Data Protection, Record Retention and Deletion Policy

Category:	Trust-wide Policy
Authorised By:	Board of Trustees
Author:	Keith Holroyd, *Head of Governance, Policy & Compliance* Sumit Parmar, *DPO* Catherine Roper, *Marketing & Communications Manager*
Owner:	Sudhi Pathak, *Chief Operating Officer*
Version:	1
Status:	Ratified
Issue Date:	March 2025
Next Review Date:	March 2026

Version Control

Ver.	Date	Comment
1	March 2025	New policy, bringing together 3 separate but related policies
Previous data protection policy		
2	October 2019	
3	November 2020	Updated to name Sumit Parmar as the DPO and a section on the transfer of hard copy data
3.1	June 2021	Updated to reflect latest ICO requirements
4	April 2022	Cyclical review
5	March 2023	Cyclical review; includes addition of statement on the collection of biological information
6	March 2024	Cyclical review; no changes
Previous record retention and deletion policy		
1	March 2020	Initial document
2	March 2023	Cyclical review

This policy will be subject to ongoing review and may be amended prior to the scheduled date of the next review in order to reflect changes in legislation, statutory guidance, or best practice (where appropriate).

Contents

SECTION A: DATA PROTECTION POLICY

1. Aims

The Eden Academy Trust (the Trust) aims to ensure that all personal data collected about staff, pupils, parents, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

2. Legislation and guidance

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

Where any of our schools use CCTV, it also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, 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 for identification purposes • Health – physical or mental

Term	Definition
	• 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

The Trust processes personal data relating to parents, pupils, staff, visitors and others, and therefore is a data controller.

The Trust is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

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

5.1. Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

5.2. Data protection officer

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.

The Trust employs Sumit Parmar to act as its DPO and he reports to the Board of Trustees through the Director of Finance & Operations and, where relevant, report to the Board their advice and recommendations on 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 contract.

Our DPO is and is contactable via dataprotection@theedenacademy.co.uk

5.3. Heads of Schools

The Heads of School act as the representative of the data controller on a day-to-day basis for each school within the Trust.

5.4. All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust 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 European Economic Area
    - 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 GDPR is based on data protection principles that the Trust 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 Trust aims to comply with these principles.

7. Collecting personal data

7.1. Lawfulness, fairness and transparency

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 Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust 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 schools within the Trust, as public authorities, can perform a task in the public interest or exercise official authority
- The data needs to be processed for the legitimate interests of the Trust (where the processing is not for any tasks the Trust 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 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 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 Trust's record retention schedule.

7.3. Collection of biometric information

The Trust's schools do not currently collect biometric information. The Protection of Freedoms Act 2012 states that:

"Biometric information" means information about a person's physical or behavioural characteristics or features which—

(a). is capable of being used in order to establish or verify the identity of the person, and

(b). is obtained or recorded with the intention that it be used for the purposes of a biometric recognition system."

Should that position change, the Trust will approve an update to this policy to cover its collection and use.

8. Sharing personal data

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 which can provide sufficient guarantees that they comply with 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 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. 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 must include a clear label for your request (e.g. use 'subject access request' as your email subject line or a heading for your letter). We may be able to respond to requests more quickly if they 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 dataprotection@theedenacademy.co.uk

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.

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 under this age 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.

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 until a pupil's ability to understand their rights has been 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
- 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

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 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 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.

10. CCTV

Where any of our schools use CCTV in various locations around the school site to ensure it remains safe, we will adhere to the ICO's code of practice for the use of CCTV.

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 Head at the relevant school.

11. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our schools.

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.

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 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 school 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 Trust or an individual school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school 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.

12. 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 an internal 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 European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the Trust 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 EEA and the safeguards for those, retention periods and how we are keeping the data secure.

13. 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 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
- Staff, pupils or Members, Trustees or Committee/LAB members who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT Usage and IT & Online Safety Policies)
- 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

14. Transfer of hard copy data

14.1. Sending data

- The Head would need to approve before dat is taken off site.
- The Head would need to identify an appropriate person to take data off site taking account of the nature of the data (e.g. safeguarding data)
- The Head would need to identify a person at the destination who would receive the data
- The person taking the data off site needs to sign a form to provide acknowledgement that they are taking the data off site.

- The person taking the data off site would have to agree where the data is going and who is receiving it
- Data should not be transferred by public transport
- Data must be taken directly to the destination
- If going to another school, the other school would need to know what data will be delivered.

14.2. Receiving the data

- The organisation receiving the data would need to sign that the data has been received
- The organisation receiving the data should inform the sending school that the data has been received

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

16. Personal data breaches

The Trust 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 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. 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

17. Training

All staff and trustees 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 Trust's processes make it necessary.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and ratified by the Board of Trustees.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Safeguarding Policy

SECTION B: RECORD RETENTION AND DELETION

20. Background

This record retention and deletion policy contains recommended retention periods for the different record series created and maintained by Eden Academy Trust in the course of our business. The schedule refers to all information regardless of the media in which it is stored.

