DATA PROTECTION & INFORMATION SYSTEMS

Achieve + Learn Trust.
Better, together.

GDPR and Data Protection Policy

Approved by:	Board of Trustees
Date:	October 2026
Date of Next Review:	October 2029



ASPIRATION	We want people to be the best they can be, and for everyone to achieve their potential
COMMUNITY	We develop local and global citizens for the future, always committed to working in partnership
BELIEF	We encourage everyone to believe in themselves and their future, providing opportunities to excel



Achieve + Learn Trust.
Better, together.

Our Vision

Our vision is to make sure all students are afforded the best educational experience. This means that alongside our broad and aspirational curriculum, we offer students diverse enrichment opportunities to help them find their passions.

It's important to us that students grow both academically and personally. To do this, we create safe, inclusive and enriched learning environments in our schools, with opportunities outside of the classroom that open up pathways to successful futures.

We respect each school's individuality and the communities they serve, so we'll work with our staff to support their development without changing the school identity. Our network of schools collaborate and share knowledge to provide exceptional learning experiences and more opportunities for students to find what they love, and to discover for themselves where they may excel.

Our Aim

Our aim is to ensure that all schools within the Trust are strong providers and that our staff are fully supported and motivated to ensure the best outcomes for all our students at every age and stage.

Our Future

We strive for continuous improvement and development. The growth of our Trust will create and nurture a strong partnership of local schools, covering both primary and secondary phases. Simply put, we believe that we are better, together. Working collaboratively allows us to build on each school's strengths, while supporting areas of improvement and we believe this approach will improve even further as we enhance our family of schools.

Our Governance

We have five Members who hold the Board of Trustees to account for the performance of the Trust. In addition to the Trust Board, each member school has its own local governing body. Policies are ratified at both Trust level and local Governance level (policies bespoke to each school/locality). These are quality assured by our Director of People.

Contents

		Page
1	Purpose and Scope	4
2	Responsibilities	4-5
	2.1 School responsibilities	
	2.2 Data Protection Officer responsibilities	
	2.3 Staff responsibilities	
3	Data Protection Principles	5-6
4	The lawful basis for processing	6
5	Accountability	6-7
6	Data Protection by design and default	7
7	Data Protection Impact Assessment	7-8
8	Rights of the data subject	8
9	Data Protection Breaches	8-9
10	Consent	9
11	CCTV	9
12	Photography	10
13	Data Sharing	10
14	Data Security and Storage of Records	11
15	Disposal of records	11
16	Training	11
17	Contacts	12
18	Glossary of Terms	12-13

1 Purpose and Scope

Achieve and Learn Trust takes its responsibilities with regards to the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) seriously. This policy sets out how the school manages those responsibilities.

Achieve and Learn Trust is committed to data protection by design and regards the lawful and appropriate processing of personal and special category data as an integral part of its purpose.

This policy sets out the accountability and responsibilities of the school, its staff and its students to comply fully with the provisions of UK GDPR and DPA.

Achieve and Learn Trust holds and processes personal data about individuals such as employees, students and others, defined as 'data subjects'. Such data must only be processed in accordance with UK GDPR and the DPA.

This policy therefore seeks to ensure that we:

1. Protect personal data and the rights and freedoms of the data subject
2. Are clear about how personal data must be processed and the school's expectations for all those who process personal data on its behalf
3. Comply with the data protection laws, guidance and good practice
4. Protect the school's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
5. Protect the school from risks of personal data breaches and other breaches of data protection law.

The school has appointed a Data Protection Officer (DPO) to monitor and advise on compliance with UK GDPR and the DPA.

This policy applies to all personal data the school processes, regardless of the location where that personal data is stored (e.g. on an employee's own device) or the format of the information (paper, electronic, audio etc).

All school staff, and others processing personal data on the school's behalf, must be aware of and comply with this policy. A failure to comply, may result in disciplinary action.

Responsibilities

2.1. School responsibilities

The school, as data controller is responsible for establishing policies and procedures in order to comply with data protection legislation.

The Data Protection (Charges and Information) Regulations 2018 requires every data controller in the UK to pay a fee to the Information Commissioner's Office (ICO).

The school's registration number is ZA276100.

