Active Learning Trust

DATA PROTECTION POLICY

Policy Review

Next Review Date:	October 2026
Ratified by:	Trust Board
Date Ratified:	23 October 2025
Dissemination:	The policy will be made available to all Trust employees

Document Control - Policy Amendments

Date	Version	Summary of Changes	Reviewer/s
Oct-23	1.0	Initial version – adapted from an ICT Service template	Chris Everard, Director of Operations
Nov-23	1.1	Updated to include section on Artificial Intelligence	Chris Everard, Director of Operations
Mar-24	1.2	Updated to correct spelling mistakes	Chris Everard, Director of Operations
Oct-24	2.0	Expanded the CCTV section Added CCTV appendices	Chris Everard, Director of Operations
Jan-25	2.1	Updated DPO details	Chris Everard, COO
Mar-25	2.2	Artificial Intelligence section updated with more comprehensive content	Chris Everard, COO
Oct-25	3.0	Reviewed against DfE guidance on data protection and model template from The Key Added generative AI to legislation section Updated central team contact under section 5 Added reference to the AI Acceptable Use Policy in section 14	Chris Everard, COO

Contents

1. Aims

1.1 Our Academy aims to ensure that all personal data collected about staff, pupils, parents, governors, trustees, visitors and other individuals is collected, stored and processed in accordance with the Data Protection Act 2018 (DPA 2018).

2. Legislation and Guidance

2.1 This policy meets the requirements of the UK GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the:

- UK GDPR – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data
- It also reflects the ICO's guidance for use of surveillance cameras and personal information.
- It follows guidance from the Department for Education (DfE) Generative artificial intelligence in education
- It also complies with our funding agreement and articles of association.

2.2 This policy follows It follows guidance from the Department for Education (DfE) Generative artificial intelligence in education

2.3 This policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics

	• Biometrics (such as fingerprints, retina and iris patterns), where used of identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The Data Controller

4.1 Our Academy processes personal data relating to parents, pupils, staff, governors, trustees, visitors and others, therefore is a data controller.

4.2 The Active Learning Trust is registered with the ICO as legally required. The registration number is ZA000790.

5. Roles and Responsibilities

5.1 This policy relates to all staff employed by the Active Learning Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.2 **The Board of Trustees** – has overall responsibility for ensuring that its Academies comply with all relevant data protection legislation.

5.3 **Data Protection Officer (DPO)** – is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the board their advice and recommendations on data protection issues. The DPO is also a point of contact for individuals whose data the Academy processes, and the first point of contact for the ICO. The DPO for the Active Learning Trust is **Data Protection Education (DPE)** and is contactable via dpo@dataprotection.education.

5.4 **Headteacher** – acts as the representative of the data controller on a day-to-day basis. They will nominate a member of staff to lead on data protection issues within their Academy.

5.5 **Data Protection Lead** – is the member of staff nominated to lead on data protection

issues within the Academy. They will ensure all staff have completed relevant data protection training and report any data breaches to the Active Learning Trust. They will also respond to Subject Access Requests (SARs) and Freedom of Information (FOI) requests.

5.6 **Chief Operating Officer** – the point of contact at the Active Learning Trust who can offer advice and guidance to the Data Protection Lead and Academy staff. They are responsible for analysing and monitoring trends in data breaches, SARs and FOIs as well as liaising with the DPO on more complex cases.

5.7 **All Staff** – are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Academy of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection right invoked by an individual, or transfer personal data outside the United Kingdom
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties.

6. Data Protection Principles

6.1 The UK GDPR is based on data protection principles that our Academy must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purpose for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

6.2 This policy sets out how the Academy aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawful, fairness and transparency

7.1.1 We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Academy can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person, i.e. to protect someone's life.
- The data needs to be processed so that the Academy, as a public authority, can **perform a task in the public interest or exercise its official authority**.
- The data needs to be processed for the **legitimate interests** of the Academy (where the processing is not for any tasks the Academy performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer where appropriate in the case of a pupil) has freely given clear **consent**.

