ACET

Striving for **Excellence**
Empowering Achievement
Shaping **Learning**

ACET Data Protection Policy

DATE: June 2026
POLICY LEAD: Data Protection Officer
APPROVED BY: Trustees

Excellence Equity Empowerment

DOCUMENT CONTROL		
Policy Level	Trust	
Approved By	Trustees	
Approval Date		
This policy remains valid until it is reviewed and replaced; it does not expire by date alone. Policies are reviewed annually, or sooner if required by statutory or legislative changes, in line with best practice		
Policy Lead / Author	Natalie Borrington	
Version Number	***Date Issued***	***Updated Information***
V2	March 2024	• Actions to minimise impact of data breaches – Page 15. And minor changes to retention schedule appendix 1
V3	March 2025	• Policy updated to ensure latest legislation is reflected throughout. Policy updated to reflect the use of Biometric Data and all relevant legislation along with the ACET Policy. Policy updated to reflect the CCTV review that has been completed and the creation of the CCTV Policy. 7.1 updated to reflect current template of lawful, fairness and transparency and criminal offence data has been added. 9.1 updated to reflect a SAR being made in any format. 9.2 updated to reflect the differences in primary and secondary academies. 13 updated to reflect primary and secondary differences and to add in the right to withdraw consent. Appendix 1 updated to reflect current DfE Guidelines and link to IRMS removed as no longer available. Appendix 2 – procedure added as a separate Appendix. Appendix 3 – Freedom of Information added as per ICO requirement
V4	March 2026	• Policy Updated to reflect DUAA • Specific updates to Section 7 further reference to privacy notices Section 8- clarification on data sharing. Section 9- timeframe clarification Section 9.1 addition of reasonable and proportionate search 9.3 added

		clarification on ‘stopping the clock’ Section 9.5 (new section)Section 14- Updated to reflect AI Policy & Steering Group Section 15 added reference to DPIAs Section 18 further clarification on the 72 hour reporting to ICO Section 20 monitoring arrangements updated slightly
V5	June 2026	• Section 9.5 (data Protection Complaints) re-written to comply with DUAA 2025. Section 9.4 linked to automated decision making. Retention schedule updated to reflect IRMS guidance on Restrictive Interventions Incident Logs. References to ICO changed to ‘Information Commission’ throughout.

Contents

1. Aims 5
2. Legislation and guidance 5
3. Definitions 5
4. The data controller 6
5. Roles and responsibilities 6
6. Data protection principles 7
7. Collecting personal data 8
8. Sharing personal data 9
9. Subject access requests and other rights of individuals 10
10. Parental requests to see the educational record 13
11. Biometric recognition systems 13
12. CCTV 13
13. Photographs and videos 14
14. Artificial intelligence (AI) 14
15. Data protection by design and default 15
16. Data security and storage of records 16
17. Disposal of records 16
18. Personal data breaches 16
19. Training 17
20. Monitoring arrangements 17
21. Links with other policies 17

Appendix 1: Records Retention Periods 17

Appendix 2: Personal data breach procedure 28

Appendix 3: Freedom of Information Publication Scheme 31

1. Aims

Aston Community Education Trust (ACET) aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (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)
- Data (Use and Access) Act 2025
- Protection of Freedoms Act 2012 (Biometrics)
- Freedom of Information Act 2000

It is based on guidance published by the Information Commission (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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 the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

This policy also reflects requirements and provisions introduced through the Data (Use and Access) Act 2025, particularly in relation to complaint handling, access rights and transparency obligations when processing personal data.

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.

TERM	DEFINITION
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 for 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 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 accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

ACET processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Trust is registered with the ICO, as legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by ACET, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Trust board

The Trust board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our 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 Trust board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is The Trust Governance Leader and is contactable via contactus@astoncetrust.org.

5.3 CEO & Principals

The CEO and Principals act as the representative of the data controller on a day-to-day basis.

5.4 All staff

- Staff are responsible for:
- Collecting, storing and processing any personal data in accordance with this policy
- Informing the trust/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 rights invoked by an individual, or transfer personal data outside the UK
    - 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

The UK GDPR is based on data protection principles that our trust and all academies 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 purposes 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

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

7. Collecting personal data

Information about how the Trust processes personal data can be found in the Trust's Privacy Notices, which are published on academy websites and reviewed regularly.

