Data Protection Policy

Academy Transformation Trust

Review Date

February 2026

Ratified

March 2026

Next Review Date

February 2028

Responsible Directorate

Data Protection Officer

About ATT

Our Values

ATT2030 sets a values-driven culture that is explicit about how we work and lead:

Belonging & Becoming: we meet each child where they are and refuse to leave them there - giving them both roots and wings.

Integrity & Excellence: we act ethically, celebrate excellence, and pursue high standards in all that we do.

High Trust, High Accountability: decision-making sits close to pupils and communities; principals are trusted as strategic leaders; the central team acts as expert partner; accountability is professional, dialogic, and focused on learning and improvement.

Our Three Goals

Everything in ATT2030 is organised around three interlinked goals that describe the kind of people - pupils and adults - that we are forming:

Capable: equipped with the knowledge, skills, and emotional readiness to perform to a high standard, adapt to change, and contribute meaningfully.

Competent: possessing the knowledge, habits, and judgement to get things done – well, reliably, and independently – handling setbacks and making steady progress.

Confident: feeling safe, happy, and known – secure enough to take risks, speak up, and grow with purpose and integrity.

Contents

1.0 Policy Statement

1.1 Everyone has rights with regard to the way in which their personal data is handled.

1.2 During the course of our activities as an academy trust (Trust"), we will collect, store, and process personal data about our pupils, workforce, parents, and others. This makes us a data controller in relation to that personal data.

1.3 We are committed to the protection of all personal data and special category personal data.

1.4 The law imposes significant fines for failing to lawfully process and safeguard personal data. This policy sets out how we comply with the relevant legislation. Breaches of this policy can result in the risk of real harm to individuals, action for damages, loss of trust and reputational harm as well as regulatory penalties, including fines.

1.5 All data users must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action. Individuals may be prosecuted for committing offences under sections 170-173 of the Data Protection Act 2018.

2.0 About This Policy

2.1 The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the retained EU law version of the General Data Protection Regulation ((EU)2016/679) ('UK GDPR'), the Data Protection Act 2018, and other regulations (together 'data protection legislation') and the Data Use and Access 2025 We also process special category data, the trusts policy on Special Category Data can be found on the Trust website.

2.2 This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

3.0 Definition of data protection terms

3.1 All defined terms in this policy are indicated in bold text.

4.0 Data Protection Officer

4.1 As a Trust, we are required to appoint a data protection officer ("DPO"). Our DPO is Clare Plant, Director of People Strategy and they can be contacted at dpo@attrust.org.uk

4.2 The DPO is responsible for informing and advising the Trust about data protection legislation, ensuring compliance with the data protection legislation and with this policy. Any questions about the operation of this policy, or any concerns that the policy has not been followed should be referred in the first instance to the DPO. Each Academy has a Data Protection lead who is responsible along with the Principal for reporting any concerns raised at school level to the DPO.

4.3 The DPO is also the central point of contact for all data subjects, the Information Commissioner's Office ("ICO") and others in relation to matters of data protection.

4.4 Our data protection commitments

- We are dedicated to ensuring that personal data is processed in alignment with the legal principles of data protection.
- Our strategy is such that our systems and processes are designed to protect data by default and design.
- We can prove our adherence to data protection legislation.
- Data subjects are well informed about how and why we use their data, and they can exercise their rights regarding their data.
- We share personal data only when it is fair and lawful, ensuring that any data sharing is conducted securely.
- We handle and report all personal data breaches, including minor ones, effectively to mitigate any potential risks and to improve our practices.

5.0 Data protection principles

5.1 Anyone processing personal data must comply with the data protection principles. We will comply with these principles in relation to any processing of personal data by the Trust.

5.2 The principles provide that personal data must be:

- Processed fairly, lawfully, and transparently in relation to the data subject. This means that we only use personal data with respect for the individual who it relates to, in line with the legal grounds for processing, and we inform data subjects on how their personal data is processed including, among other ways, in our privacy notices.
- Processed for specified purposes and in a way which is not incompatible with those purposes. This means that if we collect personal data for one purpose and then we need to use it for another reason, we will ensure that new purpose is compatible with the original reason for processing.
- Adequate, relevant, and not excessive for the purpose. This means that we will collect enough information to achieve our aim, whilst minimising that collection to what is genuinely required.
- Accurate and up to date. This means that we will try to ensure that personal data is accurate when we collect it and kept up to date over time.
- Not kept for any longer than is necessary for the purpose. This means that we will try to ensure that personal data is accurate when we collect it, and kept up to date over time; and
- Processed securely using appropriate technical and organisational measures. Our measures include; technical safeguards like security of ICT systems, control over ICT access, the use of pseudonyms and encryption, as well as organisational safeguards, including plans for business continuity, securing our premises and data physically, implementing policies and procedures, conducting regular training, and carrying out audits and evaluations of operational measures and strategic oversight of compliance.

