



# Data Protection Policy and Personal Data Breach Procedure

2026-27 revised edition

|                               |                                                                                                                |
|-------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Policy owner</b>           | Board of Trustees                                                                                              |
| <b>Approval status</b>        | Draft for Board approval                                                                                       |
| <b>Reviewed / updated</b>     | 3 October 2026                                                                                                 |
| <b>Next scheduled review</b>  | September 2027                                                                                                 |
| <b>Scope</b>                  | All AET operations in England and Wales                                                                        |
| <b>Earlier review trigger</b> | Relevant legal/regulatory change, serious incident, significant organisational change or identified deficiency |

This policy replaces the 2025 AET data protection policy and breach procedure. It is aligned with the UK GDPR and Data Protection Act 2018 as amended, including the Data (Use and Access) Act 2025 provisions in force by 19 June 2026.

## 1. Purpose

Axis Educational Trust (AET) is committed to using personal information lawfully, fairly, transparently and securely. This policy explains the standards AET applies when collecting, using, sharing, storing and deleting personal data, and the rights of individuals whose data AET processes.

## 2. Legal and regulatory framework

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018, as amended;
- Data (Use and Access) Act 2025 (DUAA);
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), where applicable to electronic marketing and cookies; and
- relevant ICO guidance and any sector-specific legal or safeguarding duties.

References in this policy to the UK GDPR include the UK data protection regime as amended from time to time.

### 3. Scope

This policy applies to trustees, employees, workers, volunteers, contractors and others who process personal data on behalf of AET. It covers personal data relating to children and young people, parents and guardians, staff and applicants, volunteers, donors, supporters, partners, suppliers, website users and other contacts.

AET will normally act as a data controller where it determines why and how personal data is processed. AET may act as a processor where it processes data solely on the documented instructions of another controller under an appropriate contract.

### 4. Governance and responsibility

- The Board of Trustees has overall responsibility for data protection governance and risk oversight.
- The Data Protection Lead (also referred to internally as the GDPR Owner) coordinates day-to-day compliance, advice, data subject requests, complaints and breach response.
- AET will appoint a statutory Data Protection Officer only where the legal criteria require one. If no DPO is required, AET will not use the title in a way that suggests a statutory appointment.
- All staff, trustees and volunteers who handle personal data are responsible for following this policy and completing appropriate training.
- Managers must ensure that new projects, systems, suppliers and data uses are reviewed for data protection risk before implementation.

Data protection contact: [admin@tuitioncentres.org](mailto:admin@tuitioncentres.org) (or any replacement address published by AET).

### 5. Data protection principles

AET will ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form no longer than necessary;
- processed with appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage; and
- handled in a way that allows AET to demonstrate compliance (accountability).

### 6. Personal data AET may collect

Depending on the service or relationship, AET may collect:

- names, addresses, email addresses and telephone numbers;
- child or young person details including date of birth, age, school, year group, attendance and educational information;
- parent/guardian, payer and emergency-contact information;
- health, allergy, disability, special educational need and safeguarding information where necessary;
- payment and transaction information (AET should avoid storing full payment-card details where a payment provider can process them securely);
- photographs, video or audio where there is an appropriate lawful basis and relevant permissions;
- staff, volunteer, trustee and applicant records, including recruitment, vetting and training information;
- donor, supporter and fundraising information;
- website, device, log and cookie information; and
- communications, enquiries, complaints, incidents and other records required to operate AET safely and effectively.

## 7. Lawful bases and special category data

Before processing personal data, AET will identify and document an appropriate lawful basis. Depending on the circumstances, this may include contract, legal obligation, legitimate interests, consent, vital interests or another basis available under law.

Special category data, such as health information, requires both an Article 6 lawful basis and an applicable additional condition under Article 9 UK GDPR and the Data Protection Act 2018. Criminal offence data will only be processed where an appropriate legal basis and safeguards exist.

