

## Data Protection Policy

### Summary policy statement

Ambitious about Autism/Ambitious about Autism Schools Trust looks after the information it holds about you and respects your privacy. We take appropriate security precautions to prevent your information being lost or falling into the wrong hands.

We make sure that the information we hold is as accurate as possible; we do not hold more information than we need; and we do not hold it longer than we need to.

We do not share your data with anyone else without your permission, except when we believe it is the only way to prevent harm to you or other people.

### Other policies to be referred to

- Data Security Policy
- Data Retention and Archiving Policy
- Confidentiality Policy
- Compliments and Complaints Policy
- Freedom of Information Act Policy (Ambitious about Autism Schools Trust)
- AaA and AaAST Purchasing Policies

### Full policy

#### Introduction and principles

This policy applies to the whole of Ambitious about Autism/Ambitious about Autism Schools Trust. It applies to all trustees, governors and workers, paid or unpaid, including employees, trainees, people on placement, temporary staff, interns, contractors and volunteers.

Ambitious about Autism/Ambitious about Autism Schools Trust processes personal data about employees, students, their parents, other service-users, donors and other stakeholders.

Ambitious about Autism/Ambitious about Autism Schools Trust are committed to good practice in the handling of personal data and careful compliance with the legal requirements of the Data Protection Act 2018 and the UK General Data Protection Regulation. Ambitious about Autism/ Ambitious about Autism Schools Trust aims above all to protect people from harm through data being misused, mismanaged or not being held securely.

Ambitious about Autism/Ambitious about Autism Schools Trust also ensures that it takes account of the legitimate concerns of individuals about the ways in which their data may be used. In particular, Ambitious about Autism/Ambitious about Autism Schools Trust aims to be open and transparent in the way it uses personal data and, where relevant, to give individuals a choice over what data is held and how it is used. Complaints can be made in line with our published Compliments and Complaints policy, or to the Information Commissioner's Office (ICO).

Ambitious about Autism/Ambitious about Autism Schools Trust has policies and procedures in place to ensure that it complies with the seven UK GDPR Principles set out in the Regulation:

- Lawfulness, fairness and transparency
- Purpose limitation (obtained for specified purposes and then only used for those purposes)
- Data minimisation (adequate, relevant and not excessive)
- Accuracy
- Storage limitation (not kept any longer than necessary)
- Integrity and confidentiality (kept securely)
- Accountability (take responsibility by having measures and records in place to demonstrate compliance)

Policy Owner	Director of Finance & Planning	Next Review Date:	December 2023
Policy No.	094	Version No.	1.1

The most important risks which this policy addresses are:

- Inappropriate disclosure of personal data about service users that puts an individual at personal risk or contravenes a duty of confidentiality;
- Negligent loss of data that would cause concern to people whose data was lost and would seriously affect the charity's reputation;
- Failure to follow good Data Protection practice in all areas of our work
- Failure to engage Data Processors on legally compliant terms.

Operational procedures and guidance to paid staff and volunteers set out more detailed ways in which these risks can be managed and the objectives achieved.

### **Responsibilities**

The Board of Trustees of Ambitious about Autism/Ambitious about Autism Schools Trust recognises its overall legal responsibility for Data Protection compliance.

Day to day responsibility for Data Protection is delegated to the Director of Finance and Planning as the nominated Data Protection Officer and the Data Protection Support Officer. The main responsibilities of the Data Protection Officer are:

- Briefing the Board of Trustees on their and Ambitious about Autism's/ Ambitious about Autism Schools Trust's Data Protection responsibilities, risks and issues;
- Reviewing Data Protection and related policies on a regular basis;
- Advising other staff on Data Protection issues;
- Ensuring that Data Protection induction and regular training takes place;
- Approving unusual or controversial disclosures of personal data;
- Approving contracts with Data Processors (external contractors and suppliers of outsourced services);
- Handling information security incidents;
- Notification (i.e. registration with the Information Commissioner); and
- Handling requests from individuals for access to their personal data.

