Rebuilding Confidence. Restoring Futures.

Data Protection Policy

Date: 01.09.2026

Data Protection Officer:

Gemma Fulcher

The Sage School

Date to be reviewed: 01.09.2027 or whenever a significant change in legislation or guidance

Author: Gemma Fulcher

Contents

Aims 3
Legislation and Guidance 3
Definitions 4
The Data Controller 5
Roles and Responsibilities 6
Data Protection Principles 7
Collecting Personal Data 8
Special categories of personal data 8
Sharing Personal Data 11
Subject Access Requests and other Rights of Individuals 12
Photographs and Videos 15
Artificial Intelligence (AI) 16
Data Protection by Design and Default 17
Data Security and Storage of Records 18
Disposal of Records 18
Personal Data Breaches 19
Training 19
Monitoring 19
Appendix 1 – Records Retention Schedule 20

Aims

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

Legislation and Guidance

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

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

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used of identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.

Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Data Controller

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

The Sage School will be registered with the ICO as legally required once trading commences. The registration number is ZB919637.

Roles and Responsibilities

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

Data Protection Officer (DPO) – is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Governing Body and, where relevant, report to them their advice and recommendations on data protection issues. They will ensure all staff have completed relevant data protection training and manage any data protection breaches, as well as responding to Subject Access Requests (SARs) and Freedom of Information (FOI) requests. The DPO is also a point of contact for individuals whose data the provision processes, and the first point of contact for the ICO.

The DPO for The Sage School is Gemma Fulcher, and is contactable via gfulcher@thesageschool.co.uk

All Staff

Are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection right invoked by an individual, or transfer personal data outside the United Kingdom.
- If there has been a data breach.
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
- If they need help with any contracts or sharing personal data with third parties.

Data Protection Principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

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

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

Collecting Personal Data

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

Special categories of personal data

We will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent.
- The data needs to be processed to perform or exercise obligations or right in relation to employment, social security or social protection law.
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.

- The data needs to be processed for the establishment, exercise, or defence or 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.

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

Whenever we first collection personal data 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.

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 to do their jobs.

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

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 Records Retention Schedule, see Appendix 1.

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 not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies.

  When doing this, we will:

  - Only appoint suppliers and contractors which can provide sufficient guarantees that they comply with UK data protection law.
  - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
  - Only share data that the supplier or contractor needs to carry out their service.

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.

Subject Access Requests and other Rights of Individuals

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 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.

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 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.

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 cannot reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

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.

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, individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances).
- Prevent the use of their personal data for direct marketing.
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement).
- Be notified of a data breach (in certain circumstances).

- Make a complaint to the ICO.

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

Photographs and Videos

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

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.

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

Where the school takes photographs and videos uses may include:

- Within the school on notice boards, brochures and newletters etc.
- Outside of the school by external agencies such as a photographers, newspapers, campaigners.
- 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. See our safeguarding policy for more information on our use of photographs and videos.

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 and Google Bard.

The school recognises that AI has many uses to help pupils learn but also poses risks to sensitive personal data. The school will treat any use of AI to bully pupils in line with our behaviour policy.

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.

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

AI must not be used:

- to make independent decisions affecting students or staff
- to create harmful, misleading, or inappropriate content
- in assessment, recruitment, or administrative decision-making

AI-generated content must be identified where used and a Data Protection Impact Assessment (DPIA) must be conducted before new AI tools are introduced. Colleagues are NOT allowed to use any new software without prior permission from the DPO.

Data Protection by Design and Default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to 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.
- 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 United Kingdom, where different data protection laws will apply (where applicable).
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our DPO as well as all information we are required to share about how we use and process their personal data, via our privacy notices.
    - For all personal data that we hold, maintain an internal record of the type of data, type of data subject, how and why are using the data, any third-party recipients, any transfers outside of the United Kingdom and the safeguards for those, retention periods and how we are keeping the data secure.

Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alternation, processing, or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Staff or pupils who store personal information on their personal devices are expected to follow the same security procedures as for school owned equipment.
- Where we share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

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.

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.

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

Personal Data Breaches

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

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

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

Training

All staff 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 make it necessary.

Monitoring

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

Appendix 1 – Records Retention Schedule

The main aim of this Records Retention Schedule is to enable The Sage School to manage its records effectively and in compliance with data protection and other regulations. As an organisation it collects, holds, stores and creates significant amounts of data and information and this schedule provides a framework of retention and disposal of categories of information and records.

The Sage School is committed to the principles of data protection including the principle that information is only to be retained for as long as necessary for the purpose concerned.

The schedule below sets out the main categories of information that The Sage School holds, the length of time that it intends to hold them, and the reason for this. It also sets out the legal requirements for certain categories of document.

It also sets out the destruction procedure for records at the end of their retention period. The DPO shall be responsible for ensuring that this is carried out appropriately, and any questions regarding this Policy should be referred to them.

If a record or piece of information is reaching the end of its stated retention period, but it is of the view that it should be kept longer, the DPO should be contacted, who will make a decision as to whether it should be kept, for how long, and note the new time limit and reasons for extension.