2.2. Data Protection Officer responsibilities

The DPO is responsible for:

- Advising the school and its staff of its obligations under UK GDPR
- Monitoring compliance with the UK GDPR and other relevant data protection law, the school's policies with respect to this, and monitoring training and audit activities related to UK GDPR compliance
- To provide advice on data protection impact assessments
- To cooperate with and act as the contact point for the ICO
- The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

2.3. Staff responsibilities

Staff members who process personal data about students, staff, applicants or any other individual must comply with the requirements of this policy. Staff members must ensure that:

- All personal data is kept securely;
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Personal data is kept in accordance with the school's retention schedule
- Any queries regarding data protection, including subject access requests and complaints, must be directed to the Information Governance Team within 24 hours of receipt. Because data protection complaints are legally bound by continuous calendar days (not school term days), staff must forward them immediately, even if received right before or during a school holiday period.
- Any data protection breaches are swiftly brought to the attention of Senior Managers and in turn the Information Governance team;
- All mandatory data protection training is completed and refreshed annually.

If staff are unsure about who are the authorised third parties to whom they can legitimately disclose personal data, they should seek advice from the Business Manager and Senior Leadership Team.

3 Data Protection Principles

Achieve and Learn Trust aims to comply with all the provisions of the DPA and the GDPR when processing personal data. The GDPR requires personal information to be processed according to seven data protection principles;

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- 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.
- Processed in a manner that ensures appropriate security of the personal data.

The seventh principle requires schools to be accountable and demonstrate how they comply with the principles.

4 The lawful basis for processing

The first principle requires all personal data to be processed lawfully, fairly and in a transparent manner. We will only process personal data where we have one of six 'lawful bases' to do so under data protection law:

1. **Consent:** the individual has given clear consent for the school to process their personal data for a specific purpose.
2. **Contract:** the processing is necessary for a contract the school has with the individual, or because they have asked us to take specific steps before entering into a contract.
3. **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
4. **Vital interests:** the processing is necessary to protect someone's life.
5. **Public task**: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
6. **Legitimate interests:** the processing is necessary for the school's 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.

For special categories (see glossary) of personal data, we will also meet one of the special category conditions for processing, which are set out in the UK GDPR and Data Protection Act 2018.

5 Accountability

- The school must implement and evidence appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. To demonstrate this, the school has implemented the following:
    - Appointed a suitably qualified DPO.
    - Implemented Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects (further information may be found below).
- Integrated data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches.
- Trained staff on compliance with Data Protection and keeping records accordingly.
- Regular testing of the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

6 Data Protection by design and fault

- Under UK GDPR, the school has an obligation to consider the impact on data privacy during all processing activities. There is an obligation to consider the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the personal data. In particular, by default, personal data should not be available to an indefinite number of persons. The school will ensure that:
- Appropriate technical and organisational measures are implemented to minimise the potential negative impact processing can have on the data subjects' privacy.
- Senior managers understand their responsibility for ensuring there is a privacy culture within the school and ensure policies and procedures are developed with Data Protection in mind.
- Privacy and data protection issues are always considered at the design phase of any system, service, product or process.
- Only data that is necessary to achieve a specific purpose is processed. This links to the fundamental data protection principles of data minimisation and purpose limitation.

7 Data Protection Impact Assessment

When considering new processing activities or setting up new procedures or systems that involve personal data, privacy issues must always be considered at the earliest stage and a Data Protection Impact Assessment (DPIA) will be conducted where applicable. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection requirements are not an after-thought.

A DPIA will be completed (and findings discussed with the information governance team/DPO) in the following circumstances:

- The use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated processing including profiling;
- Large scale processing of sensitive (special category) data; and
- Large scale, systematic monitoring of a publicly accessible area.

8 Rights of the data subject

UK GDPR was designed to strengthen the privacy rights of individuals. It offers more control to the data subject over what happens to their personal data. This has been expressed in UK GDPR under the following eight rights:

- The Right to be Informed
- The Right of Access
- The Right to Rectification
- The Right to Erasure
- The Right to Restrict Processing
- The Right to Data Portability
- The Right to Object
- The Right to Automated Decision Making

Achieve and Learn Trust has an individual Data Subject Rights policy – more information about individual rights and how to exercise them can be found on the school website.