Consent will only be relied on where it is freely given, specific, informed and unambiguous, and capable of being withdrawn. AET will not use consent where another lawful basis is more appropriate or where there is an imbalance that prevents consent from being genuinely optional.

## 8. Children and young people

AET recognises that children merit particular protection. Privacy information intended for children will be clear and age-appropriate. AET will collect only data necessary for education, safeguarding, administration and other stated purposes, and will apply enhanced care to photographs, health information, safeguarding records and online services.

Where consent is relied upon for an online service offered directly to a child, AET will apply the relevant UK rules on children's consent and will verify parental responsibility where required. In other contexts the appropriate lawful basis may not be consent.

## 9. Transparency and privacy information

AET will provide privacy information at or before the point personal data is collected, or within the statutory period where data is obtained from another source. Privacy notices will explain, as applicable, the controller identity and contact details, purposes and lawful bases, categories of data, recipients, international transfers, retention, rights, complaints routes and any relevant automated decision-making.

## 10. Sharing and disclosure

Personal data will only be shared where there is a lawful and necessary reason. Recipients may include service providers, professional advisers, funders where appropriately anonymised or authorised, education partners, safeguarding bodies, regulators, law-enforcement agencies and other organisations where the law permits or requires disclosure.

AET will use written data-processing terms with processors as required by Article 28 UK GDPR and will conduct proportionate due diligence on providers. Access will be limited to what each recipient needs.

Safeguarding information may be shared without consent where necessary and lawful to protect a child or another person. Staff must not delay a necessary safeguarding referral while seeking data-protection consent.

## 11. International data transfers

AET will not make a restricted transfer of personal data outside the UK unless the transfer is permitted under the UK GDPR. This may be because UK adequacy regulations apply or because AET uses an appropriate safeguard, such as the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, or another lawful mechanism. Where required, AET will complete a transfer risk assessment and implement supplementary safeguards.

## 12. Data quality, retention and secure disposal

AET will take reasonable steps to keep data accurate and will correct or update inaccurate information when identified. Individuals should tell AET when relevant contact or other details change.

AET will maintain a documented retention schedule based on the purpose of processing, legal and regulatory requirements, safeguarding needs, limitation periods, contractual requirements and organisational risk. Records will not be retained indefinitely merely because storage is available.

Where a particular regulated activity imposes a specific retention period, that requirement will be reflected in the retention schedule. At the end of the retention period, information will be securely deleted, anonymised or destroyed unless a documented reason justifies continued retention.

## 13. Information security

- role-based access and least-privilege permissions;
- strong authentication and appropriate password controls;
- secure configuration, patching, malware protection and backups;
- encryption or equivalent safeguards where proportionate;
- secure handling of paper records and confidential waste;
- screen locking and protection against unauthorised viewing;
- secure transfer methods for sensitive information;
- supplier and cloud-service due diligence;
- staff training on phishing, confidentiality and incident reporting; and
- prompt removal or adjustment of access when roles change or people leave.

Personal data must not be copied to personal accounts, unapproved apps or devices, or disclosed to unauthorised people. Any loss, mistaken disclosure, cyber incident or suspected compromise must be reported immediately to the Data Protection Lead.

## 14. Data protection by design and DPIAs

AET will consider privacy and security from the start of new projects and changes to systems. A Data Protection Impact Assessment (DPIA) will be carried out where processing is likely to result in a high risk to individuals, and may also be used as good practice for other significant projects. High residual risk that cannot be mitigated will be handled in accordance with ICO requirements before processing begins.

## 15. Individual rights

Subject to the conditions and exemptions in law, individuals may have rights to:

- be informed about processing;
- access their personal data;
- have inaccurate data rectified;
- have data erased in certain circumstances;
- restrict processing;
- receive portable data in certain circumstances;
- object to processing, including direct marketing; and
- receive safeguards in relation to significant decisions based solely on automated processing.

Requests should be sent to [admin@tuitioncentres.org](mailto:admin@tuitioncentres.org). AET will verify identity proportionately and respond within the statutory time limit. Rights are not absolute; where AET cannot fully comply it will explain the applicable reason unless the law prevents this.