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the trust/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 trust/academy 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 trust/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 trust/academy (where the processing is not for any tasks the trust/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 when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet 1 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 rights 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

For criminal offence data, we will meet both a 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 connection 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

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

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

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.

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.

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

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

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

8. Sharing personal data

The Trust will only share personal data where there is a clear lawful basis under UK GDPR and where the sharing is necessary, proportionate and secure.

Where appropriate, data sharing agreements or information sharing protocols will be used to ensure personal data is handled lawfully.

We will not 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 are 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 or contractors that 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

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

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.

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. The Academy will conduct a search that is reasonable and proportionate. 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

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

If staff receive a subject access request in any form they must immediately forward it to the DPO.

9.2 Children and subject access requests

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.

For the ACET **Primary** Academies:

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 school 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.

For the ACET **Secondary** Academies:

Children aged 12 and above are generally 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 school may not 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

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
- May 'pause' the one-month limit for a SAR if we need further clarification on the scope or nature of the data being requested
- 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 In accordance with UK GDPR, the Trust may extend this period by up to **two further months** where requests are particularly **complex or numerous**. Where an extension is applied, the requester will be informed within the initial one-month period and provided with an explanation.

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 can't 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

If the 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.

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

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 use of their personal data for direct marketing

- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests

- The right to challenge significant decisions made solely by automated means, this right applies particularly where special category data is involved. Where the Trust uses automated processes that significantly affect individuals, we will ensure appropriate human oversight is in place and will inform individuals of their rights.

- Be notified of a data breach (in certain circumstances)

- Make a complaint to the ICO

- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9.5 Data Protection Complaints

Under Section 164A of the Data Protection Act 2018, as inserted by Section 103 of the Data (Use and Access) Act 2025, individuals have a statutory right to raise a data protection complaint directly with ACET where they believe their personal data has been processed in breach of data protection law.

ACET takes all such concerns seriously. Individuals may submit a data protection complaint by:

- Emailing the details of the complaint to the Trust DPO at contactus@astoncetrust.org
- Writing to the Trust DPO at ACET House, 66 Holderness Drive, Aston, Sheffield, S26 2BH
- Telephoning 0114 287 1181 during office hours

All complaints will be acknowledged within 30 calendar days of receipt. The Trust will investigate the matter without undue delay and communicate the outcome in writing. Where a complaint is complex, the individual will be kept informed of progress.

A record of all complaints received, actions taken, and outcomes will be maintained by the DPO.

If an individual remains dissatisfied following the Trust's response, they may escalate their complaint to the Information Commission (formerly the ICO) at www.ico.org.uk or by calling 0303 123 1113. Under the DUAA, individuals are required to raise their complaint with the Trust in the first instance before escalating to the Information Commission.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil). If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it. This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash) we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, the person will be able to use ParentPay/Schoolcomms/Parental Engagement App to top up their account which synchronises with the till system, or pay with cash at the till.

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

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).

Where staff members or other adults use the school's biometric system(s), we will also 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 school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around certain academies to ensure they remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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.

Any enquiries about the CCTV system should be directed to the Data Protection Officer. Further details can be found within the ACET CCTV Policy.

13. Photographs and videos

As part of our trust/academy activities, we may take photographs and record images of individuals within our academies.

For the ACET Primary Academies:

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 the pupil.

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 or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

For the ACET Secondary Academies:

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

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 or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within academies on notice boards and in academy magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our trust/academy website or social media pages

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.

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.

14. Artificial intelligence (AI)

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, CoPilot and Google Gemini. ACET recognises that AI has many uses to help pupils learn but also poses risks to sensitive and personal data. ACET have an AI policy as well as an AI Steering group to oversee the use of Artificial Intelligence and ensure the trust remains safe whilst accessing the benefits.

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.

