



Diocese of Salisbury
Academy Trust
'Beyond expectations for all of God's children'

Retention and Destruction Policy

Policy Date: May 2023

Review Date: May 2026

This policy is to be adopted by all Academies

1 Policy statement

- 1.1 The Diocese of Salisbury Academy Trust ('the Trust') recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the Trust and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited.

2 Scope of this policy

- 2.1 This policy applies to all records created, received or maintained by staff of the Trust in any form in the course of carrying out its functions.
- 2.2 Records are defined as all those documents which facilitate the business carried out by the Trust and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.
- 2.1 A small percentage of the Trust's records will be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the County Archives Service.

3 Responsibilities

- 3.1 The Trust has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Data Protection Officer of the Trust.
- 3.2 The person responsible for records management in the Trust will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.
- 3.1 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the Trust's records management guidelines.

4 Relationship with existing policies

- 4.1 This policy has been drawn up within the context of:
 - (a) Freedom of Information policy
 - (b) Data Protection policy
 - (c) Other legislation or regulations (including audit, equal opportunities and ethics) affecting the Trust.

5 Retention Guidelines

- 5.1 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. The retention schedule lays down the basis for normal processing under both the Data Protection Act 1998 and the Freedom of Information Act 2000.
- 5.2 The Trust has adopted the retention schedule from the 2016 IRMS Information Management Toolkit for Schools (see appendix 3).
 - 5.2.1 This retention schedule contains recommended retention periods for the different record series created and maintained by schools in the course of their business.
 - 5.2.2 The schedule refers to all information regardless of the media in which it is stored.
 - 5.2.3 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 Data Protection Act 1998 and the Freedom of Information Act 2000.
 - 5.2.4 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.
- 5.3 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 record series regardless of the media in which they are stored.
 - 5.3.1 Members of staff should be aware that once a Freedom of Information request is received or a legal hold imposed then records disposal relating to the request or legal hold must be stopped.
 - 5.3.2 By adhering to the retention guidelines, members of staff can be confident about safe disposal information at the appropriate time.
 - 5.3.3 Use of the retention guidelines ensures that information which is subject to Freedom of Information and Data Protection legislation will be available when required.
 - 5.3.4 Use of the retention guidelines ensures that the Trust is not maintaining and storing information unnecessarily.
- 5.4 Where appropriate the retention schedule should be reviewed and amended to include any new record series created and remove any obsolete record series.

6 Safe disposal of records which have reached the end of their administrative life

- 6.1 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- 6.2 In each location, local records managers must ensure that records that are no longer required for business use are reviewed as soon as possible under the criteria set out so that only the appropriate records are destroyed. The local review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the organisation for research or litigation purposes.
- 6.3 Whatever decisions are made they need to be documented as part of the records' management

7 Safe destruction of records

- 7.1 All records containing personal information, or sensitive policy information should be made either unreadable or un-reconstructable.
 - 7.1.1 Paper records should be shredded using a cross-cutting shredder
 - 7.1.2 CDs / DVDs / Floppy Disks should be cut into pieces
 - 7.1.3 USB memory sticks will not be used – old ones will be dismantled and destroyed
 - 7.1.4 Audio / Video Tapes and Fax Rolls should be dismantled and shredded
 - 7.1.5 Hard Disks should be dismantled and sanded
 - 7.1.6 Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in with the regular waste or a skip unless there is no other alternative.
 - 7.1.7 There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.
- 7.2 Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction.
 - 7.2.1 Staff working for the external provider should have been trained in the handling of confidential documents.
 - 7.2.2 The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.
 - 7.2.3 It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received they MUST still be provided.

- 7.3 Where records are destroyed internally, the process must ensure that all records are recorded and authorised to be destroyed by a Senior Manager and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed.
- 7.4 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:
- a) File reference (or other unique identifier);
 - b) File title (or brief description); Number of files and date range
 - c) The name of the authorising officer
 - d) Date action taken
- 7.5 Following this guidance will ensure that the school is compliant with the Data Protection Act 1998, the Freedom of Information Act 2000.

8 Transfer of records to the archives

- 8.1 Where records have been identified as being worthy of permanent preservation arrangements should be made to transfer the records to the County Archives Service.
- 8.2 The school should contact the local record office if there is a requirement to permanently archive the records, and the records will continue to be managed via the DPA 1998 and the FoIA 2000.

