Record Retention Policy and Retention Schedule

Version:	1
Trust Board Approval:	Jan 22
Date of Last Review:	Jan 22
Date of Next Review:	Jan 25

Contents

1 Introduction

1.1. Aldridge Education is committed to maintaining the confidentiality of information we hold about pupils, parents, staff and volunteers. In line with the requirements of the General Data Protection Regulation (GDPR), the Trust has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were originally intended.

1.2. This policy outlines how information will be processed, stored, accessed, monitored, retained and disposed of, to meet the Trust's statutory requirements to comply with the General Data Protection Regulation and other relevant statutory legislation.

1.3. Information assets (or 'records') are defined as all documents and materials, regardless of format, which facilitate the activities carried out by the Trust. These records may be created, received and maintained in hard copy or electronically (including emails).

1.4. The Trust will manage records in line with the Records Retention Schedule, to ensure that it can meet Freedom of Information requests and respond to data subject access requests under the GDPR and other financial or legal requirements.

1.5. The retention periods are based on the latest guidance from the Information Records Management Society (IRMS) and are not an exhaustive list of records that may be kept by academies/Trust. Where the IRMS has not provided guidance for disposal methods or retention periods, good practice recommendations have been provided. Schools should consult the Trust's Data Protection Officer for further guidance.

2. Legal Framework and Related Policies

2.1. This policy has due regard to the following legislation and guidance including, but not limited to, the following:

- General Data Protection Regulation (2018)
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)
- Data Protection Act 2018
- The Education Regulations 2014 (with reference to educational record)
- Information Records Management Society 'Information Management Toolkit for Academies' 2020

2.2. The following Trust policies also apply

- E Safety Policy
- Data Protection Policy
- Privacy Notices

- Acceptable Use Policy (Staff)
- Code of Conduct for Staff
- Safeguarding and Child Protection Policy
- HR Policies including Grievance, Disciplinary and Capability
- Social Media Policy

3. Responsibilities

3.1. The Trust has a corporate responsibility to maintain its records and records management systems in accordance with legislation.

3.2. The Trust Data Protection Officer is responsible for providing guidance and advice on good records management practice and promoting compliance with this policy. Such guidance is formulated within the context of existing Trust policies and guidelines regarding data protection, national legislation and sector-wide standards.

3.3. The Principal at each academy (supported by the school's Data Protection Lead) is responsible for ensuring this policy is implemented and that all records are stored securely, in accordance with the retention periods outlined, recorded, and are disposed of correctly.

3.4. The Principal may delegate to the Data Protection Lead in their school the responsibility for maintaining the information asset register (IAR) and the record of processing activity (RoPA) in accordance with per Article 30 of GDPR and steps 2–5 of the Department for Education (DfE) Data Protection Toolkit for Schools.

3.5. It is essential that all records have an identified Information Asset Owner (IAO) whose responsibility it is to ensure records are managed in accordance with Trust Data Protection Policies and the GDPR.

3.6. The Trust has adopted GDPR Software System as the Trust's tool for holding the Information Asset Register. The Data Protection Officer will provide support and guidance to individual schools to ensure this is kept up to date. Maintaining the RoPA should not be a one-off activity and the document needs to be regularly reviewed.

3.7. Records containing Personally Identifiable Information (PII) must be logged in a school's GDPR software system to ensure the school meets its obligations under GDPR to have a current data map. For example, 'HR records' would be entered in the GDPR system, outlining the data fields, the purpose for processing/ retention, the IAO, location, and retention. This information must be reviewable by the school's Data Protection Lead and Trust's Data Protection Officer to ensure that data sources are managed in line with policy and can be identified in the event of a Data Subject Access Request.

3.8. All Trust staff are responsible for ensuring that any records for which they are responsible or which they process are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3.9. Each school (including Adult Learning) within the Trust is individually responsible for the management of their records generated by its activities.

3.10. The Trust HR Onboarding and Offboarding procedures ensure managed access to systems and records. This should include limits on how users access the resources, which user actions can be performed, and what resources users can access. Where individuals are given access to personal or sensitive data, training is provided to ensure that they are aware of the increased risks, responsibilities (including confidentiality responsibilities), and the consequences of unauthorised access.