Where AI or automated tools are used to support administrative or educational processes, the Trust will ensure that:

- Human oversight is maintained
- Personal data is processed lawfully and transparently
- No solely automated decisions with legal or significant effects are made about individuals without appropriate safeguards.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, ACET will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1. Action could be taken against the individual in line with HR policies.

15. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil 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 school'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 UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO, and 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, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure
    - The Trust will carry out Data Protection Impact Assessments (DPIAs) where processing is likely to result in a high risk to individuals' rights and freedoms.

16. Data security and storage of records

We will 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 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
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites and a blacklist of commonly used passwords is enforced to meet Cyber Essentials standards and prevent weak password use.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices Staff, pupils or governors should not store ACET personal information on their personal devices. ACET devices are configured to protect the usage of personal information and staff are expected to follow the same security procedures for school-owned equipment whether in or out of the Trust (see our E-safety policy and relevant acceptable use agreement / policy on acceptable use)

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 (see section 8)

17. Disposal of records

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.

For example, 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 school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Please refer to Appendix 1 for further guidance on retention periods.

18. Personal data breaches

ACET and its Academies will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 2.

Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, the Trust will report the breach to the Information Commission within 72 hours, where feasible, in accordance with UK GDPR.

Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school 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 laptop containing non-encrypted personal data about pupils

19. Training

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

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

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually and approved by the Trust board. The Trust's Data Protection Officer will monitor compliance with this policy, report on non-compliance to the Trustees and provide advice and support to academies across the Trust

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy notices
- CCTV Policy
- Child Protection & Safeguarding Policy
- Protection of Biometric Data Policy
- E-Safety Policy
- AI Policy

Appendix 1: Records Retention Periods

These guidelines have been produced by ACET to assist schools in the management of their records. The guidelines outline the recommended retention periods for schools based on legislation and common practice.

It is the responsibility of Academies to retain their records for the appropriate retention period, or to securely dispose of them. The retention guidelines produced in this document are some of the key retention periods which need to be considered.

Pupil records

Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each School that a pupil attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement.

All pupil records and associated information should be stored securely to maintain confidentiality, whilst keeping information accessible to those authorised to see it. Electronic records should have appropriate security and access controls in place; equally, paper records should be kept in lockable storage areas with restricted access

Document type	Retention period	Action at end of retention period	Further information
Restrictive Interventions Incident Record	This record must travel with the child to their new educational setting. The 'last known school' is responsible for retaining this in line with pupil educational and safeguarding records (usually date of birth of the pupil + 25 years)	Dispose of records securely. If the pupil leaves to go to another school, transfer the records to that school.	The individual incident record form (or a copy of it) filed as part of the pupil's safeguarding or educational record.
Primary school pupil records	Until the pupil leaves the school.	Transfer to secondary school or other primary school when the pupil leaves.	See The Education (Pupil Information) (England) Regulations 2005 for details of what to keep in the pupil record. There is guidance on how to transfer information to another school.
Secondary school pupil records	Until the pupil's 25th birthday.	Dispose of records securely. If the pupil leaves to go to another school, transfer the records to that school. There is guidance on what to do if the school closes before the end of the retention period.	See The Education (Pupil Information) (England) Regulations 2005 for details of what to keep in the education record. Retain as detailed in section 2 of the Limitation Act 1980.
Special educational	Until the pupil's 30th birthday.	Dispose of records	SEND code of practice: 0 to 25 years. Retain as detailed in

Document type	Retention period	Action at end of retention period	Further information
needs and disabilities (SEND), including SEND statements and accessibility plans		securely, unless the document is subject to a legal hold. If the pupil leaves to go to another school, transfer the records to that school.	section 2 of the Limitation Act 1980.
Attendance and absence	Until the pupil's 30th birthday.	Dispose of records securely, unless the document is subject to a legal hold. If the pupil leaves to go to another school, transfer the records to that school.	SEND code of practice: 0 to 25 years. Retain as detailed in section 2 of the Limitation Act 1980.