9 Transfer of information to other media

- 9.1 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.
- 9.2 Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media. It is essential to have procedures in place so that conversion is done in a standard way. This means that organisations can prove that the electronic version is a genuine original and could not have been tampered with in any way. Reference should be made to 'British Standard 10008:2008 'Evidential weight and legal admissibility of electronic information' when preparing such procedures.

10 Digital Continuity

- 10.1 The long term preservation of digital records is more complex than the retention of physical records. A large number of organisations create data in electronic format which needs to be retained for longer than 7 years. If this data is not retained in accessible formats the organisation will be unable to defend any legal challenge which may arise. In order to ensure that digital records are retained in a way that ensures they can be retrieved in an accessible format when they are required, all records which are required to be retained for longer than 6 years should be part of a digital continuity statement (Appendix 1). The average life of a computer system can be as little as 5 years, however, as digital continuity is resource intensive, only

records which are required to be retained for 6 years (in line with the Limitation Act 1980) or longer should be subject to digital continuity statements

- 10.2 A digital continuity statement will not need to be applied to all the records created by the school. The retention schedule should indicate which records need to be subject to a digital continuity statement. Any record which needs to be preserved for longer than 6 years needs to be subject to a digital continuity statement. Appropriate records need to be identified as early in their lifecycle as possible so that the relevant standards can be applied to them and conversely any records which do not need to be included in the policy should also be identified in the early part of the lifecycle. Digital continuity statements should only be applied to principal copy records.
- 10.3 Responsibility for the management of the digital continuity strategy, including the completion of the digital continuity statements should rest with one named post holder. This will ensure that each information asset is “vetted” for inclusion in the strategy and that resources are not allocated to records which should not be included in the strategy.
- 10.4 Where possible records subject to a digital continuity statement should be “archived” to dedicated server space which is being backed up regularly. Where this is not possible the records should be transferred to high quality CD/DVD, if they are to be included with paper documentation in a paper file or onto an external hard drive which is clearly marked and stored appropriately. Records stored on these forms of storage media must be checked regularly for data degradation. Flash drives (also known as memory sticks) must not be used to store any records which are subject to a digital continuity statement – our Trust policy is that they should not be used at all. This storage media is prone to corruption and can be easily lost or stolen. Storage methods should be reviewed on a regular basis to ensure that new technology and storage methods are assessed and where appropriate added to the digital continuity policy.
- 10.5 Migration of electronic data must be considered where the data contained within the system is likely to be required for longer than the life of the system. Where possible system specifications should state the accepted file formats for the storage of records within the system. If data migration facilities are not included as part of the specification, then the system may have to be retained in its entirety for the whole retention period of the records it contains. This is not ideal as it may mean that members of staff have to look on a number of different systems to collate information on an individual or project. Software formats should be reviewed on an annual basis to ensure usability and to avoid obsolescence.
- 10.6 In the same way as physical records can degrade if held in the wrong environmental conditions, electronic records can degrade or become corrupted. Whilst it is relatively easy to spot if physical records are becoming unusable it is harder to identify whether an electronic record has become corrupted, or if the storage medium is becoming unstable. When electronic records are transferred from the main system to an external storage device, the data should be backed up and two safe copies of the data should be made. The data on the original device and the back-ups should be checked periodically to ensure that it is still accessible. Additional back-ups of the data should be made at least once a year and more frequently if appropriate. Where possible digital records should be archived within a current

system, for example, a designated server where “archived” material is stored or designated storage areas within collaborative working tools such as SharePoint.

- 10.7 Records which are the subject of a digital continuity statement must be “archived” in one of the internationally recognised file formats.

Exemplar Digital Continuity Strategy Statement

Our digital continuity statement is a work in progress and will include the following information:

1. Statement of business purpose and statutory requirements for keeping records

The statement should contain a description of the business purpose for the information assets and any statutory requirements including the retention period for the records. This should also include a brief description of the consequences of any loss of data. By doing this the records owner will be able to show why and for how long the information assets needs to be kept. As digital continuity can be resource intensive, it is important that the resources are allocated to the information assets which require them.

2. Names of the people/functions responsible for long term data preservation

The statement should name the post-holder who holds responsibility for long term data preservation and the post holder responsible for the information assets. The statement should be updated whenever there is a restructure which changes where the responsibility for long term data preservation is held. If the responsibility is not clearly assigned there is the danger that it may disappear as part of a restructure process rather than be reassigned to a different post.

3. Description of the information assets to be covered by the digital preservation statement

A brief description of the information asset taken from the IAR.