Record Type	Reason for Retention	Retention
Records relating to the creation and distribution of circulars to staff, parents or pupils	Information and Record Management Society Toolkit Recommendation	Current plus one year
Visitor signing in books	Information and Record Management Society Toolkit Recommendation	Current plus six years
Subject Access Requests – unredacted and redacted copies (not originals)	Best practice	Six months if no further queries/correspondence else a year if further correspondence or complaints (case by case basis)
Freedom of Information requests and responses	Best practice	Six months if no further queries/correspondence else a year if further correspondence or complaints (case by case basis)
Whistleblowing – correspondence and report of investigation	Limitation Act 1980	Closure of case plus six years
Complaints	Best practice	Date of resolution of the complaint and three years - then review in cases of contentious disputes.
Documentation relating to an applicant who withdrew their application.	Information and Record Management Society Toolkit Recommendation	Six months after date of application.
Application forms, short listing forms and interview notes for unsuccessful candidates.	Information and Record Management Society Toolkit Recommendation	Six months from the date that the provision notifies a candidate of its decision.
Application forms and interview notes (for unsuccessful candidates) where consent has been provided to retain on file to identify if a person might be suitable for any other vacancies that may arise.	Information and Record Management Society Toolkit Recommendation	Two complete academic years.
Pre-employment vetting information – DBS copy or original certificate.	Information and Record Management Society Toolkit Recommendation	Six months

Copies of documents used for identity authentication for DBS and Asylum and Immigration Act purposes. UK Border Agency Documentation (Work Permit).	An Employer's guide to right to work checks (Home Office May 2005)	Termination plus two years.
Employee Personnel File: Job application form Qualifications certificates References Acceptance of Contract Contract acceptance and contract of employment and any variations Annual appraisal/ assessment records Salary assessment forms Training records Management Letters	Appraisal – to provide subsequent employment references. Salary assessment - To secure against challenge of accuracy of salary and related payments Contract – employment legislation (contractual) requirements Limitation Act 1980 (Section 2)	Termination of Employment plus six years
Exit Interview Notes/Letter of Resignation and other documentation relating to the termination of employment	To secure against challenge re deductions from earnings claim	Termination of Employment plus seven years
Confirmation of DBS outcome and any other associated documents e.g. risk assessment or certificate of good conduct. CRB self-declaration form; Barred List Check; Prohibition Check.	Recommended within the DfE Guidance, "Data Protection: a toolkit for schools", current version.	Termination of Employment plus twenty-five years
Formal disciplinary warnings – not child protection related	To be able to provide subsequent employment references.	Termination plus six years
Disciplinary Proceedings - Oral Warning Level 1 written warning	Information and Record Management Society Toolkit Recommendation	Date of warning plus six months
Disciplinary Proceedings - Level 2 written warning	Information and Record Management Society Toolkit Recommendation	Date of warning plus twelve months
Disciplinary Proceedings - Final warning	Information and Record Management Society Toolkit Recommendation	Date of warning plus eighteen months
Disciplinary Proceedings - Case not found	Information and Record Management Society	If child protection related - Until the person's normal retirement age or

	Toolkit Recommendation	10 years from the date of the allegation whichever is the longer then REVIEW. Allegations that are found to be malicious should be removed from personnel files. If not child protection related, dispose at the conclusion of the case.
Health and Safety Risk Assessments	Information and Record Management Society Toolkit Recommendation	Life of risk assessment plus three years
Records relating to accident/ injury at work	Health & Safety Legislation- ability to respond knowledgeably to subsequent injury compensation challenges	Date of incident plus twelve years.
Accident Books/Register Incident/near-miss reporting form/Accident & incident forms/First Aid Book/Head Bump Book/School Medicine Administering Form/Records of Medication Administered in Schools/Medical Form for local visits	Limitation Act 1970	3 years from the date of the last entry (or if the accident involves a child/young adult, then until that person reaches age 21).
Medical certificates – i.e. formal documents issued by a GP or hospital, Occupational Health service reports related to the fitness to work, and sickness absence record of an employee. Absence notifications and sickness self-certification forms.	To demonstrate proper processing of sickness and absence from work payments and processes.	Current year plus six years.
SMP, SAP, SSPP records, calculations, certificates (Mat B1s) or other medical evidence, notifications, declarations and notices including written notes of sickness absence meetings	Maternity Pay (General) Regulations 1986 (SI 1986/1960) revised 1999 (SI 1999/567)	Three years after the end of the tax year in which the leave period ends.
Statutory Sick Pay records, calculations, certificates, self-certificates	To demonstrate proper processing of sickness and absence from work payments and processes and to provide the ability to respond to	Six years after the employment ceases