Child protection records

Document type	Retention period	Action at end of retention period	Further information
Child protection files	Until the child's 25th birthday. If the file relates to child sexual abuse, retain until the child's 75th birthday.	Dispose of records securely. Child protection files should be passed on to any new school a child attends. This should be transferred separately from the main pupil file.	Should be stored in a separate child protection file. Keeping children safe in education sections 66, 67, 121 and 122. The Report of the Independent Inquiry into Child Sexual Abuse (IICSA), recommendation on access to records.
Allegations of child protection against a member of staff,	Until the staff member's normal	Dispose of records securely.	Keeping children safe in education. Working together to safeguard children.

Document type	Retention period	Action at end of retention period	Further information
including unfounded allegations	retirement age, or 10 years from the date of the allegation, whichever is later.		

Finance records

Document type	Retention period	Action at end of retention period	Further information
Contracts	6 years from the last payment on the contract.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Contracts under seal	12 years	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Debtor's records	6 years from the end of the financial year.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
VAT records	6 years from the end of the financial year.	Dispose of records securely.	May include invoices, budgets, bank statements and annual accounts. Record keeping (VAT Notice 700/21).
Annual accounts	6 years from the end of the financial year.	Archive	
Invoices, receipts, and other financial records covered by financial regulations	6 years from the end of the financial year.	Dispose of records securely	Standard financial regulations

Document type	Retention period	Action at end of retention period	Further information
Employer's Liability Certificate	Retain for 40 years	Dispose of records securely.	Transfer to ACET Record Office on closure of school
Inventories of equipment/furniture	Retain for 6 years	Dispose of records securely.	

Governance records

Document type	Retention period	Action at end of retention period	Further information
Admissions	3 years from the admission date.	Dispose of records securely.	Working together to improve school attendance.
Successful school admissions applications	Retain for 1 year	Dispose of records securely.	
Unsuccessful school admission applications (where no appeal is made)	Retain for 1 year	Dispose of records securely.	
Unsuccessful school admission applications (where an appeal is made)	Retain for 1 year	Dispose of records securely.	
Proofs of address supplied by parents as part of the admissions process	Retain for 1 year	Dispose of records securely.	
Attendance registers	3 years from the date of entry.	Dispose of records securely.	Regulation 14 of the Education (Pupil Registration) (England) Regulations 2006.
Annual governors report	10 years.	Dispose of records securely.	The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002. Retain as detailed in section 2 of the Limitation Act 1980.

Document type	Retention period	Action at end of retention period	Further information
Curricular record	At least one year.	Dispose of records securely.	The Education (School Records) Regulations 1989. Regulation 3 of the Education (Pupil Information) (England) Regulations 2005.
Directors – disqualification	15 years from the date of disqualification.	Dispose of records securely.	The Education (Company Directors Disqualification Act 1986: Amendments to Disqualification Provisions) (England) Regulations 2004
Records of educational visits	10 years from the date of the visit. If there was an incident on the visit, retain the permission slips for all pupils and the incident report in the pupil record, or until the pupil reaches the age of 25.	Dispose of records securely.	Health and safety on educational visits. Retain as detailed in section 2 of the Limitation Act 1980.
School vehicles	6 years from the disposal of the vehicle.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Statutory registers and compliance	Retention periods vary, for example: Memorandums of understanding should be retained for the life of the academy plus 6 years. Annual reports should be retained for 10 years from the date of the report. Board meeting	Dispose of records securely.	May include annual reports and governance records. Companies Act 2006 contains information on which statutory registers to keep. Compliance guidance in the maintained schools governance guide. Compliance guidance in the academy trust governance guide. Academy trust handbook.

Document type	Retention period	Action at end of retention period	Further information
	records should be.		
Board Meeting Minutes	Minutes must be kept for at least 10 years from the date of the meeting	Archive	Companies Act 2006 section 248
Records relating to the management of General Members' Meetings Records relating to the management of the Annual General Meeting	Minutes must be kept for at least 10 years from the date of the meeting	Archive	Companies Act 2006 section 248
Agendas	Dispose after meeting	One copy should be retained with the master set of minutes. All other copies can be disposed of	Common practice