4. Description of when the record needs to be captured into the approved file formats

The record may not need to be captured in to the approved file format at its creation. For example, an MSWord document need not be converted to portable document format until it becomes semi-current. The digital preservation statement should identify when the electronic record needs to be converted to the long term supported file formats identified above.

Workflow process diagrams can help identify the appropriate places for capture.

5. Description of the appropriate supported file formats for long term preservation

This should be agreed with the appropriate technical staff.

6. Retention of all software specification information and licence information

Where it is not possible for the data created by a bespoke computer system to be converted to the supported file formats, the system itself will need to be mothballed. The statement must contain a complete system specification for the software that has been used and any licence information which will allow the system to be retained in its entirety. If this information is not retained it is possible that the data contained within the system may become inaccessible with the result that the data is unusable with all the ensuing consequences.

7. Description of where the information asset is to be stored.

See section 4 above.

8. Description of how access to the information asset is to be managed within the data security protocols

The data held for long term preservation must be accessible when required but also must be protected against the standard information security requirements which are laid down for records within the authority. The statement must contain the policy for accessing the records and the information security requirements attached to the information assets.

Appropriate Storage for Physical Records

Records must be stored in the workplace in a way that does not cause a health and safety hazard. Records must not be stored in corridors or gangways and must not impede or block fire exits. There should be where appropriate, heat/smoke detectors connected to fire alarms, a sprinkler system and the required number of fire extinguishers. The area should be secured against intruders and have controlled access as far as possible to the working space.

Storage areas should be regularly monitored and checked for any damage or emerging risks, especially during holiday periods.

The following are hazards which need to be considered before approving areas where physical records can be stored.

Environmental Damage - Fire

Records can be damaged beyond repair by fire. Smoke and water damage will also occur to records which have been in a fire, although generally records damaged by smoke or water can be repaired. Core records should be kept in cabinets or cupboards. Metal filing cabinets will usually suffice, but for important core records, fire proof cabinets may need to be considered. However, fireproof cabinets are expensive and very heavy so they should only be used in special circumstances. Records which are stored on desks or in cupboards which do not have doors will suffer more damage than those which are stored in cupboards/cabinets which have close fitting doors.

Environmental Damage - Water

Records damaged by water can usually be repaired by a specialist document salvage company. The salvage process is expensive, therefore, records need to be protected against water damage where possible. Where flooding is involved the water may not always be clean and records could become contaminated as well as damaged.

Records should not be stored directly under water pipes or in places which are liable to flooding (either from excess rainfall or from the overflow of toilet cisterns). Records should be stored in cabinets/cupboards with tight fitting doors which provide protection from water ingress. Records stored on desks or in cabinets/cupboards without close fitting doors will suffer serious water damage.

Records should be stored at least 2 inches off the ground. Most office furniture stands 2 inches off the ground. Portable storage containers (i.e. boxes or individual filing drawers) should be raised off the ground by at least 2 inches. This is to ensure that in the case of a flood that records are protected against immediate flood damage.

Storage areas should be checked for possible damage after extreme weather to ensure no water ingress has occurred.

Environmental Damage – Sunlight

Records should not be stored in direct sunlight (e.g. in front of a window). Direct sunlight will cause records to fade and the direct heat causes paper to dry out and become brittle.

Environmental Damage – High Levels of Humidity

Records should not be stored in areas which are subject to high levels of humidity. Excess moisture in the air can result in mould forming on the records. Mould can be a hazard to human health and will damage records often beyond repair.

The temperature in record storage areas should not exceed 18°C and the relative humidity should be between 45% and 65%.

Temperature and humidity should be regularly monitored and recorded. Storage areas should be checked for damage after extreme weather conditions to reduce the risk of mould growth.

Environmental Damage – Insect/Rodent Infestation

Records should not be stored in areas which are subject to insect infestation or which have a rodent problem (rats or mice).

Appendix 3

Data Retention Schedule

Management of the School

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.1 Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL ¹
1.1.2 Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
Principal Set (signed)			PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
Inspection Copies ²			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.
1.1.3 Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
1.1.4 Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL

¹ In this context SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a cross cut shredder.

² These are the copies which the clerk to the Governor may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

1.1 Governing Body				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.5 Instruments of Government Including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.6 Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.7 Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8 Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
1.1.9 Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.1.10 Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
1.1.11 Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

Please note that all information about the retention of records concerning the recruitment of Head Teachers can be found in the Human Resources section below.