Some of the retention periods are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the General Data Protection Regulations (GDPR), Data Protection Act 2018 (DPA) and the Freedom of Information Act 2000 (FOI).

Managing record series using these retention guidelines will be deemed to be "normal processing" under the legislation mentioned above. If record series are to be kept for longer or shorter periods than laid out in this document the reasons for this need to be documented.

This policy will be reviewed at intervals of no less than three years, or exceptionally, if required by changes in Data Protection, Freedom of Information or other relevant legislation.

21. The purpose of the retention schedule

Under the Freedom of Information Act 2000, schools are required to maintain a

retention schedule listing the record series which the school creates in the course of its business. The retention schedule lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use.

Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

The retention schedule refers to all information, regardless of the media in which they are stored.

22. Benefits of a retention schedule

There are several benefits which arise from the use of a complete retention schedule:

a) Managing records against the retention schedule is deemed to be "normal processing" under the General Data Protection Regulations, Data Protection Act 2018 and the Freedom of Information Act 2000. Provided members of staff are managing records using the retention schedule they cannot be found guilty of unauthorised tampering with files once a freedom of information request or a data subject access request has been made.

b) Members of staff can be confident about destroying information at the appropriate time.

c) Information which is subject to Freedom of Information and Data Protection legislation will be available when required.

d) The school is not maintaining and storing information unnecessarily.

23. Maintaining and amending the retention schedule

Where appropriate the retention schedule should be reviewed and amended to include any new record series created and remove any obsolete record series.

24. What to do with records once they have reached the end of their administrative life

24.1. Destruction of records

Where records have been identified for destruction, they should be disposed of in an appropriate way. All records containing personal information, or sensitive policy information should be shredded before disposal (if possible). Any other records should be bundled up and disposed of to a wastepaper merchant or disposed of in other appropriate ways.

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction.

Members of staff should record at least:

- File reference (or another unique identifier)
- File title (or brief description)
- Number of files
- The name of the authorising officer

This could be kept in an Excel spreadsheet or other database format.

24.2. Transfer of records to the archives

Where records have been identified as being worthy of permanent preservation, arrangements should be made to transfer the records to the Archives.

24.3. Transfer of information to other media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as microform or digital media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

24.4. Transfer of information between schools

When a child leaves the school all records for the child should be transferred in a secure manner to the child's new school. If the records contain sensitive information (e.g. child protection records) proof of receipt should be obtained. All

data held by the school should then be deleted including all paper records and data stored electronically. A record should be kept for tracking and auditing purposes only.

25. All staff

Everyone is responsible for:

- Following procedures and guidance for managing, retaining and disposing of records
- Only disposing of records in accordance with the requirements outlined in this policy (if authorised to do so).

Ensuring that any proposed divergence from the records retention and disposal policies is authorised by the School Head.

26. References and links with other policies

- General Data Protection Regulations 2016/679
- Data Protection Act 2018
- Article 8, The Human Rights Act 1998
- Freedom of Information Act 2000
- Code of Practice on Records Management (under Section 46 of the Freedom of Information Act 2000)
- EAT Attendance Policy
- EAT Disciplinary Policy and Procedure
- EAT Capability Policy and Procedure
- EAT Complaints Policy
- EAT Data Protection Policy

SECTION C: KEEPING AND RETAINING PERSONNEL RECORDS

27. Information on employees' personal files

The following table indicates the information that should be kept on an employee's personal file.

Area	Information
Recruitment and Selection	Advert Job Description Person Specification Application Form & Supporting Statement (including equal opportunity monitoring form) Pre-employment Checks (Single Central Record) • Identity • Qualifications • Barred List check • DBS* • Right to Work in the UK • Overseas Checks • Check of the Prohibition List In addition: • References • Medical clearance Offer of Employment *DBS certificates must not be photocopied and retained on the personal file.
Contractual Documents	Copy of the employment contract together with any subsequent variations
Payroll Paperwork	Bank Details Pension Documentation Contract variation notification forms
Induction/Training	Copy of the completed Induction Sheet Details of any training/courses attended

Area	Information
Absence/Leave	Annual Leave cards Record of absence/lateness Sickness absence including medical certificates, self-certification forms and return to work meeting records, occupational health information, hospital appointment letters Maternity/paternity/adoption details Applications for Special Leave e.g. bereavement leave (paid or unpaid)
Employment Procedures	Probationary Reports Appraisal/Performance Management/Supervision notes Grievances Formal live warnings under the Disciplinary & Capability Procedures Formal meetings under the Managing Attendance Procedures Redundancy
Accident & Industrial Injury	Copy of Accident/Incident Reporting Form
Termination of Employment	Letter of Resignation/Reason Exit Interview Form/Notes

The personnel file should be retained during the course of the employee's employment and for a further six (6) years after the employment has ceased.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- 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
- The DPO will alert the Director of Finance & Operations and the Chair of Trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out 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
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the DPO.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:
    - 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. 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
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. 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

As above, any decision on whether to contact individuals will be documented by the DPO.