4. Storage and security

4.1. As a general principle, the Trust favours electronic storage of information, in order to:

a) assist data sharing where appropriate
b) ensure access to information by authorized users
c) ensure availability of information in the event of disaster recovery or business continuity
d) minimize duplication of data e.g. information stored in a school's management information system will not also be printed and stored in a paper file.

4.2. The Trust's Acceptable Use Policy for Staff details measures to ensure safe and secure storage and access to electronic records and should be read in conjunction with this policy.

4.3. Schools must ensure that key information is securely stored and can still be accessed in the event of a data breach including loss of access due to fire or flood or malware, to limit any loss or theft of data.

4.4. It is strongly recommended that schools should store key information in DfE approved enterprise-level cloud storage such as Microsoft Office or G Suite, to ensure access in the event of school closures.

4.5. Confidential paper records must be kept in a locked filing cabinet, drawer or safe, with restricted access. They must not be left unattended or in clear view when held in a location with general access.

4.6. Staff must not use computer/ laptop hard drives (c:/drive) or the desktop to store personal store information as this drive is not backed up. Use your personal drive only for information that is confidential or personal or does not need to be shared within the Trust. Use cloud storage such as Microsoft One Drive or Google Drive where available to do so.

4.7. All electronic devices must be password-protected to protect the information on the device in case of theft.

4.8. All members of staff are provided with their own secure login and password which must not be divulged to anyone else.

4.9. All staff members should implement a clear desk policy to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.

4.10. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of school containing sensitive information should be supervised at all times.

4.11. The physical security of the Trust's buildings and storage systems, and access to them, is reviewed by the Director of Estates, the Trust Lead for Inclusion (safeguarding matters) and the DPO to evaluate the risks of vandalism, burglary or theft, safeguarding risk or data security and provide guidance on measures to reduce risk accordingly.

5. Email

5.1. Staff, governors and trustees must not use their own personal email addresses for school/Trust purposes.

5.2. Emails containing sensitive or confidential information must be encrypted to ensure that only the recipient is able to access the information. Microsoft Office and Gmail have system encryption that can be used.

5.3. The consequences of an e-mail containing sensitive information being sent to an unauthorised person can result in a fine of up to 20 million euros (or equivalent in sterling) or restrictions on processing from the Information Commissioner, along with adverse publicity for your Trust.

Confidential or sensitive information should be sent by a secure encrypted e-mail or data transfer system. Personal information (such as a pupil's name) should never be used in the subject line of an e-mail.

5.4. Circular emails to parents should by preference be sent using third-party communication systems to ensure security of recipients. Where emails must be sent, they must be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

5.5. E-mail systems are commonly used to store information which should be stored somewhere else. E-mail and attachments that need to be kept should be identified by content, for example: Does it form part of a pupil record? Is it part of a contract? Does it relate to an employee? They should then be saved into an appropriate electronic filing system. Where the text of the e-mail adds to the context or value of the attached documents, it may be necessary to keep the whole e-mail.

Information contained within e-mails may need to be transferred or logged in the appropriate place (e.g., the management information system (MIS) or behaviour management system). Once this is done, the original can be deleted.

5.6. The retention period for keeping information held as email files should correspond with the types of records found in the Trust Retention below.

5.7. All staff should adopt best practice guidance and routinely delete email over 24 months old. This will assist greatly in reducing the amount of information potentially disclosable in the event that a subject access request is received.

6. Confidentiality

6.1. It may be appropriate to label records or archives as 'Confidential'. This does not exempt the record from being admissible under the Freedom of Information Act 2000. Further information can be obtained from the Trust's Freedom of Information Policy.

6.2. The Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

6.3. E-mails may be disclosed in response to a Freedom of Information or Subject Access Request and in legal cases. Electronic messages can be legally binding

6.4. Before sharing data, staff must always ensure that:

- They have consent from data subjects to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice

7. Information Audit

7.1. The Data Protection Officer will conduct an information audit on an annual basis with the school's Data Protection Lead against all information held by the Trust and each academy to evaluate the information each is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR.