5.3 Personal data must also:

- Be processed in line with data subjects' rights.
- Not be transferred to people or organisations situated in other countries without adequate protection.
- Legal grounds for processing

- For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the data protection legislation. We will normally process personal data under the following legal grounds:
    - Where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract.
    - Where the processing is necessary to comply with a legal obligation that we are subject to).
    - Where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest.
    - Where we are pursuing legitimate interests, (or these are being pursued by a third party), for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects; and

5.4 Where none of the above apply, then we will seek the consent of the data subject to the processing of their personal data.

5.5 When special category personal data is being processed, then an additional legal ground must apply to that processing. We understand that for certain types of processing of special category personal data, we must have, and comply with, an appropriate policy document. Our special category personal data policy is our appropriate policy document for these purposes.

5.6 We will normally only process special category personal data under following legal grounds:

- Where the processing is necessary for employment law purposes, for example, in relation to sickness absence.
- Where the processing is necessary for reasons of substantial public interest, for example, for the purposes of equality of opportunity and treatment.
- Where the processing is necessary for health or social care purposes, for example, in relation to pupils with medical conditions or disabilities; and
- Where none of the above apply, then we will seek the explicit consent of the data subject to the processing of their special category personal data.

5.7 We will inform data subjects of the above matters by way of appropriate privacy notices, which shall be provided to them when we collect the data, or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

5.8 If any data user is in doubt as to the legal ground for processing personal data for any purpose, then they must contact the DPO before doing so.

6.0 Vital Interests

6.1 There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not able to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances, we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

7.0 Consent

7.1 Where none of the other bases for processing set out above apply, then the Trust must seek the consent of the data subject before processing any personal data for any purpose.

7.2 There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

7.3 When pupils and/or our workforce join the Trust, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate, third parties may also be required to complete a consent form.

7.4 In relation to all pupils under the age of 13 years old we will seek consent from an individual with parental responsibility for that pupil.

7.5 We will generally seek consent directly from a pupil who has reached the age of 13, however we recognise that this may not be appropriate in certain circumstances, and therefore we may be required to seek consent from an individual with parental responsibility.

7.6 If consent is required for any other processing of personal data of any data subject, then the form of this consent must:

- Inform the data subject of exactly what we intend to do with their personal data.
- Require them to positively confirm that they consent – we cannot ask them to opt out rather than opt in; and
- Inform the data subject of how they can withdraw their consent.
- Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent. We will ensure that it will be as easy for the data subject to withdraw their consent as it was to give it.
- Consent may need to be refreshed where we may need to process the personal data for a different and incompatible purpose, which was not disclosed when the consent was first considered by the data subject.

7.7 The DPO must always be consulted in relation to any consent form before consent is obtained.

7.8 A record must always be kept of any consent, including how it was obtained and when.

7.9 Data subjects' rights. In addition to the right to be informed and the right to withdraw consent, we will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any personal data we hold about them.
- Object to the processing of their personal data, including the right to object to direct marketing.
- Have inaccurate or incomplete personal data about them rectified.
- Restrict processing of their personal data.
- Have personal data we hold about them erased.
- Have their personal data transferred; and
- Object to the making of decisions about them by automated means.

7.10 The DPO must be consulted in relation to any data subject rights request.

8.0 The right of access to personal data

8.1 Data subjects may request access to the personal data we hold about them and which we are able to provide based on a reasonable and proportionate search for that personal data. Such requests will be considered in line with the Trust's subject access request procedure.

9.0 Data Protection by design and default

9.1 The Trust will consider and comply with the requirements of data protection legislation in relation to all its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

9.2 In certain circumstances, where the law requires us to, we shall carry out detailed assessments of proposed processing in a data protection impact assessment ("DPIA"). This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing, or there is a change in our existing ways of working.

9.3 The Trust will complete a DPIA of any such proposed processing, and has a template document, which ensures that all relevant matters are considered. This can be obtained from the Trust DPO

9.4 The DPO should always be consulted as to whether a DPIA is required, and if so, how to undertake that assessment. Then a copy should be provided to the DPO for central record purposes.