- The DPO will 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 relating to the breach

- 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

- The DPO and Director of Finance & Operations will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, 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.

For example:

- Special category data (sensitive information) being disclosed via email (including safeguarding records)
  - If special category data 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 recall it
  - In any cases where the recall is unsuccessful, the DPO will 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 ensure we receive 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

Appendix 2 – Protocol for Transfer of Document between Schools

1. Data is defined as the following;
    - Any Documents which can identify the person/child in question.
    - This applies only to paper format documents/USB device.
2. If any physical data leaves a school in hard copy format the following steps must be taken;

Transfer of data

- Head would need to approve this before it is taken off site.
- Head would need to identify an appropriate person to take data off site taking account of the nature of the data (e.g. safeguarding data)
- The Head would need to identify a person at the destination who would receive the data
- The person taking the data needs to sign a form to provide acknowledgement that they are taking the data off site.
- The person taking the data would have to agree where the data is going and who is receiving it
- Data should not be transferred by public transport
- Data must be taken directly to the destination
- If going to another school, the other school would need to know what data will be delivered.

Receiving the data

- The school receiving the data would need to sign that the data as received
- The school receiving the data should inform the sending school that the data has been received

The above is industry standard with the Information Commissioners Office

The following forms should be used:

Data leaving the school

Type of data being taken from the school (e.g. HR file, pupil file, other information)	Data reference (e.g. name or further description)	Purpose data taken	Destination of data (e.g. school and a named individual)	Date/time taken	Signed by the person taking the data	Signed and dated by the Head as authority to take data	Comments

Data received by the school

Type of data being taken from the school (e.g. HR file, pupil file, other information)	Data reference (e.g. name or further description)	Purpose data received	Originating destination of data (e.g. school and a named individual)	Date & time received	The person receiving the data should; sign and date for receipt of data, inform the Head of the receiving school, and inform the Head of the sending school	Comments

Appendix 3: Retention schedule - Pupil records

Document type	Retention period	Action at end of retention period	Guidance/legislation
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 and 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.	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. See guidance on what to do if your school will close before the end of the retention period.
Special educational needs and disabilities (SEND), including SEND statements and accessibility plans	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.	See the SEND code of practice: 0 to 25 years. Retain as detailed in section 2 of the Limitation Act 1980.

Document type	Retention period	Action at end of retention period	Guidance/legislation
Attendance and absence	Every entry in the admission and attendance register – 6 years from the date of entry. Every back-up copy of the register – 6 years after the end of the school year that it relates to.		The School Attendance (Pupil Registration) (England) Regulations 2024.

Appendix 4: Retention schedule - Child protection records

Document type	Retention period	Action at end of retention period	Guidance/legislation
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 (transferred separately from the main pupil file).	Store 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, including unfounded allegations	Until the staff member's normal retirement age, or 10 years from the date of the allegation, whichever is later.	Dispose of records securely.	Keeping Children Safe in Education and Working together to safeguard children.

Appendix 5: Retention schedule - Finance records

Document type	Retention period	Action at end of retention period	Guidance/legislation
Contracts	6 years from the last payment on the contract.	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).

Appendix 6: Retention schedule - Governance records

Document type	Retention period	Action at end of retention period	Guidance/legislation
Admissions	3 years from the admission date.	Dispose of records securely.	Working together to improve school attendance.
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.
Curricular record	At least 1 year.	Dispose of records securely.	The Education (School Records) Regulations 1989 and 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.

Document type	Retention period	Action at end of retention period	Guidance/legislation
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 – for the life of the academy plus 6 years • Annual reports – 10 years from the date of the report • Board meeting records – 10 years from the date of the 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 and the academy trust governance guide. Academy Trust Handbook.

Appendix 7: Retention schedule - Health & safety records

Document type	Retention period	Action at end of retention period	Guidance/legislation
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 and 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 and Health surveillance – Record keeping.
Fire assessments	Life of the risk assessment plus 6 years.	Dispose of records securely.	The Regulatory Reform (Fire Safety) Order 2005. Retain as detailed in section 2 of the Limitation Act 1980.

Appendix 8: Retention schedule - Property records

Document type	Retention period	Action at end of retention period	Guidance/legislation
Maintenance records	6 years from the end of the financial year.	Dispose of records securely.	Record keeping (VAT Notice 700/21).
Title deeds	2 years from the end of the deed.	Dispose of records securely.	Section 2 of the Limitation Act 1980.

Appendix 9: Retention schedule - Staff records

Document type	Retention period	Action at end of retention period	Guidance/legislation
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.