AXIS EDUCATIONAL TRUST(AET)

DATA PROTECTION POLICY

Policy Aims

AET is committed to being transparent about how it collects and uses the personal data of its members and its workforce, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

AET is committed to complying with data protection legislation and good practice including:

- Processing personal information only where this is strictly necessary for legitimate organisational purposes
- Collecting only the minimum personal information required for these purposes and not processing excessive personal information
- Providing clear information to individuals about how their personal information will be used and by whom
- Only processing relevant and adequate personal information
- Processing personal information fairly and lawfully
- Maintaining an inventory of the categories of personal information processed by AET
- Keeping personal information accurate and, where necessary, up to date
- Retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes
- Respecting individuals' rights in relation to their personal information, including their right of subject access
- Keeping all personal information secure

Responsibilities under the General Data Protection Regulation (GDPR)

- AET is a Data Controller and a Data Processor under the GDPR.
- Senior Management and all those in managerial or supervisory roles throughout AET are responsible for developing and encouraging good information handling practices within the organisation.
- A member of the senior management team is accountable to the Board of Directors for the management of personal information within AET and for ensuring that compliance with data protection legislation and good practice can be demonstrated.
- AET has a GDPR Owner who has been appointed to take responsibility for Axis Educational trust's compliance with this policy on a day-to-day basis.
- The GDPR Owner has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.
- Compliance with data protection legislation is the responsibility of all staff at AET who process personal information.

When you express interest in AET and book a free trial session, we will collect and process the following data from you:

- your name
- email address which will be used to send you a confirmation email
- contact telephone numbers which will be used to send you a confirmation SMS and confirmation call
- child's name, age, school and reason for interest in tuition

When you join AET, we will collect and process the following data from you:

- Parent/Guardian's name, postal and email address, contact phone numbers
- Membership payer's name, postal and email address, contact phone numbers (if not parent/guardian)
- Emergency contact's names and phone numbers
- Child/ren's name, age, date of birth and school
- Information about any medical conditions, allergies or Special Educational Needs of child/ren
- Details of Direct Debit and debit/credit cards in order for us to accept payment

Members should notify AET of any changes in circumstances to enable personal records to be updated accordingly.

What can I opt out of?

When you join AET, you have two consent options:

- You have the option of allowing us to use your child's photo for the purpose of promoting Explore Learning during and/or after your membership.
- You have the option of allowing us to share your data with external companies

Who will your personal information be shared with?

If we are obliged to disclose personal data by law, or if the disclosure is necessary for purposes of national security, taxation and criminal investigation or to safeguard your child, we will do so. In some circumstances, you may not be notified first.

Your data is hosted on several different systems. All these providers have relevant safeguards in place to protect your data in the same way that we do.

What happens with my data when my membership ends and how is it retained?

- Upon cancellation of membership, your data will be stored safely and securely. We will retain your personal data for a minimum of 2 years and a maximum of 3 years following cancellation of your membership to comply with relevant safeguarding bodies regulations.
- Accident/Incident reports and Administration of Medication records will be kept indefinitely.
- Registers of attendance will be kept for 3 years.

Data Protection Principles

All processing of personal data must be done in accordance with the following data protection principles of the Regulation, and Axis Educational trust's policies and procedures are designed to ensure compliance with them. These are:

1. **Personal data must be processed lawfully, fairly and transparently**
   The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the data subject in an intelligible form using clear and plain language.

   The specific information that must be provided to the data subject must as a minimum include:
   - the contact details of the Data Protection Officer, where applicable

- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- the period for which the personal data will be stored
- the existence of the rights to request access, rectification, erasure or to object to the processing
- the categories of personal data concerned
- the recipients or categories of recipients of the personal data, where applicable
- any further information necessary to guarantee fair processing

2. **Personal data can only be collected for specified, explicit and legitimate purposes**
   Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of Axis Educational trust's GDPR registration.
3. **Personal data must be adequate, relevant and limited to what is necessary for processing**
   - The GDPR Owner is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.
   - All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the GDPR Owner.
   - The GDPR Owner will ensure that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

4. **Personal data must be accurate and kept up to date**
   - Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
   - Members should notify AET of any changes in circumstance to enable personal records to be updated accordingly.
   - It is the responsibility of staff at AET to ensure that data held by AET is accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate at the date of submission.

5. **Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing**
   - Where personal data is retained beyond the processing date, it will be pseudonymised in order to protect the identity of the data subject in the event of a data breach.
   - Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

6. **Personal data must be processed in a manner that ensures its security**
   - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
   - These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.
   - Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.
   - The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.

7. **Accountability**
   The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR.
   Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs (Data Processing Impact Assessment), comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer if required.

8. Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- To request the ICO to assess whether any provision of the GDPR has been contravened.
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- The right to object to any automated profiling without consent.

9. Right to be forgotten

Data Subjects who wish to exercise their right to be forgotten can request this by contacting admin@tuitioncentres.org. However, due to our Ofsted/Care Inspectorate registration, we are required to keep the following data for 2 years following cancellation of membership:

- The name, home address and date of birth of each member
- The name, home address and telephone number of a parent/guardian of each member
- A daily record of the names of the children and their hours of attendance.

The right to be forgotten can be exercised after this 2 year period of non-membership. For any Data Subject who did not become a member of AET, a request for the right to be forgotten will be completed within 30 days.

10. Complaints

Data Subjects who wish to complain to AET about how their personal information has been processed may lodge their complaint directly with the GDPR Owner by email to admin@tuitioncentres.org

Data subjects may also complain directly to the supervisory authority.

11. Consent

Explore Learning understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

12. Security of data

All Employees/Staff are responsible for ensuring that any personal data which AET holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised to receive that information and has entered into a confidentiality agreement. Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/ Staff. Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day membership support, they should be archived. Personal data may only be deleted or disposed of in line with the Data Retention Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'.

13. Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held in electronic format and manual records which form part of a relevant filing system.

14. Disclosure of data

AET must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies. AET will only disclose and discuss personal data with the Primary contact. The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security
- prevention or detection of crime including the apprehension or prosecution of offenders
- assessment or collection of tax duty
- to protect the vital interests of the individual
- to safeguard our members including contact with local safeguarding boards

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the GDPR Owner.

Cookies

A cookie is a small text file that we store on your device. Our website uses cookies to distinguish you from other users of our website. Cookies also provide us with information about how this website is used so we can keep it as up to date, relevant and error-free as possible. Our use of cookies also allows registered users to be presented with a personalised version of the site, carry out transactions and have access to information about their account. Most browsers will allow you to turn off cookies. If you want to know how to do this, please look at the menu on your browser or look at the instruction on www.allaboutcookies.org. Please note however that turning off cookies will restrict your use of our website. Further information about the types of cookies that may be used on this website is set out in the list below.

- Strictly necessary cookies – these are cookies that are essential to the operation of our website
- Analytical/performance cookies. These cookies allow us to recognise and count the number of visitors to our website.
- Functionality cookies – These cookies are used to recognise you when you return to our website.
- Targeting Cookies – These cookies record your visit to our website, the pages you have visited and the links you have followed.
- We may monitor traffic to our site and collect the following information:
- The IP address of your computer
- The referring website from which you have got to our website from

The reasons for this are:

- To make ongoing improvements to our website based on this data
- To see our most popular sources of business
- To monitor and track the use of our member-only online services

Date: September 2020
Reviewed by: HG
Next Review Date: September 2022

AXIS EDUCATIONAL TRUST(AET)

PERSONAL DATA BREACH PROCEDURES

This procedure applies in the event of a personal data breach under Article 33 *Notification of a personal data breach to the supervisory authority,* and Article 34 *Communication of a personal data breach to the data subject* of the General Data Protection Regulation (GDPR).

Procedure – Breach Notification Data Processor to Data Controller

All of Axis Educational trust's Data Controllers will report any personal data breach to AET without undue delay and the GDPR Owner will record it on the Internal Breach Register.

Procedure – Breach Notification Data Controller to Supervisory Authority

AET will notify the supervisory authority of a personal data breach (ICO: Information Commissioner's Office) without undue delay. AET will assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach. If a risk to the aforementioned is likely, AET will report any personal data breach to the ICO without undue delay, and where feasible within 72 hours. Where data breach notification to the supervisory authority is not made within 72 hours, it shall be accompanied by the reasons for the delay.

The data controller shall provide the following information to the supervisory authority:

- A description of the nature of the breach
- The categories of personal data affected
- Approximate number of data subjects affected
- Approximate number of personal data records affected
- Likely consequences of the breach
- Any measures that have been or will be taken to address the breach, including mitigation
- The information relating to the data breach, which may be provided in phases

Procedure – Breach Notification Data Controller to Data Subject

Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, AET will notify the affected data subjects without undue delay.

- The notification to the data subject shall describe in clear and plain language the nature of the breach including the information specified above.
- Appropriate measures have been taken to render the personal data unusable to any person who is not authorised to access it, such as encryption.
- The controller has taken subsequent measure to ensure that the rights and freedoms of the data subjects are no longer likely to materialise.
- It would require a disproportionate amount of effort. In such a scenario there shall be a public communication or similar measure whereby the data subject is informed in an equally effective manner.