	retrospective benefit claim enquiries of statutory bodies.	
Other special leave of absence including parental leave, maternity leave	To maintain an accurate record of employment and to respond to references and other benefit/agency or other organization enquiries.	Current year plus six years
Maternity pay records	Information and Record Management Society Toolkit Recommendation	Current year plus three years
Salaries & Wages Records	Information and Record Management Society Toolkit Recommendation	Seven years
Inland Revenue/HMRC correspondence	Statutory	Termination plus six years
Employer's Liability Insurance Certificate	Employers' Liability (Compulsory Insurance Regulation) 1998	Closure of a school and forty years
Insurance Policies (Excluding Liability)	Information and Record Management Society Toolkit Recommendation	Three years after lapse
Inventories of furniture and equipment	Information and Record Management Society Toolkit Recommendation	Current year plus six years
Records relating to management of software licences	Information and Record Management Society Toolkit Recommendation	Date of licence expiry plus six years
Annual Financial Statements	Companies Act 2006	Current year plus six years
Invoices, receipts, order books and requisitions, delivery notices and cheques.	Finance Act 1998 Taxes Management Act 1970	Current financial year plus six years
Records relating to the collection and banking of monies including bank statements	Companies Act 2006 Charities Act 2011	Current financial year plus six years

Information relevant for VAT purposes	Finance Act 1998 HMRC Notice 700/21	Current financial year plus six years
Free School Meals Registers	Information and Record Management Society Toolkit Recommendation	Current year plus six years
Leases	Limitations Act 1980	Expiry of lease plus twelve years
Pupil Educational Record – hard copy - The file should follow the pupil when he/she leaves the provision.	The Education (Pupil Information) (England) Regulations 2005, SI 2005 (2005 No: 1437	Retain whilst the child is at the provision and then transfer to their new school. If the new school is unknown or a child goes missing in education retain until the former pupil is 25 years of age.
Child Protection Record – Hard Copy File	KCSiE	Retain whilst the child is at the primary school and then transfer to their new school – refer KCSiE. If the new school is unknown or a child goes missing in education retain until the former pupil is 25 years of age.
Pupil Photographs and videos	Best Practice	Until no longer required.
Attendance Register	Regulation 14 – The Education (Pupil Registration) (England) Regulations 2006	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.
Special Educational Needs files, reviews, Individual Education Health and Care Plans and Statements of Special Educational Needs and amendments to those Statements. Advice and information provided to parents regarding educational needs.	Limitation Act 1980 Special Educational Needs and Disability Regulations 2014 Children and Families Act 2014, part 3	Retain whilst the child is at the provision and then transfer to their new school. If the new school is unknown or a child is missing in education retain until the former pupil is 25 years of age
Looked After Children (LAC) files.	Pupil Information Regulations 2005 (maintained schools only). Same approach applied in provision context.	Retain whilst the child is at the provision and then transfer to their new school. If the new school is unknown or a child is missing in education retain until the former pupil is 25 years of age.
Exam Register (from Exam Board), Internal Register, Exam Seating Plan	Best practice	One year after exam to which they relate.
Controlled assessments and internal tests	Information and Record Management Society	Until after results/ appeals have been processed

	Toolkit Recommendation	
Schemes of Work	Information and Record Management Society Toolkit Recommendation	Current year plus one year
Timetable	Information and Record Management Society Toolkit Recommendation	Current year plus one year
Mark Books	Information and Record Management Society Toolkit Recommendation	Current year plus one year
Record homework set	Information and Record Management Society Toolkit Recommendation	Current year plus one year
Pupils' Work	Information and Record Management Society Toolkit Recommendation	Where possible pupils' work should be returned to the pupil at the end of the academic year – else destroy
Records created by schools to obtain approval to run an Educational Visit outside the Classroom	Outdoor Education Advisers' Panel National Guidance website – http://oeapng.info – section 3 Legal Framework and Employer Systems and Section 4 Good Practice	Date of visit plus ten years
Parental consent forms for school trips where there has been no major incident.	Information and Record Management Society Toolkit Recommendation	Conclusion of the trip
Reports for outside agencies - where the report has been included on the case file created by the outside agency	Information and Record Management Society Toolkit Recommendation	Whilst child is attending the provision.
Referral forms	Information and Record Management Society Toolkit Recommendation	While the referral is current

Deletion of Records

When a record is at the end of its retention period, it should be dealt with in accordance with this Policy.

Confidential waste - this should be securely shredded on site. Anything that contains personal information should be treated as confidential.

Other records - other records can be deleted or placed in recycling bins where appropriate.

Individual responsibility

When faced with a decision about an individual record, you should ask yourself the following:

- Has the information come to the end of its useful life?
- Is there a legal requirement to keep this information or record for a set period?
- Would the information be likely to be needed in the case of any legal proceedings? In particular, is it potentially relevant to an historic child abuse enquiry? (Is the information contentious, does it relate to an incident that could potentially give rise to proceedings?)
- Would the record be useful for the organisation as a precedent, learning document, or for performance management processes?
- Is the record of historic or statistical significance?

If the decision is made to keep the record, this should be referred to the DPO and reasons given.

List of Records

A list of hard copy records to be destroyed in bulk at the end of a retention period must be maintained and should include:

- File reference (or other unique identifier).
- File title (or brief description) and number of files.
- The name of the authorising officer and the date action taken.

This list should be kept in an Excel spreadsheet or similar suitable format.