Health and safety records

Document type	Retention period	Action at end of retention period	Further information
Restrictive Interventions Incident Log	Current academic year + 6 years as a minimum. Where incidents involve physical injury to a pupil, or where pupils with SEND are involved, schools should consider extending retention to the date of birth of the youngest pupil involved in any incident recorded in the log + 25 years, by analogy with accident records involving children.	Dispose of records securely.	This is the school's own governance and management record of all incidents of use of force, seclusion and non-force related restraint involving pupils, maintained as an incident log or incident book at school level and separate from individual pupil education or safeguarding records
Accessibility plans	Life of plan plus 6 years.	Dispose of records securely.	Retain as detailed in section 2 of the Limitation Act 1980.
Accident records	3 years from the date of the accident.	Dispose of records securely.	Accidents involving pupils should be retained in the pupil record. Regulation 25 of the Social Security (Claims and Payments) Regulations 1979.
Monitoring exposure to substances hazardous to health, including asbestos	5 years.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002.
Health surveillance records	40 years.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002. Health surveillance - Record keeping.
Other health records of staff	While the worker is employed in your school.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002. Health surveillance - Record keeping.

Document type	Retention period	Action at end of retention period	Further information
Restrictive Interventions Incident Log	Current academic year + 6 years as a minimum. Where incidents involve physical injury to a pupil, or where pupils with SEND are involved, schools should consider extending retention to the date of birth of the youngest pupil involved in any incident recorded in the log + 25 years, by analogy with accident records involving children.	Dispose of records securely.	This is the school's own governance and management record of all incidents of use of force, seclusion and non-force related restraint involving pupils, maintained as an incident log or incident book at school level and separate from individual pupil education or safeguarding records
Fire assessments	Life of the risk assessment plus 6 years.	Dispose of records securely.	Fire Service Order 2005. Retain as detailed in section 2 of the Limitation Act 1980.
Parental permission slips for school trips where there has not been a major incident	No retention required	Dispose of records securely.	
Parental permission slips for school trips where there has been a major incident	Retain for 25 years from the date of birth of the pupil/s involved in the incident	Dispose of records securely.	The Limitations Act 1980
Records created by schools to obtain approval to run an Educational Visit outside the classroom where there has not been a major incident	Retain for 14 years	Dispose of records securely.	The Health and Safety at Work Act 1974
Records created by schools to obtain approval to run an Educational Visit outside the classroom where there has been a major incident	Retain for 21 years from the date of birth of the pupil/s involved in the incident	Dispose of records securely.	The Limitations Act 1980

Document type	Retention period	Action at end of retention period	Further information
Restrictive Interventions Incident Log	Current academic year + 6 years as a minimum. Where incidents involve physical injury to a pupil, or where pupils with SEND are involved, schools should consider extending retention to the date of birth of the youngest pupil involved in any incident recorded in the log + 25 years, by analogy with accident records involving children.	Dispose of records securely.	This is the school's own governance and management record of all incidents of use of force, seclusion and non-force related restraint involving pupils, maintained as an incident log or incident book at school level and separate from individual pupil education or safeguarding records
Records of the administration of medicines for all routine medication (e.g. Calpol, antibiotics, treatments for asthma and diabetes)	Retain for 1 year	Dispose of records securely.	Events significantly outside individual treatment plan should be treated as non-routine
Records of administration of medicines for all non-routine medication (e.g. peg feeding, epi-pen, invasive drugs, anti-depressants) and any records governing a reported incident, difficulty or issues with administering medication.	Retain for 21 years and 6 months from pupil's date of birth	Dispose of records securely.	
Major Incident e.g. Emergency Services, disease outbreak/ Ofsted Reports & Papers	Retain whilst current	Archive	

Property records

Document type	Retention period	Action at end of retention period	Further information
Maintenance records	6 years from the end of the financial year.	Dispose of records securely.	Record keeping (VAT Notice 700/21).
Title deeds	12 years from the end of the deed.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Building plans	Retain whilst operational	Archive	

Staff records

Document type	Retention period	Action at end of retention period	Further information
Copies of DBS certificates	6 months from the date of recruitment.	Dispose of records securely.	Keeping children safe in education.
Maternity pay records	3 years after the end of the tax year in which the maternity pay period ends.	Dispose of records securely.	The Statutory Maternity Pay (General) Regulations 1986.
Pay records	3 years from the end of the tax year they relate to.	Dispose of records securely.	PAYE and payroll for employers: Keeping records.
Personnel files	6 years from termination of employment.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Retirement benefits	A minimum of 6 years from the end of the year in which the accounts were signed.	Dispose of records securely.	Regulation 15 of the Retirement Benefits Schemes (Information Powers) Regulations 1995.