10.0 Data Security

10.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

10.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

10.3 Security procedures include:

- Entry controls. Any stranger seen in entry-controlled areas should be reported to the Principal of the Academy concerned or the relevant Head of department or Directorate.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal data is always considered confidential.)
- Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the ICO guidance on the disposal of IT assets.
- Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by, and that they log off from their PC when it is left unattended.
- Working away from the school premises – paper documents. It is not permitted for employees to take off site official paper documents that contain personal data (PID) of employees, pupils and other stakeholders. If there is an exceptional reason as to why this must take place then approval must be sought from the Principal or Head of Directorates and advice from DPO and an assessment of any risk will take place.
- Working away from the school premises – electronic working. All employees that have an ATT asset laptop must ensure that the equipment is kept in a locked and secure place at all times when off site from ATT premises and that they observe caution and care when on site in ATT premises. This includes during travel for work purposes such as at hotels or off site meetings and during times where individuals may be commuting to ATT workplaces.

- Document printing. Documents containing personal data must be collected immediately from printers and not left on photocopiers.
- Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

11.0 Personal data breaches

11.1 The Trust recognises that a breach of personal data could happen, despite our policies, procedures, and measures in place to protect personal data, and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm to individuals.

11.2 The Trust has a personal data breach procedure, and this must be followed in relation to any actual or suspected breach of personal data.

11.3 The Trust will use ICO guidance and risk assessment when assessing whether a breach is reportable and will review breaches to identify where any training or coaching is required for individuals or teams.

12.0 Disclosure and sharing of personal information

12.1 We may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, the local authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

12.2 The Trust will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

12.3 Where necessary, we will enter into a data sharing agreement to help facilitate the safe sharing of personal data with organisations.

12.4 In some circumstances we will not share safeguarding information. Please refer to our child protection policy.

13.0 Data processors

13.1 We contract with various organisations who provide services to the Trust. These include people, companies, and systems that process personal data on our behalf and under our instruction. In order that these services can be provided effectively, we are required to transfer personal data of data subjects to these data processors.

13.2 Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

13.3 Contracts with data processors will comply with data protection legislation and contain explicit obligations on the data processor to ensure compliance with the data protection legislation, and compliance with the rights of data subjects.

14.0 Images and Videos

14.1 Parents and others attending Trust events are allowed to take photographs and videos of those events for personal and domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Trust does not prohibit this as a matter of policy.

14.2 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part are outside of the ability of the Trust to prevent.

14.3 The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

14.4 Whenever a pupil begins their attendance at the Trust, they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. Images and videos of pupils may be required for safeguarding, assessment and learning purposes and we will not seek consent for the taking and use of these images. However, as a Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements.

14.5 We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

15.0 Video Surveillance

15.1 The Trust operates a CCTV system. Please refer to the Trust CCTV policy/video surveillance policy.

16.0 Biometric Data

16.1 The Trust operates a biometric recognition system for the purposes of:

- Payment of dinner monies.
- A secure entrance system on site.

16.2 Before we can obtain the biometric data of pupils or the workforce we are required to give notification and obtain consent for this special category data due to additional requirements for processing such data under the data protection legislation and/or Protection of Freedoms Act 2012.

16.3 For the workforce, explicit written consent will be obtained at the commencement of their position within the Trust and shall continue to be effective unless an objection in writing to the processing of the biometric data is received from the individual.

16.4 For pupils under the age of 18 years, the Academy will notify each parent of that pupil (that the Academy has the contact details for and is able to contact prior to them commencing their education at the school, of the use of our biometric recognition system. The Academy will then obtain the written consent of one of the pupil's parents before obtaining any biometric data.

16.5 In the event that written consent cannot be obtained from a parent, or any parent objects in writing, or the pupil objects or refuses to participate in the processing of their biometric data, the Trust will not process the pupil's biometric data and will provide alternative means of accessing the above services, please contact the Academy for local arrangements.

16.6 Further information about this can be found in our privacy notices.

17.0 Complaints

17.1 Data subjects have the right to make a complaint to the Trust if they consider we have not complied with data protection legislation. Any complaints relating to data protection must be directed to our DPO.

17.2 When dealing with complaints relating to data protection, we shall:

- Acknowledge receipt of the complaint within 5 days of the date on which the complaint is received by the Trust;
- Take appropriate steps to respond to the complaint, including making enquiries into the subject matter of the complaint, to the extent appropriate;
- Inform the complainant about progress of the complaint; and
- Inform the complainant of the outcome of the complaint.

17.3 Related policies and documents

- Special Category Data Policy
- Safeguarding Policies
- CCTV Policy
- Code of Conduct (employee policy)

17.4 We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.