7.2 The audit may involve interviews or questionnaires with key operational staff to identify information and information flows which may include the following:

- Paper documents and records
- Electronic documents and records
- Databases
- Sound recordings

- Video and photographic records
- Hybrid files, containing both paper and electronic information
- Archives and archive logs

8. Retention Schedule

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

8.2. Managing records against the retention schedule is deemed to be "normal processing" under the General Data Protection Regulation, Data Protection Act 2018 and the Freedom of Information Act 2000. Members of staff should be aware that once a Freedom of Information request is received or a legal hold imposed, then records disposal must be stopped.

8.3. 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 General Data Protection Regulation, Data Protection Act 2018 and the Freedom of Information Act 2000.

8.4. Managing records 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 those laid out in this document, the reasons for this need to be documented in each school's Archive Log.

9.Transferring Pupil Records

9.1. Where a pupil transfers to a new school, it is vital to ensure swift transfers of information to the new school to ensure appropriate decisions can be made regarding a pupil, using relevant and accurate information.

9.2. The pupil record should not be weeded before transfer, unless any duplicates or records with a short retention period have been included; these can be removed and securely destroyed.

9.3. The following should be transferred to the next school within 15 school days of receipt of confirmation that a pupil is registered at another school.

9.4. Common Transfer File (CTF) from the School Information Management System when used

9.5. Any elements of the pupil record, held in any format, not transferred as part of the CTF

9.6. SEN or other support service information, including behaviour, as only limited information may be included in the CTF

9.7. Child protection information; this must be sent as soon as possible by the Designated Safeguarding Lead (DSL) or a member of their team to their equivalent at the new Trust.

9.8. Academies must ensure the information is kept secure and traceable during transfer. Pupil records should not be sent by post, even Special Delivery. They may be delivered or collected in person, with signed confirmation.

9.9. If held electronically, records may be sent to a named contact via secure encrypted email, or other secure transfer method.

910. If the pupil is transferring to an independent school or a post-16 establishment, the existing school/college should transfer copies of relevant information only and retain the original full record as the last known school.

9.11. If a request is received to transfer the pupil record or other information about a pupil to a school outside of the European Union (EU), the school seek written consent from the parent prior to forwarding any information to the new school and should retain a copy of the original full record as the last known school.

10.Organisation and Storage

10.1. Administrators / Managers are strongly recommended to create electronic filing systems (folders) which reflect the categories below in order to ensure efficient management of records on an ongoing basis and timely disposal as required.

10.2. Where information is held in third party systems e.g. SIMS, there is no requirement to also hold a paper copy and the duplication of records is not considered good practice.

10.3. All records must be securely stored. Schools must risk assess those records held only in paper format, assessing the risks of loss of access, for example through fire or theft, in particular those records of a confidential nature, such as personnel records and consider appropriate back up.

10.4. Electronic records must be backed up whether through DfE approved enterprise-level cloud storage such as Microsoft Office 365 or GSuite.

11.Disposal of Data

11.1. A trust-wide contract for the secure destruction of paper records has been facilitated for all schools in the Trust. All records produced through the day- to- day operations of the Trust containing personal identifying information must be disposed of through this route.

11.2. Where the Retention Schedule mentions SECURE DISPOSAL, this must be via the Trust's confidential waste disposal service which provides confidential waste consoles in all schools, or via crosscut shredder.

11.3. All schools and the central team must keep an electronic log of archived records, held and managed by the school Data Protection Lead. The log must record the date and method of secure destruction of records due for destruction at the end of the requisite retention period.

11.4. Data Protection Leads are responsible for risk assessing whether records normally due for destruction, e.g. complaints records, should be retained for longer and recording this on the archives log.

11.5. IT cluster managers will provide support and guidance to schools and central teams regarding secure disposal of computer and electronic records through approved recycling services.

