GDPR is based.

AoA commits to the following:

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

AoA must ensure that it complies with all these principles both in the processing it carries out and as part of the introduction of new methods of processing such as new IT systems.

7. Rights of the individual

The data subject has rights under the UK GDPR. These are:

- The right to be informed (Article 14)
- The right of access (Article 15)
- The right to rectification (Article 16)
- The right to erasure (Article 17)
- The right to restrict processing (Article 18)
- The right to data portability (Article 20)
- The right to object (Article 21)
- Rights in relation to automated decision making and profiling (Article 22)

Each of these rights must be supported by appropriate procedures within AoA that allow the required action to be taken within the timescales stated in the UK GDPR. The timescale for all data subject requests is one month, however this can be extended if the request is sufficiently complicated. The one-month period begins when AoA have confirmed the identity of the data subject.

Subject access requests will be processed free of charge unless there is repeated or excessive requests in which case a nominal fee will be charged to the subject per request.

Individuals must exercise these rights at any time by submitting an email request in writing to a registered AoA email address. If an individual attempts to make a request via the telephone, then they will be asked to confirm the request in writing via email.

In responding to a subject access request where personal data is requested to be provided to a subject, AoA will always provide the personal data in a secure electronic

format including but not limited to the following file formats: CSV, Word, Excel, PDF, MSG, ZIP, JPG, EML. The information should be accompanied by an index of documents which will be numbered for reference accordingly.

All digital information will be provided to the subject in a compressed ZIP file format which will be encrypted, and password protected. The ZIP file will be electronically transmitted to the subject and the password will be communicated to the subject via alternative means such as verbally communicated over the telephone or via SMS message.

Personal data will only be provided to the subject in paper format if explicitly requested.

8. Consent

Unless it is necessary and only for a reason allowable in the UK GDPR, consent must be obtained from a data subject to collect and process their data.

Although AoA does not process the data of minors, in the event that it is required to do so, personal data relating to children below the age of 13 requires parental consent to be obtained prior to collection. Transparent information about our usage of minor's personal data must be provided to data subjects at the time that consent is obtained, and their rights explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

9. Privacy by design

AoA will adopt the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of data protection impact assessments (DPIAs) if applicable.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation
- Use of techniques such as data minimisation and pseudonymisation will be considered where applicable and appropriate.

10. Transfer of personal data

AoA will only transfer personal data outside of the UK and EEA if you register to be part of our community platform. In this event, we will share your name and email address with Mighty Networks, who are based in the US and operate the community platform on our behalf.

If we transfer data outside of the UK and EEA, and the third country is not deemed adequate, then we will ensure that an appropriate UK GDPR approved International Data Transfer Agreement (IDTA) is in any agreement with processors (and their sub-processors) as part of a due diligence process. If AoA is relying on IDTAs to transfer personal data to a third country, then we will conduct a Transfer Risk Assessment (TRA) to ensure that the third country has suitable controls to enable us to maintain the privacy of our exported personal data.

11. Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the UK GDPR if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

AoA have appointed a qualified Data Protection Officer Dougie Reid from Blenheim Chalcot who has been allocated responsibility for data protection activities and will act as an advisory in all such matters. He can be contacted on dpo@associationofapprentices.org.uk.

12. Breach notification

It is AoA's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the UK GDPR, where a breach is known to have occurred which is likely to result in a high-risk to the rights and freedoms of individuals, the relevant Data Protection Authority (DPA) will be informed within 72 hours.

Under the UK GDPR the relevant DPA, the ICO, has the authority to impose a range of fines for infringements of the regulations.

13. Addressing further compliance with the UK GDPR

The following actions are undertaken to ensure that AoA always complies with the accountability principle of the UK GDPR:

- The legal basis for processing personal data is clear and unambiguous
- A Data Protection Officer has been appointed with specific responsibility for data protection in the organisation
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- A written record of personal data processing activities is maintained
- Data Subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively

- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes

These actions will be reviewed on a regular basis as part of a management review process conducted alongside the management review of the information security management system.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this Policy or responding to subject access requests under this Policy, receive additional training to help them understand their duties and how to comply with them.

14. Ensure that records containing personal data are managed effectively

The organisation will seek to maintain standards of data quality and avoid duplication, inaccuracies and inconsistencies across personal data wherever possible.

AoA will maintain a records management procedure and records retention schedule which will be followed to help avoid excessive retention or premature destruction of personal data.

Personal data will be retained for a period suitable for processing or as required to meet statutory requirements. In most cases, where relevant, records will be kept for as long there remains a relationship in force or an employee is employed and then for the statutory retention period after.

15. Lawful basis

The lawful bases for processing personal information are set out in Article 6 of the UK GDPR. At least one of these must apply whenever we process your personal data:

- Consent (Article 6.1.a) the individual has given clear consent for you to process their personal data for a specific purpose;
- Contract (Article 6.1.b) the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract;
- Legal obligation (Article 6.1.c) the processing is necessary for you to comply with the law (not including contractual obligations);
- Vital interests (Article 6.1.d) the processing is necessary to protect someone's life.
- Public task (Article 6.1.e) the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law;
- Legitimate interests (Article 6.1.f) the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

The personal information we process is your name, email address, gender, date of birth, your home address and post code. For employees, we will additionally process your marital status, right to work documentation, references from previous employers, National Insurance Number, tax codes, bank account details, information relating to your employment with us, Next of Kin details, CV. We will only process your Personal Information using the Lawful Basis of Consent, or Consent, Contract and Legal Obligation for employees of the Association of Apprentices.

In addition to processing your personal information, we may collect and process Special Category data about you so that we can monitor equal opportunities. The Special Category data we may collect is information about your ethnicity and/or any disabilities you may have that affect your apprenticeship experience. One of the following conditions must apply for us to process your Special Category data:

- Explicit Consent (Article 9.2.a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- Employment, social security and social protection (Article 9.2.b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- Vital interests (Article 9.2.c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- Not-for-profit bodies (Article 9.2.d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union;
- Made public by the data subject (Article 9.2.e) processing relates to personal data which are manifestly made public by the data subject;
- Legal claims or judicial acts (Article 9.2.f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- Reasons of substantial public interest (Article 9.2.g) processing is necessary for reasons of substantial public interest;
- Health or social care (Article 9.2.h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Public health (Article 9.2.i) processing is necessary for reasons of public interest in the area of public health;
- Archiving, research and statistics (Article 9.2.j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

We would only process your Special Category information using the Lawful Basis of Explicit Consent.

16. Data retention and deletion

All personnel data will be stored for five years in accordance with statutory requirements, these and any variations are contained within the Record Retentions Schedule, supported by the Record Retention Policy.

17. Complaint handling

All complaints regarding data protection should be addressed in writing to dpo@associationofapprentices.org.uk

If you are not satisfied with any response from us, then you may contact the Information Commissioner's Office at:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline number: 0303 123 1113 https://ico.org.uk/global/contact-us/email/

Document Control

Version	Date	Author	Description	Review Date
0.1	29/04/22	Peter Stubley	Updated to include IDTAs and TRAs	29/04/23
0.2	24/05/22	Peter Stubley	Updated to include transfer of data to the US, and Special Category processing	
1.0	24/5/22	Emily Austin	Adopted	24/5/23
2.0	20/05/25	Dougie Reid	Reviewed	19/05/26