7.1.2 **Special categories of personal data** – we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**.
- The data needs to be processed to perform or exercise obligations or right in relation to **employment, social security or social protection law**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for the establishment, exercise, or defence of **legal claims**.
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

7.1.3 **Criminal offense data –** we will meet both lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.

- The data needs to be processed for or in conjunction with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**.
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

7.1.4 Whenever we first collect personal data from individuals, we will provide them with the relevant information required by data protection law.

7.1.5 We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, Minimisation and Accuracy

7.2.1 We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

7.2.2 If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

7.2.3 Staff must only process personal data where it is necessary to do their jobs.

7.2.4 We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

7.2.5 When staff no longer need the personal data they hold, they must ensure it is deleted or anonymized. This will be done in accordance with the Retention Schedule set out in the Information and Record Management Society's Toolkit for Schools (Academies).

8. Sharing Personal Data

8.1 We will normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- 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 and contractors which can provide sufficient guarantees that they comply with UK data protection law.
    - Establish a contract with the supplier or contractor 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.

8.2 We will also share personal data with law enforcement and government bodies where we are legally required to do so.

8.3 We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

8.1 Where we transfer personal data internationally, we will do so in accordance with data protection law.

9. Subject Access Requests and other Rights of Individuals

9.1 Subject Access Requests

9.1.1 Individuals have a right to make a subject access request to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- The safeguards provided if the data is being transferred internationally.

9.1.2 Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

9.1.3 If staff receive a subject access request in any form, they must immediately forward it to the Academy's data protection lead.

9.2 Children and Subject Access Requests

9.2.1 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

9.2.2 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our

Academy may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

9.3.1 When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant).
- Will provide the information free of charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

9.3.2 We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we cannot reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

9.3.3 If a request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

9.3.4 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other Data Protection Rights of the Individual

9.4.1 In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances).
- Prevent the use of their personal data for direct marketing.
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling

(i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement).
- Be notified of a data breach (in certain circumstances).
- Make a complaint to the ICO.
- Ask for their data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

9.4.2 Individuals should submit a request to exercise these rights to the Academy's data protection lead in the first instance. If staff receive such as request, they must immediately forward it to the Academy's data protection lead.

10. Parental Requests to see the Educational Record

10.1 There is no automatic parental right of access to the educational record for Academies.

11. Biometric Recognition Systems

11.1 Where we use pupils' biometric data as part of an automated biometric recognition system we will comply with the requirements of the Protection of Freedoms Act 2012 *(in the context of the Protection of Freedoms Act 2012, a 'child' means a person under the age of 18)*.

11.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Academy will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

11.3 Parents/carers and pupils have the right to choose not to use the Academy's biometric system. We will provide an alternative means of accessing the relevant services for those pupils.

11.4 Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

11.5 As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

11.6 Where staff members or other adults use the Academy's biometric system, we will obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Academy will delete any relevant data already captured.

12. CCTV

12.1 We use CCTV in various locations around the Academy site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

12.2 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by

prominent signs explaining that CCTV is in use.

12.3 A Data Protection Impact Assessment (DPIA) will be conducted if CCTV is being installed at a new location.

12.4 Viewing of live CCTV images is restricted to employees approved by the Headteacher.

12.5 CCTV recording systems must be located in restricted areas and only viewed by approved employees authorized by the Headteacher.

12.6 Recorded images will be stored in a way that ensures their integrity (e.g. password protected or encrypted) and in a way that allows specific times and dates to be identified.

12.7 An access log (Appendix A) should be used to record who has accessed recordings.

12.8 An extraction log (Appendix B) should be used to record the images that have been extracted from the system.

12.9 CCTV systems should be checked regularly to ensure they are operating effectively. A systems log (Appendix C) should be used to record the checks carried out on the system.

12.10 Recordings will be retained for a limited time period only and for no longer than their intended purpose. This will be up to a maximum of 30 days. All recordings are to be erased before disposal.

12.11 Any queries about the CCTV system should be directed to the Data Protection Lead.

13. Photographs and Videos

13.1 We may take photographs and record images of individuals within our Academy as part of our routine activities.

13.2 We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

13.3 Any photographs and videos taken by parents/carers at Academy events for their own personal use are not covered by data protection legislation. However, we will ask that photos of videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

13.4 Where the Academy takes photographs and videos uses may include:

- Within the Academy on notice boards and magazines, brochures and newletters etc.
- Outside of the Academy by external agencies such as a school photographer, newspapers, campaigners.
- Online on our Academy website or social media pages.

13.5 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

13.6 When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13.7 See our safeguarding policy for more information on our use of photographs and videos.

14. Artificial Intelligence (AI)

14.1 Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

14.2 The Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive personal data.

14.3 The Academy will treat any use of AI to bully pupils in line with our behaviour policy.

14.4 To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

14.5 If personal data and/or sensitive data is entered into an unauthorized generative AI tool, the Academy will treat this as a data breach and will follow the personal data breach procedure.

14.6 AI must not be used to make independent decisions affecting students or staff.

14.7 AI tools must not be used to create harmful, misleading, or inappropriate content.

14.8 The use of AI in assessment, recruitment, or administrative decision-making must be documented.

14.9 AI-generated content must be identified where used.

14.10 A Data Protection Impact Assessment (DPIA) must be conducted before new AI tools are introduced. Colleagues are NOT allowed to use any new software without prior permission from the IT and Data Protection team.

14.11 See our AI Acceptable Use Policy for more information on the use of AI tools.

15. Data Protection by Design and Default

15.1 We will put measures in place to show that we have integrated data protection into all of our processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfill their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing data protection impact assessments where the Academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).

- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside of the United Kingdom, where different data protection laws will apply (where applicable).
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Academy data protection lead and the DPO as well as all information we are required to share about how we use and process their personal data, via our privacy notices.

    - For all personal data that we hold, maintain an internal record of the type of data, type of data subject, how and why are using the data, any third-party recipients, any transfers outside of the United Kingdom and the safeguards for those, retention periods and how we are keeping the data secure.

16. Data Security and Storage of Records

16.1 We will protect personal data and keep it safe from unauthorised or unlawful access, alternation, 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 hard drives that contain personal data, are kept under lock and key when not in use.

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.

- Staff, pupils, governors or trustees who store personal information on their personal devices are expected to follow the same security procedures as for Academy owned equipment.

- Where we 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 (see section 8).

17. Disposal of Records

17.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

17.2 We will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Academy's behalf. If we

do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17.3 We will base our retention schedule on guidance set out in the Information and Record Management Society Toolkit.

18. Personal Data Breaches

18.1 The Academy will make all reasonable endeavours to ensure that there are no personal data breaches.

18.2 If appropriate, we will report the data breach to the ICO within 72 hours of becoming aware of it. Such breaches in an Academy context may include, but are not limited to:

- A non-anonymised dataset being published on the Academy website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptops containing non-encrypted personal data about pupils.

19. Training

19.1 All staff, governors and trustees are provided with data protection training as part of their induction process.

19.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance of the Academy's processes make it necessary.

20. Monitoring

20.1 The DPO is responsible for monitoring and reviewing this policy. The policy will be reviewed **annually** and shared with trustees.

Appendix A – CCTV Access Log

This log should be used to document all viewing access to CCTV footage.

Date viewed	Camera locations	Reason	Footage start date / time	Footage end date / time	Employees viewing	Comments	Authorised by	Signature

Appendix B – CCTV Extraction Log

This log should be used to document all extracted CCTV footage and recipients.

Date extracted	Data extracted	Reason	Footage start date / time	Footage end date / time	Recipient	Delivered to recipient date	Comments	Authorised by	Signature

Appendix C – CCTV Systems Log

This log should be used to record the condition of the CCTV system. It can also be used to document damage or physical security concerns.

Date of review	Completed by	Confirmation system operates correctly	Confirmation settings are correct	Confirmation system is secure	Faults / issues	Action to be taken	Date completed	Signature