Document type	Retention period	Action at end of retention period	Further information
Interview notes for unsuccessful candidates	Retain for 6 months	Dispose of records securely.	
Written warnings (level 1)	Retain for 6 months	Dispose of records securely.	
Written warning (level 2)	Retain for 12 months	Dispose of records securely.	
Final warning	Retain for 18 months	Dispose of records securely.	
Warnings subsequently found to be based on an unfounded case (excluding child protection related warning)	No retention required	Dispose of records securely.	
Staff appraisal records	Retain for 5 years	Dispose of records securely.	

Appendix 2: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commission (ICO).

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust/ school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the trust / school's computer system.

- The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and Principal will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Other key examples of breaches may include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen

- Hardcopy reports sent to the wrong pupils or families

Appendix 3: Freedom of Information Publication Scheme

1. Introduction

In accordance with the Freedom of Information Act 2000 (FOIA) and the guidance set by the Information Commission ACET has adopted the Model Publication Scheme provided by the ICO. This scheme ensures that information is made available to the public proactively, reducing the need for individual requests.

Our Publication Scheme outlines:

- The classes of information we publish.
- How this information is available.
- Any charges that may apply.

2. The Trust's Commitment to Transparency

We are committed to openness and accountability. Our **Publication Scheme** provides access to key information about our policies, decisions, and operations, ensuring compliance with FOIA and ICO guidance.

3. Information We Publish

Under this scheme, we publish the following categories of information as per the ICO's Definition Document for Academies (ICO Guidance):

Category	Examples of Information Available	How to Access	Charges
Who we are and what we do	Academy structure, governance details, trust leadership Academy funding agreements	Trust and school websites. DfE Get Information About Schools	Free
What we spend and how we spend it	Annual financial reports, procurement, staff pay structures. Executive pay disclosures (as required under ESFA guidance)	Trust website or upon request. ACET Website	Free/Copying charges apply.
What our priorities are and how we are doing	Trust improvement plans, Ofsted reports, performance data.	Trust website. Ofsted website DfE Performance Tables	Free
How we make decisions	Board minutes (subject to redaction where necessary), policies, admissions arrangements.	Website or upon request. ACET Website	Free

Policies and procedures	Statutory policies, including safeguarding, complaints, and data protection policies	Website.	Free
Lists and registers	Asset registers, staff pay bands.	Upon request.	Copying charges apply.
Services we offer	Extra-curricular activities, community engagement.	Website.	Free

4. How to Access Information and Costs

Information covered by this **Publication Scheme** is available **free of charge** on our website at https://www.astoncetrust.org/

For **printed copies** or information provided in an alternative format, charges may apply. Fees are based on:

- **Printing and photocopying**: Charged at 5p per A4 page (black & white) and 10p A3 per page (black & white).
- **Postage**: Charged at actual cost (Royal Mail standard second-class).

5. Making a Freedom of Information Request

If information is not available through our **Publication Scheme**, you may submit a **Freedom of Information Request**. Requests must be:

- Made in writing (email or letter).
- Include the requester's name and contact details.
- Clearly describe the information sought.

Requests should be sent to: The DPO – contactus@astoncetrust.org

We will respond within **20 working days**, in accordance with FOIA and ICO guidance. If a request is refused, we will provide reasons and details of the appeals process.

If you are dissatisfied with how we handle your request, you may ask for an internal review by contacting:

ACET – Governance Team

Email: governance@astoncetrust.org

If you remain unsatisfied, you can escalate your complaint to the Information Commissioner's Office (ICO):

ICO Website: https://ico.org.uk

Helpline: 0303 123 1113

6. Review and Updates

This **Publication Scheme** is reviewed annually to ensure compliance with **FOIA 2000** and **ICO best practice**.