13.Monitoring and Review

12.1. This policy will be reviewed every three years by the Trust Data Protection Officer or when best practice guidance is updated.

RECORDS RETENTION SCHEDULE

1. MANAGEMENT OF THE SCHOOL/TRUST

This section contains retention periods connected to the general management of the School/Trust.
It covers the work of Trust and School Committees, the Principal and SLTs, the admissions process and operational administration.

1.1 Trust and School Committee

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
1.1.1	Agendas for Committee 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	
1.1.2	Minutes of Committee meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff	Date of meeting + 6 years, then review	SECURE DISPOSAL	
	Trust / School set (unredacted for confidential information)	There may be data protection issues if the meeting is dealing with confidential issues relating to staff	PERMANENT	If the school / Trust is unable to store these then they should be offered to archives	
	Inspection and Public Copies (redacted for confidential information)		Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.	
1.1.3	Reports presented to the Committees	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 parents' meeting held under Section 33 of the Education Act 2002	No	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL	
1.1.5	Instruments of Government including Articles of Association	No	PERMANENT	These should be retained in the school/Trust whilst the school/Trust is open and then offered to archives when the school/Trust closes	
1.1.6	Trusts and Endowments managed by the School / Trust	No	PERMANENT	These should be retained in the school/Trust whilst the school/Trust is open and then offered to archives when the school/Trust closes	

1.1.7	Action plans created and administered by the School/Trust or Committees	No	Life of the action plan + 3 years	SECURE DISPOSAL	
1.1.8	Policy documents created and administered by the School/Trust or Committees	No	Life of the policy + 3 years	SECURE DISPOSAL	
1.1.9	Records relating to complaints dealt with by the School/Trust or Committees	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 Regulations 2002	No	Date of report + 10 years	SECURE DISPOSAL	

1.2 Central Team, Principal and Senior Leadership Teams (SLTs)

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
1.2.1	Log books of activity in the School / Trust	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 archives if appropriate	
1.2.2	Minutes of Central Team and School SLT meetings and the meetings of other internal administrative bodies	There may be data or minutes that 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 Central Team, Principal or SLTs	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 Central Team, Principals, SLTs, heads of year/depts 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 Central Team, Principals, SLTs, heads of year/depts 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	Trust or School Development Plans	No	Life of the plan + 3 years	SECURE DISPOSAL	

1.3 Admissions Process					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.3.1	All records relating to the creation and implementation of the School Admissions Policy	No	Life of the policy + 3 years then review	SECURE DISPOSAL	
1.3.2	Admissions – if the admission is successful	Yes	Date of admission + 1 year	SECURE DISPOSAL	
1.3.3	Admissions – if the appeal is unsuccessful	Yes	Resolution of case + 1 year	SECURE DISPOSAL	
1.3.4	Register of Admissions	Yes	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.	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	Current year + 1 year	SECURE DISPOSAL	
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc	Yes	This information should be added to the pupil file	SECURE DISPOSAL	
	For successful admissions	Yes	This information should be added to the pupil file	SECURE DISPOSAL	
	For unsuccessful admissions	Yes	Until appeals process completed	SECURE DISPOSAL	

1.4 Operational Administration					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.4.1	General files	No	Current year + 5 years then review	SECURE DISPOSAL	
1.4.2	Records relating to the creation and publication of the school / trust 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 Alumni	No	Current year + 6 years then REVIEW	SECURE DISPOSAL	

2. HUMAN RESOURCES

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

2.1 Recruitment

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
2.1.1	All records leading up to the appointments – successful candidates	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 the successful candidate + 6 months	SECURE DISPOSAL	
2.13	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 and all other information retained for 6 months	SECURE DISPOSAL	
2.1.4	Pre-employment vetting information – DBS Checks	No	The school/Trust does not have to keep copies of DBS certificates. If the School/Trust 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	These should be checked and a note kept of what was seen and what has been checked and placed on the member of staff's personal file		
2.1.6	Pre-employment vetting information – Evidence proving the right to work in UK	Yes	Where possible these documents should be added to the Staff Personal File but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than 2 years		