Data Protection Complaints Handling
Individuals have a statutory right to complain directly to the Trust regarding how their data is handled, as well as to the Information Commissioner's Office (ICO).

- Timeline: All data protection complaints will be formally acknowledged within 30 calendar days of receipt, regardless of school holiday closures or recess periods.
- Separation of Issues: If a data protection complaint is raised alongside a general school complaint, the data protection element will be fast-tracked and resolved independently to prevent undue legal delays.
- Child Complainants: Complaints received from children will be assessed for competence and responded to using plain, age-appropriate language.

9 Data Protection Breaches

Achieve and Learn Trust is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction, or damage of the data. Potential incidents include:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

Any suspected data protection incident will be brought to the attention of the school's Information Governance Team and DPO, who will investigate and decide if the incident constitutes a data protection breach.

If a reportable data protection breach occurs, the school is required to notify the ICO as soon as possible, and no later than 72 hours after becoming aware of it. Any member of the school who encounters something they believe may be a data protection incident must report it immediately.

More information can be found here in the school data breach policy on the school website.

10 Consent

UK GDPR sets a high standard for consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement between the school, parents and students.

UK GDPR is clear that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

Achieve and Learn Trust will keep clear records to demonstrate where consent has been given.

11 CCTV

Achieve and Learn Trust understands that recording images of identifiable individuals is processing personal information and must be done in line with data protection principles.

The school notifies all students, staff and visitors of the purpose for collecting CCTV images via the Privacy Notice.

For more information regarding how we use CCTV please view our CCTV Policy on the school website.

12 Photography

Achieve and Learn Trust takes images/video footage of students throughout their school life. Photographs/video footage often consist of personal data and must be managed under data protection principles.

The school ensures it gathers [parent/student] consent in order to process images of students for school purposes such as, internal displays, school website, prospectus, or recordings of school plays.

Images captured by individuals for their domestic purposes, and videos made by parents for family use, fall outside the scope of UK GDPR.

A consent form for the particular usage of images will be sent to parents/carers annually/when the student starts at the school.

13 Data Sharing

Achieve and Learn Trust will usually only share data with third parties when they have a legal or statutory obligation or have the consent of parents/pupils.

Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
- Establish a data sharing agreement (see with the supplier or
- contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

14 Data Security and Storage of Records

Achieve and Learn Trust will aim to protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and servers that contain personal data are kept locked away when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to choose strong passwords and never reveal their passwords to others.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

15 Disposal of records

Achieve and Learn Trust only keeps personal data for as long as is required under legislation or business need. The school refers to a records retention schedule to determine when records no longer need to be retained.

Once personal data is no longer needed it is confidentially disposed of using secure methods.

16 Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of staff members' continuing professional development on an annual basis. This training will explicitly include how to recognize a data protection complaint and the mandatory protocol for routing it to the Information Governance Team during holiday periods.

17 Contacts

GDPR/Data Protection queries can be addressed in the first instance to the school's Data Manager. However, the school's official Data Protection Officer can be contacted here:

Karen Hillan

Town Hall

Stockport

SK1 3XE

dpa.officer@stockport.gov.uk

0161 474 4299

18 Glossary of Terms

Term	Description
Data	information which is stored electronically, on a computer, or in certain paper-based filing systems.
Processing	any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
Data subjects	all living individuals about whom we hold personal data.
Personal data	data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.
Data controller	person/business who determines the purposes for which personal data will be processed, and the manner in which it will be processed.
Data processor	person/business that processes personal data on behalf, and in accordance with the instructions, of a data controller.
Special category data	information about a person's race, ethnic origin, political opinions, religion, trade union membership, genetics, Biometrics (where used for ID), health, sexual life, or Sexual orientation.
Consent	an agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive

	action, signifies agreement to the processing of personal data relating to them.
Data Protection Officer (DPO)	person appointed as such under UK GDPR. A DPO is responsible for advising the school on its obligations under data protection, for monitoring compliance with data protection law, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.
Personal Data Breach	any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject.
Data Protection by Design and Default	involves implementing appropriate technical and organisational measures in an effective manner to ensure compliance with UK GDPR.