Executive Leadership Team (ELT) members and managers have responsibility for data protection within their own area of operation. However, all employees and volunteers are responsible for ensuring information and data is maintained securely in accordance with this policy and procedures that apply to their area of work. All employees and volunteers have the following responsibilities:

- Assisting the Data Protection Officer in identifying aspects of their area of work which have Data Protection implications so that guidance can be provided as necessary;
- Ensuring that their activities take full account of Data Protection requirements including conditions for processing data, privacy and consent notices; and
- Engaging fully in Data Protection and confidentiality training.

The Head of IT is responsible for ensuring that all systems, services, software and equipment including cloud-based systems meet acceptable security standards.

### **Confidentiality, security and consequences for failing to comply**

Ambitious about Autism/Ambitious about Autism Schools Trust recognises that a clear policy on confidentiality of personal data – in particular that of service users – underpins security. It maintains a policy that sets out how staff and volunteers are authorised to access which data and for which purposes. We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

All staff and volunteers are required to abide by any security measures designed to protect personal data from loss, misuse or inappropriate disclosure.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

Policy Owner	Director of Finance & Planning	Next Review Date:	December 2023
Policy No.	094	Version No.	1.1

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Officer.

### Reporting breaches

All members of staff have an obligation to report actual, 'near miss' or potential data protection compliance failures at the earliest opportunity (within two hours). This allows the Data Protection Officer to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Information Commissioner of any compliance failures that are material either in their own right or as part of a pattern of failures
- Identify trends of compliance failures and address them accordingly through training, awareness-raising campaigns, or technical solutions

### Principles underlying operational procedures

Good Data Protection practice is, wherever relevant, incorporated into everyday operational procedures through the concept of Data Protection by Design and Default. These aim to include:

- Transparency, so that all the individuals about whom data is collected are made aware of the uses that Ambitious about Autism/Ambitious about Autism Schools Trust makes of information about them, and in particular to whom it may be disclosed;
- Informed consent, where necessary, especially in the case of service users;
- Good quality data, so that all the data held about individuals is accurate and can be justified as adequate, relevant and not excessive;
- Clear archiving and retention periods; and
- Security, proportionate to the risk of information being lost or falling into the wrong hands.

### Specific legal provisions

Ambitious about Autism/Ambitious about Autism Schools Trust maintains an up to date Notification with the Information Commissioner as required by law.

All contracts between Ambitious about Autism/Ambitious about Autism Schools Trust and external data processors are reviewed by the Data Protection Officer for compliance with UK GDPR requirements.

### General Data Protection Regulations (GDPR)

#### *Conditions for processing*

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. For processing under the legitimate interests condition we will assess using the three part purpose, necessity and balancing test, and keep a record of our Legitimate Interests Assessment (LIA). All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing, including legitimate interests where relevant, will be available to data subjects in the form of a privacy notice.

#### *Justification for personal data*

We will process personal data in compliance with all seven UK GDPR data protection principles.

We will document the additional justification for the processing of sensitive data.

#### *Consent*

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time, unless an exemption applies where consent is overridden by legal obligations, contractual terms, or special circumstances such as safeguarding concerns'

*Right to Access* Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Policy Owner	Director of Finance & Planning	Next Review Date:	December 2023
Policy No.	094	Version No.	1.1

*Right to be forgotten*

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

*Right to Rectification*

A data subject can, at any time and for any reason, request that information held about them is corrected or updated to be accurate and we must comply on any systems where that data may be present.

*Privacy by design and default*

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Data Protection Officer will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

*International data transfers*

No data may be transferred outside of the EEA without first discussing it with the Data Protection Officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

*Data audit and register*

Regular data audits to manage and mitigate risks will inform the Records of Processing Activities (ROPA). This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Policy Owner	Director of Finance & Planning	Next Review Date:	December 2023
Policy No.	094	Version No.	1.1