## 16. Automated decision-making

Following the changes made by the Data (Use and Access) Act 2025, UK law permits a wider range of solely automated significant decisions where there is a valid lawful basis and required safeguards are in place. Additional restrictions continue to apply to special category data. Where AET uses solely automated processing to make a significant decision, it will identify the lawful basis, provide required transparency, and enable relevant safeguards such as obtaining human intervention, allowing the individual to express their point of view and enabling the decision to be contested where the law requires.

AET does not currently intend to make significant decisions about children solely by automated means without appropriate governance and safeguards.

## 17. Direct marketing and cookies

AET will comply with UK GDPR and PECR when sending electronic direct marketing. Where consent is required, it will be obtained before marketing is sent and withdrawal will be respected. Where a lawful soft opt-in or another permitted route applies, AET will still provide a clear opt-out.

Non-essential cookies or similar technologies will not be placed or accessed without the consent required by PECR. AET will maintain clear cookie information and a mechanism for users to manage preferences.

## 18. Data protection complaints procedure

AET will provide a clear way for individuals to complain about its use of personal data. Complaints may be sent to the Data Protection Lead at [admin@tuitioncentres.org](mailto:admin@tuitioncentres.org).

1. AET will acknowledge a data protection complaint within 30 days of receipt.
2. AET will investigate the complaint appropriately, including obtaining relevant records and speaking to appropriate staff where necessary.
3. AET will respond without undue delay, explain the outcome and any action taken or proposed, and keep a record of the complaint and response.
4. If a complainant remains dissatisfied, they may complain to the Information Commissioner's Office (ICO). AET will provide the relevant ICO information in its response where appropriate.

## 19. Personal data breach procedure

### 19.1 Immediate reporting and containment

Any person who becomes aware of an actual or suspected personal data breach must report it immediately to the Data Protection Lead and take safe steps to contain the incident without destroying evidence. Examples include sending information to the wrong recipient, loss or theft of a device or paper file, unauthorised access, ransomware, accidental deletion, or disclosure beyond the intended audience.

### 19.2 Assessment and breach register

The Data Protection Lead will record the incident in AET's breach register and assess the nature of the breach, categories and approximate numbers of people and records affected, sensitivity of the data, likely consequences, existing safeguards and mitigation undertaken.

### 19.3 Notification to the ICO

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, AET will notify the ICO without undue delay and, where feasible, within 72 hours after becoming aware of it. If notification is later

than 72 hours, AET will provide reasons for the delay. Where a breach is not reported, AET will document the assessment and reasons.

#### **19.4 Communication to affected individuals**

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, AET will communicate the breach to affected individuals without undue delay unless an applicable legal exception applies. Communications will be clear and will explain the nature of the breach, likely consequences, protective steps and a contact point for further information.

#### **19.5 Other reporting**

A significant data breach may also require consideration as a Charity Commission serious incident and may engage safeguarding, contractual, insurance or other regulatory reporting obligations. The Board will ensure these are considered promptly.

### **20. Training, monitoring and review**

- Relevant staff and volunteers will receive data protection and information-security training at induction and appropriate refreshers.
- AET will maintain appropriate records of processing, contracts, DPIAs, data-sharing arrangements, data breaches and significant rights requests.
- The Board and senior management will review significant data risks, incidents and recurring complaints and ensure lessons are implemented.
- This policy and related privacy notices will be reviewed at least annually and sooner where required.

### **21. Key legal and regulatory references**

- [ICO - Data \(Use and Access\) Act 2025: summary of changes](#)
- [ICO - Data protection complaints law and guidance](#)
- [ICO - International transfers: UK IDTA and Addendum](#)
- [Data Protection Act 2018](#)
- [Data \(Use and Access\) Act 2025](#)
- [Privacy and Electronic Communications Regulations 2003](#)

Reviewed by: Hakan Gokce