2.2 Operational Staff Management

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
2.2.1	Staff Personal File	Yes	Termination of Employment + 6 years	SECURE DISPOSAL	
2.2.2	Timesheets, annual leave and absence records	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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded	Yes	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 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]	
	written warning – level 1		Date of warning + 6 months		
	written warning – level 2		Date of warning + 12 months		
	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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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			
	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	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	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	
2.4 Payroll and Pensions					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.5.1	General payroll and pension information	Yes	Current year + 6 years	SECURE DISPOSAL	
2.5.2	Maternity pay records	Yes	Current year + 3 years	SECURE DISPOSAL	
2.5.3	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	Current year + 6 years	SECURE DISPOSAL	

3. FINANCIAL MANAGEMENT OF THE SCHOOL/TRUST

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

3.1 Risk Management and Insurance

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
3.1.1	RPA certificates	No	Closure of the school + 40 years	SECURE DISPOSAL	
3.1.2	Any other Employer's Liability Insurance Certificate	No	Closure of the school + 40 years	SECURE DISPOSAL	

3.2 Asset Management

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
3.2.1	Inventories of furniture, equipment and other valuable assets	No	Current year + 6 years	SECURE DISPOSAL	
3.2.2	Burglary, theft and vandalism reports	No	Current year + 6 years	SECURE DISPOSAL	

3.3 Accounts and Statements including Budget Management

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
3.3.1	Annual Accounts	No	Current year + 6 years	STANDARD DISPOSAL	
3.3.2	Student Grant applications	Yes	Current year + 3 years	SECURE DISPOSAL	
3.3.3	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No	Life of the budget + 3 years	SECURE DISPOSAL	
3.3.4	Invoices, receipts, order books and requisitions, delivery notices	No	Current financial year + 6 years	SECURE DISPOSAL	
3.3.5	Records relating to the collection and banking of monies	No	Current financial year + 6 years	SECURE DISPOSAL	
3.3.6	Records relating to the identification and collection of debt	No	Current financial year + 6 years	SECURE DISPOSAL	

3.4 Contract Management					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.4.1	All records relating to the management of contracts under seal	No	Last payment on the contract + 12 years	SECURE DISPOSAL	
3.4.2	All records relating to the management of contracts under signature	No	Last payment on the contract + 6 years	SECURE DISPOSAL	
3.4.3	Records relating to the monitoring of contracts	No	Current year + 2 years	SECURE DISPOSAL	
3.5 School Meals					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.5.1	Free School Meals Registers	Yes	Current year + 6 years	SECURE DISPOSAL	
3.5.2	School Meals Registers	Yes	Current year + 3 years	SECURE DISPOSAL	
3.5.3	School Meals Summary Sheets	No	Current year + 3 years	SECURE DISPOSAL	

4.1 Property Management

This section covers the management of buildings and property.

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
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/Trust 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 or Trust	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

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
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 Trust/school. For information about accident reporting see under Health and Safety above

5.1 Pupil's Educational Record

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes			
	Primary		Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. [3]	
	Secondary		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		
5.1.3	Child Protection information held on pupil file		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		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 principleal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded	

5.2 Attendance					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.2.1	Attendance Registers	Yes	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		Current academic year + 2 years	SECURE DISPOSAL	
5.3 Special Educational Needs					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	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. We may wish to choose to keep SEN files for a longer period of time to defend 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	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	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	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

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

6.1 Statistics and Management Information

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
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 –	Yes			
	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	Yes	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

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
6.2.1	Schemes of Work	No	Current year + 1 year	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 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	SECURE DISPOSAL	

7. EXTRA CURRICULUM MANAGEMENT

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

7.1 Educational Visits outside the Classroom

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	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	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	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		

7.3 Family Liaison Officers and Home School Liaison Assistants

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
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		

5. CENTRAL GOVERNMENT AND LOCAL AUTHORITY

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

8.1 Local Authority

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
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

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
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	

Any queries regarding the retention of trust/school records should be sent to:

Email: DPO@Aldridgeeducation.org