1.2 Head Teacher and Senior Management Team				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.2.1 Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate
1.2.2 Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3 Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
1.2.4 Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5 Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL
1.2.6 Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
1.2.7 School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

1.3 Admissions Process					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
1.3.1 All records relating to the creation and implementation of the School Admissions' Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL	
1.3.2 Admissions – If the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL	
1.3.3 Admissions – If the appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL	
1.3.4 Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made. ³	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.	
1.3.5 Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL	
1.3.6 Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL	

1.3 Admissions Process					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
1.3.7 Supplementary Information form including additional information such as religion, medical conditions etc	Yes				
For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL	
For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL	

1.4 Operational Administration					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
1.4.1 General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL	
1.4.2 Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL	
1.4.3 Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL	
1.4.4 Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL	
1.4.5 Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL	
1.4.6 Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL	

2. Human Resources

This section deals with all matters of Human Resources management within the school.

2.1 Recruitment				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.1.1 All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2 All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.1.3 All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4 Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June 2014; Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	
2.1.5 Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff’s personal file	
2.1.6 Pre-employment vetting information – Evidence proving the right to work in the United Kingdom ⁴	Yes	An employer’s guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	
2.2 Operational Staff Management				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.2.1 Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2 Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3 Annual appraisal/ assessment records	Yes		Current year + 5 years	SECURE DISPOSAL
2.3 Management of Disciplinary and Grievance Processes				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.3.1 Allegation of a child protection nature against a member of staff including where the allegation is unfounded ⁵	Yes	“Keeping children safe in education Statutory guidance for schools and colleges March 2015”; “Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015”	Until the person’s normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2 Disciplinary Proceedings	Yes			
oral warning			Date of warning ⁶ + 6 months	
written warning – level 1			Date of warning + 6 months	SECURE DISPOSAL
written warning – level 2			Date of warning + 12 months	[If warnings are placed on personal files then they must be weeded from the file]
final warning			Date of warning + 18 months	
case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

2.4 Health and Safety				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.4.1 Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2 Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3 Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
2.4.4 Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
Adults			Date of the incident + 6 years	SECURE DISPOSAL
Children			DOB of the child + 25 years	SECURE DISPOSAL
2.4.5 Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL
2.4.6 Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7 Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8 Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL

⁴ Employers are required to take a "clear copy" of the documents which they are shown as part of this process

2.5 Payroll and Pensions				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.5.1 Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2 Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

3. Financial Management of the School

This section deals with all aspects of the financial management of the school including the administration of school meals.

3.1 Risk Management and Insurance				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.1.1 Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL

3.2 Asset Management				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.2.1 Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2 Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

⁵ This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention.

⁶ Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter please contact your Safeguarding Children Officer for further advice.

3.5 School Fund					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
3.5.1	School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL

3.6 School Meals Management					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
3.6.1	Free School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL
3.6.2	School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL

4. Property Management

This section covers the management of buildings and property.

4.1 Property Management					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
4.1.1	Title deeds of properties belonging to the school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
4.1.2	Plans of property belong to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL

4.2 Maintenance					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL

5. Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above.

5.1 Pupil's Educational Record				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.1.1 Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: <ul style="list-style-type: none"> to another primary school to a secondary school to a pupil referral unit If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2 Examination Results – Pupil Copies	Yes			
Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
Internal			This information should be added to the pupil file	

5.1 Pupil's Educational Record				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention				
5.1.3 Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4 Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.

5.2 Attendance					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
5.2.1	Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL
5.2.2	Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3	Advice and Information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold

6. Curriculum Management

6.1 Statistics and Management Information					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records – Results	Yes			
				The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATS results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2 Implementation of Curriculum					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
6.2.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.2	Timetable	No		Current year + 1 year	
6.2.3	Class Record Books	No		Current year + 1 year	
6.2.4	Mark Books	No		Current year + 1 year	
6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	

7. Extra Curricular Activities

7.1 Educational Visits outside the Classroom					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	
7.2 Walking Bus					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
7.2.1	Walking Bus Registers	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]
7.3 Family Liaison Officers and Home School Liaison Assistants					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	
7.3.1	Day Books	Yes		Current year + 2 years then review	
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	
7.3.3	Referral forms	Yes		While the referral is current	
7.3.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	
7.3.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
7.3.6	Group Registers	Yes		Current year + 2 years	

8. Central Government and Local Authority

This section covers records created in the course of interaction between the school and the local authority.

8.1 Local Authority					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
8.1.1	Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
8.1.2	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3	School Census Returns	No		Current year + 5 years	SECURE DISPOSAL
8.1.4	Circulars and other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL

8.2 Central Government					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
8.2.1	OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2	Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL
8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL