



Policy/Procedure/Guideline Review

Policy/Procedure/Guideline:	Data Information Policy including data retention schedule
Senior Manager Responsible:	Data Protection Officer
Approval:	May 2025
Review date:	Annually



Introduction

Pendle Education Trust (Trust) is committed to maintaining the confidentiality of its information and ensuring that all records within the Trust are only accessible by appropriate individuals. In line with the requirements of the General Data Protection Regulation (GDPR), the Trust also 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 intended.

The Trust has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the Trust's statutory requirements.

This policy applies to all records created, received or maintained by permanent and temporary staff of the Trust in the course of carrying out its functions. Also, by any agents, contractors, consultants or third parties acting on behalf of the Trust.

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 electronic format, e.g. paper documents, scanned documents, emails which document business activities and decisions, audio and video recordings, text messages, notes of telephone and online conversations, spreadsheets, MS Word documents and presentations.

This policy has due regard to legislation including, but not limited to, the following:

- General Data Protection Regulation (2018)
- Freedom of information act 2000
- Data Protection Act 2018
- Human rights act 1998
- Defamation act 2013
- Privacy and electronic communications regulations 2003

Responsibilities

The Trust Board has a statutory responsibility to maintain the Trust and its academies' records and record keeping systems in accordance with the regulatory environment specific to the Trust. The responsibility is delegated to the Chief Executive and each academy principal.

The person responsible for day-to-day operational management in each academy will give guidance on 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.

Each academy will manage and document its records disposal process inline with the records retention schedule. This will help to ensure that it can meet Freedom of Information requirements requests and respond to requests to access personal data under data protections legislation (subject access requests, SARS).

Individual staff and employees must ensure, with respect to records for which they are responsible, that they:

- Manage the Trust and academies' records consistently, in accordance with the Trust's policies and procedures
- Properly document their actions and decisions
- Hold personal information securely
- Only share personal information appropriately and do not disclose it to any unauthorised third party
- Dispose of records securely, in accordance with the Trust's records retention schedule

Relationship with existing policies

This policy has been developed within the context of:

- Freedom of Information policy
- Data Protection policy
- Other legislation or regulations (including audit, equal opportunities and ethics) affecting the Trust

Management of pupil records

All schools, including academies, are under a duty to maintain a pupil record for each pupil. It is made up of specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and includes personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement.

Pupil records may be held in paper form, or else electronically (for instance: as part of the academy's management information system).

All information must be easy to find, accurately and objectively recorded, and expressed in a professional manner, as pupils and parents have a right to access to their educational record via the Data Protection Act 2018 and the GDPR. Requests for information by pupils, or their parents, are to be treated as subject access requests under Data Protection legislation.

Paper files

The following information is useful at the front of a paper file, if one is held:

- Surname and forename
- Date of birth
- Unique pupil number
- Date file was started/opened

It may also be useful to have the following information inside the front cover, so that it is easily accessible to authorised staff; this is not necessary if accessible on the academy information management system:

- Emergency contact details
- Preferred name
- Names and contact details of adults who have parental responsibility/care for the pupil
- Reference to further information held on allergies/medical conditions
- Other agency involvement, e.g. special educational needs (SEN), speech and language therapist
- Reference to any other linked files

Contents of the pupil record

The table below lists common and potential record types that may form part of the pupil record.

Record Type	Notes
Record of transfer from Early Years setting	If applicable
Admission form	
Data collection/checking form – current	This should be checked regularly by parents to ensure details are accurate
Annual written report to parents	
National curriculum and religious education locally agreed syllabus record sheets	

Any information relating to a major incident involving the child	
Statements/plans, reports, etc. for educational support, e.g., SEN, speech and language	Store in a separate area of the record or keep in a separate linked file
Medical information relevant to the child's on-going education/behaviour	Store in a separate area of the record or keep in a separate linked file
Child protection reports/disclosures and supporting documentation	Store in a separate area of the record or keep in a separate linked file, so as to limit access to specific staff
Any information relating to exclusions (fixed or permanent)	
Specific correspondence with parents or outside agencies relating to major issues	This may be in e-mail form. Once the matter is closed, save any correspondence that records sequence of events, pertinent issues and outcomes to pupil record
Summary details of complaints made by the parents or the pupil relevant to the child's on-going education/behaviour	This may be in e-mail form, see note above. Most complaints records are retained by the school and not as part of the pupil record
Examination results – pupil copy	Send uncollected certificates back to exam board after all reasonable efforts to contact the pupil have been exhausted [this is a recommendation, not a requirement]

Records not forming part of the pupil record

The following record types should be stored separately from the main pupil record, as they are usually subject to shorter retention periods (please see the retention schedule section); they should not be forwarded to the pupil's next academy:

- Attendance registers and information
- Absence (authorised notes and correspondence)
- Parental consent forms for trips/outings
- Accident forms (a copy can be placed on the pupil record if it is a major incident)
- Medicine consent and administering records (this is the academy's record)
- Copies of birth certificates, passports etc.
- Generic correspondence with parents about minor issues (i.e. 'Dear Parent')
- Pupil work, drawings etc.
- Previous data collections forms which have been superseded (there is no need to retain these)
- Photography (image) consents (this is the academy's record)

Information stored electronically

Those principles relevant to paper records will apply to those pupil records stored electronically. Academy information management systems may incorporate features to enable elements of the electronic pupil record to be deleted in accordance with retention schedules, whilst the remainder of the record remains intact.

Storage and security

All pupil records and associated information should be stored securely to maintain confidentiality, whilst keeping information accessible to those authorised to see it. Electronic records should have appropriate security and access controls in place; equally, paper records should be kept in lockable storage areas with restricted access. Not everyone in the academy has a need to access all of the information held about a pupil; this is particularly relevant to child protection information.

Transferring pupil records

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.

Weeding

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.

Transfer process

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

- Common transfer file (CTF) from the academy information management system via the school2school system, when used
- Any elements of the pupil record, held in any format, not transferred as part of the CTF
- SEN or other support information, including behaviour, as only limited information may be included in the CTF
- 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 school.

Academies must ensure the information is kept secure and traceable during transfer:

- Records can be delivered or collected in person, with signed confirmation for tracking purposes
- Pupil records should not be sent by post. If the use of post is absolutely necessary, records should be sent by "Special Delivery Guaranteed" or via a reputable and secure courier to a pre-informed named contact, along with a list of the enclosed files. The new school should sign a copy of the list to confirm receipt of the files and securely return to the previous school
- If held electronically, records may be sent to a named contact via secure encrypted e-mail, or other secure transfer method

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

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 academy should contact their Data Protection Officer for further advice.

Retention and disposal

Retention – transferring academy

Responsibility for maintaining the pupil record passes to the next school. Academies may wish to retain information about a pupil for a short period to allow for any queries or reports to be completed or where linked records in the academy information management system have not yet reached the end of their retentions period and deleting would cause problems.

Certain elements of the record may need to be retained for longer, for example: if litigation is pending, or for transfer to the Local Record Office, in accordance with the retention schedule.

Further to the publication of the Independent Inquiry into Child Sexual Abuse (IICSA) child protection records should be retained for 75 years with review periods as appropriate. Academies from which a pupil transfers should consider retaining a copy of the child protection file. Further details can be found here [Independent Inquiry into Child Sexual Abuse](#)

Retention – last known school

The last known or final school is responsible for retaining the pupil record. The academy is the final or last known academy if:

- A secondary phase and the pupil left at 16 years old or for post-16 or independent education, or;
- It is a school at any point and the pupil left for elective home education, they are missing from education or have left the UK.

The pupil record should be retained as a whole for 25 years from the date of birth of the pupil, after which time, if no longer required, it can be deleted or destroyed. SEN and other support service records can be retained for a longer period of 31 years to enable defence in a “failure to provide a sufficient education” case.

If an academy wishes to retain data for analysis or statistical purposes, it should be done in an anonymised fashion.

Disposal

Pupil records will contain personal and confidential information and so must be destroyed securely. Electronic copies must be securely deleted, and hard copies disposed of as confidential waste. Please refer to the section on safe disposal of records for further information.

Records management programme

Information audits

An information audit is typically a record of the following:

- What information is retained
- Why information is retained
- What type of information it is
- How information is processed and shared
- Where information is stored
- What the relevant retention period is
- Who the responsible owners or day to day users are

An information audit should capture all information held, regardless of its form. The academy should consider:

- Paper documents and records
- Electronic documents and records
- Databases (proprietary or developed in-house)
- Microfilm/microfiche
- Sound recordings
- Video/photographic records (including those records taken on traditional magnetic tape and photographic paper, but increasingly, digital sound, video and photo files)
- Hybrid files
- Knowledge
- Apps and portals

The information audit is designed to help the Trust and its academies complete an information asset register which is a record of processing activities (RoPA). The Trust uses GDPR Sentry, an online platform to record this information. It is now generally accepted that information is an organisation's greatest asset and that it should be managed in the same way as the organisation's more tangible assets, such as staff, buildings and money.

Effective information management is about getting the right information to the right people at the right time and an information audit is key to achieving this.

The information audit is designed to allow organisations to discover the information they are creating, holding, receiving and using, and therefore, to manage that information in order to get the most effective business use from it. For an academy, the concept is much more concerned with accessibility of information. The information audit allows the academy to identify the personal information it creates and stores to facilitate correct management (e.g. record of processing activities) under the Data Protection Act (DPA)2018, the General Data Protection Regulation (GDPR) and the Freedom of Information (FOI) Act 2000.

The following are all benefits to maintaining an information audit:

- It saves time – an information audit can be used as a quick point of reference for all staff; it ensures information can be easily located on a daily basis. This may also be useful for new starters or in the event of temporary cover arrangements.
- It avoids duplication – duplicating information is unnecessary, it adds to workloads and takes up unnecessary storage space, which can be costly. Duplicating personal data would be a breach of the DPA 2018, as personal data must not be excessive. Identifying where the principal copy of a piece of information is held means that individual members of staff do not need to hold their own copy.
- Compliance with the DPA – individuals have numerous rights under the DPA in relation to their personal information. Whether you are dealing with a request to access information or an erasure request, the first step is identifying whether the information is held and where. If you don't maintain a record of processing, information may be missed and the Trust could risk Information Commissioner's Office (ICO) enforcement.

The general timescale for dealing with requests under the DPA is one calendar month. Knowing where to locate information and identify if it has been shared with third parties can help save crucial time.

- Development of a record of processing activities (RoPA) – the information collected as part of the information audit can be included in the RoPA which an Academy develops.
- It assists the Data Protection Officer – the Data Protection Officer needs an overview of what personal information is held and how it is handled.
- Compliance with the FoI Act 2000 – under the Academies Act 2010, Academies are obligated to provide certain information within 20 school days or 60 working days, whichever is shorter. Knowing what is held and where to locate information is an essential first step. Wrongly refusing a request or non-compliance with the statutory timescales could lead to ICO enforcement action.
- Identification of information which has passed its retention date – storing information can be costly, regardless of whether it is physical or electronic. Significant savings can be made by ensuring that the relevant retention periods are identified and complied with. Applying retention periods also reduces the risk of not complying with the DPA 2018, GDPR or the FoI Act 2000. Finding information and preparing it in response to a request is much more difficult if there is a need to sort through significant quantities of information which should have been disposed of.
- It improves your ability to make the right decisions – Academies deal with sensitive information on a daily basis. When making any decision in relation to the care of a child, it is essential you consider all the relevant details, whether they are medical or otherwise. You cannot complete any DPIA without knowing what information you hold or will hold.
- It reduces the possibility of an information security breach – names change, addresses change and family relationships change. Knowing where to locate the correct up-to-date information is essential. It reduces the risk of a breach, which helps prevent unnecessary distress and the likelihood of the Trust facing ICO enforcement action and/or legal claims.
- It supports accountability and transparency, which is increasingly important under GDPR requirements.

Any information audit is a snapshot in time and only as good as the information provided by those taking part. In order for information systems to be kept up to date (including capturing information

created by new and developing technologies and to take account of new functions and legislation) the audit results should be regularly reviewed and updated.

Management and monitoring of electronic communications

The following guidelines provide information about electronic communications best practice and will help balance staff and student privacy with the oversight necessary to ensure safeguarding obligations are maintained.

All electronic communications, whilst they are held, are disclosable under Freedom of Information and Data Protection legislation. Anything staff write in an email, an instant message, a text, or on a message board could potentially be made public. Electronic communications are very easy to copy and transmit and, although a staff member may have deleted their copy, the recipients may not. Because of this, they can form part of the Trust's records, commit the Trust to contracts and expose the Trust to risk, if used badly.

Email

Watch the language - As communicating by email is quick and easy, the language in which email is written is often less formal and more open to misinterpretation. Staff are requested to use spellcheck and consider the tone of the wording used.

Choose recipients- Check the recipients are appropriate and typed correctly. Ensure that Bcc is used, where appropriate, to avoid the unauthorised disclosure of email addresses of intended recipients.

Secure data – The consequences of an email containing sensitive information being sent to an unauthorised person can result in a fine of up to the sterling equivalent of 20 million euros, along with restrictions on processing from the Information Commissioner, along with adverse publicity for the Trust. Confidential or sensitive information should be sent by a secure encrypted email or data transfer system. Never put personal information (such as a pupil's name) in the subject line of an email.

Secure devices – Email apps on phones are usually unprotected. By default, outlook will download the entire contents of a person's mailbox on a personal device, which can be easily accessed.

If members of staff access Trust and academy emails on personal devices, the Trust's IT support team should be contacted for help with configuring the device and check for encryption, as well as ensuring that all devices require suitable password for access. Accessing work emails via the internet is recommended as appose to using email apps, as the web client does not save data locally.

It's not a filing system – Email systems are commonly used to store information which should be stored somewhere else. Emails and attachments should be saved into any appropriate electronic filing system.

Where the text of the email adds to the context or value of the attached documents, it may be necessary to keep the whole email. The best way to do this, and retain information which makes up the audit trail, is to save the email in .msg format. Where you just want recipients to read a document, consider sending a link to the documents rather than attaching them.

How long should emails be kept – Email is a communication tool, and email applications are not

designed for keeping email as a record. Email that needs 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?

The retention for keeping these emails will then correspond with the types of record found in the retention schedule. These emails may need to be saved into an appropriate electronic filing system or printed out and placed on paper files. Similarly, information contained within these emails should be recorded in the appropriate place. (e.g. the management information system or behaviour management system). Once this is done, the original can be deleted.

The Trust has implemented an electronic rule whereby emails in inboxes are automatically deleted after a period of time. Currently, this period of time is 18 months. This assists in reducing the amount of information potentially disclosable in the event that a subject access request is received.

Beware of phishing – Be aware of the dangers of providing information over email. Never provide passwords or personal data or click on a link in an email without verifying its source. If in doubt, contact IT for advice.

Messaging: Texts, instant messaging

Text messaging and IM applications provide a quick, efficient way of communicating with individuals or groups.

These methods are largely suited to brief, informal messages; more formal conversations may be better suited to e-mail, telephone or delivered face-to-face. Avoid sending and posting sensitive/personal data, as these systems may not be as secure as e-mail.

Consider your audience – it may be necessary for a message to be sent to an individual or a group of people, but bear in mind that not everyone may have access to these tools and may not have given permission for their contact details to be used in this way. It may also create privacy issues, if third parties are able to read messages not intended for them.

Internal discussion boards and forums

Internal discussion boards and forums (e.g., intranets, Microsoft Teams) provide flexibility for collaboration in the workplace. They can also be very informal and are essentially public within the organisation, although some functionality can be shared with external parties, and because of this they should never be used to share confidential or personal information.

Always ensure that staff or students that use these groups and spaces are aware of exactly who will see any information posted.

Any recorded information is subject to the same Data Protection and FoI legislation, regardless of format; therefore, it would be advisable to only use these methods of communication to transmit information which you would be content to publish, that is, low risk information due to the lack of effective security and assurance.

Records management

Content created and shared by messaging and discussion forums should be regarded as ephemeral and temporary. If the content subsequently becomes important (and is something that needs to be

retained as a formal record, for example: in a safeguarding case file), then it should be copied and moved into the filing system, either by saving it in a readable electronic format, printing it out or taking a screenshot. Whilst content does exist though, it is subject to both FOI and DPA.

Social Media

Social media forms a range of versatile tools that can be used in several ways. As a communication tool, it can broadcast information, enabling a quick way to share information about the Academy in the form of text, pictures, video and/or audio. It can be used to have direct communications with stakeholders on a one-to-one, one-to-many or many-to-many basis, or it can make use of provided information to see who the Academy is engaging with.

The Trust and Academy must ensure that staff contributors maintain the Trust's standards for written communications on social media platforms.

Use of social media may require a risk assessment prior to implementing social media; staff must think about information security when they are sending or replying to messages/posts. Use of social media should follow protocols and procedures established by the Academy to ensure consistent use of social media and that staff do not release information inappropriately or illegally.

Social media is not always a secure and private platform

Social media tools have a range of settings for both security and access to published posts/comments. This needs to be taken into consideration when publishing information and controlling who has access to it. Confidential or sensitive information should never be put online or shared via direct contact on social media. Where images, names of individuals or other personal data is used, Academies must ensure that they have a lawful basis for doing so.

Where this involves consent from the parents/children, the consent should be clear and unambiguous, including where the information will be shared and for how long. Records of consent should be kept with other records for the individuals involved, where possible, but access must be provided for those that require it as part of day-to-day operations. It is important for parents and students to understand that, when giving their consent, the Academy cannot control the re- posting of information.

Social media posts vary in their retention

Social media tools vary in their retention periods. When signing up for any tool, the Academy needs to ensure that users are aware of these retention periods and ensure that it checks on a regular basis for changes. Where the retention period is longer than that set out as part of standard Academy policies, processes must be in place to remove any posts or comments, or to publish this fact within the retention schedule. Where posts include items which are hard to clearly index/search (e.g., images, video or audio), then a content register may be needed to manage when items have been shared, when they were shared, who it was in reference to, etc.

Social media posts and messages don't necessarily delete immediately

Posts and messages can remain on the social media network for a period after the Academy has deleted them. Once messages have been posted they may be shared, liked and commented on (in ways not originally intended). If so, there will still be copies in existence and if the recipient saves an image/screenshot, they will have copies that can be distributed. These copies could be disclosable under the Freedom of Information (FoI) Act 2000 or under the Data Protection Act (DPA) 2018 – they will also form part of the child or subject's digital footprint, and thus, clear and unambiguous consent is therefore key.

Social media is disclosable under the access to information regimes

Both the FoI Act 2000 and DPA 2018 provide regimes for access to information based on specific requests. When completing risk assessments for publishing personal data, this must be considered as part of enabling the rights of data subjects. FoI legislation also mandates that anything published as publicly accessible is potentially disclosable (subject to exemptions), either at the time or as part of any request.

Do staff and governors need another account for work?

In the same manner that using personal e-mail accounts for work means that they will be subject to FoI requests, the same applies for social media accounts. It is recommended, on safeguarding grounds, that dedicated work accounts are used and managed by the Academy. Any official Academy account should be tied to Academy e-mail addresses and ensure that there is transparency within the Academy on who has access to these accounts.

Sending attachments

Sending attachments on social media should be avoided; you should not be sending content to parents etc. via this platform. If they want to receive content, then they should make a request in person at the Academy or via authorised means for it to be processed.

This ensures that compliance with data protection legislation is followed, as well as ensuring safeguarding issues are considered.

Broadcasting information

Where information is broadcast across social media, a record of content/audience/information may be recorded. This is both good practice for ensuring a 'draft' is clearly written and recorded, but also allows the Academy to monitor what information has been shared and about whom.

Safe disposal of records which have reached the end of their retention period

The fifth data protection principle states that "Personal data must be kept for no longer than is necessary for the purpose for which it is processed". Therefore, all records, in all formats, should be subject to an applicable retention period, as defined by business, statutory, regulatory, legal or historical requirements. All retention and disposal decisions should be documented in a retention schedule, as part of the Academy's records management policy (see Retention Guidelines section).

Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling

Where disposal of information is outlined as secure disposal, hard copies will be shredded. Deletion of electronic data should be suitable for the type of information. The trust's IT Team will advise on the most appropriate up to date method of deletion from: overwriting, degaussing, physical destruction, dismantling, sanding or submerging in water (USBs). The academy will keep a Data Destruction Log to record of all files that have been destroyed.

Where an external provider is used to destroy confidential hard copy waste, the records should be shredded on site. The provider should produce a certificate of destruction. Staff working for the external provider should be trained in the handling of confidential documents and this should be confirmed with the provider. A contract must be in place between the data controller (the school) and the processor (the contractor) which outlines their obligations, responsibilities and liabilities.

Where the disposal action is indicated as reviewed before it is disposed, the Safeguarding Lead/ SENCO/ DPO will review the information against its administrative value – if the information should be kept, the academy will keep a record of this.

If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

Where information has been kept for administrative purposes, the Safeguarding Lead/ SENCO will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.

Where information must be kept permanently, this information is exempt from the normal review procedures.

Retention Guidelines

The purpose of retention guidelines

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

Members of staff are expected to manage their current recordkeeping systems using the retention schedule and to take account of differing retention periods when creating new recordkeeping systems.

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

Benefits of a retention schedule

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

- 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.
- Members of staff can be confident that information has been disposed of safely and at the appropriate time.
- Information which is subject to the General Data Protection Regulation, Data Protection Act 2018 and the Freedom of Information Act 2000 legislation will be available when required.
- The school is not maintaining and storing information unnecessarily.

Maintaining and amending the retention schedule

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

This retention schedule contains recommended retention periods for the various record series created and maintained by Academies in the course of their business. The schedule refers to all information, regardless of the media in which it is stored.

Some of the retention periods are governed by statute; others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the General Data Protection Regulation, Data Protection Act 2018 and the Freedom of Information Act 2000.

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 those laid out in this document, the reasons for this need to be documented.

This schedule should be reviewed on a regular basis.

1. Governance, Funding and Financial Management of the Academy Trust

Academies are governed by the Academy Trust, which will usually be a company limited by guarantee¹. The Academy Trust may also be a charitable trust.

1.1 Governance of the Academy Trust					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.1.1	Governance Statement	No		Life of governance statement + 6 years	SECURE DISPOSAL
1.1.2	Articles of Association	No		Life of the Academy	
1.1.3	Memorandum of Association	No		This can be disposed of once the Academy has been incorporated	SECURE DISPOSAL
1.1.4	Memorandum of Understanding of Shared Governance among Schools	No	<i>Companies Act 2006 section 355</i>	Life of Memorandum of Understanding + 6 years	SECURE DISPOSAL
1.1.5	Constitution	No		Life of the Academy	
1.1.6	Special Resolutions to amend the Constitution	No		Life of the Academy	
1.1.7	Written Scheme of Delegation	No	<i>Companies Act 2006 section 355</i>	Life of Written Scheme of Delegation + 10 years	SECURE DISPOSAL

¹ A **company limited by guarantee** does not usually have a share capital or shareholders, but instead has members who act as guarantors. The guarantors give an undertaking to contribute a nominal amount (typically very small) in the event of winding up of the **company**. In the case of an Academy, the guarantors will guarantee the sum of £10 each.

1.1 Governance of the Academy Trust

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.1.8	Directors – Appointment	No		Life of appointment + 6 years	SECURE DISPOSAL
1.1.9	Directors – Disqualification	No	Company Directors Disqualification Act 1986	Date of disqualification + 15 years	SECURE DISPOSAL
1.1.10	Directors – Termination of Office	No		Date of termination + 6 years	SECURE DISPOSAL
1.1.11	Annual Report – Trustees Report	No	<i>Companies Act 2006 section 355</i>	Date of report + 10 years	SECURE DISPOSAL
1.1.12	Annual Report and Accounts	No	<i>Companies Act 2006 section 355</i>	Date of report + 10 years	SECURE DISPOSAL
1.1.13	Annual Return	No	<i>Companies Act 2006 section 355</i>	Date of report + 10 years	SECURE DISPOSAL
1.1.14	Appointment of Trustees and Governors and Directors	Yes		Life of appointment + 6 years	SECURE DISPOSAL
1.1.15	Statement of Trustees Responsibilities	No		Life of appointment + 6 years	SECURE DISPOSAL
1.1.16	Appointment and removal of Members	No		Life of appointment + 6 years	SECURE DISPOSAL
1.1.17	Strategic Review	No		Date of the review + 6 years	SECURE DISPOSAL

1.1 Governance of the Academy Trust

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.1.18	Strategic Plan [also known as School Development Plans]	No		Life of plan + 6 years	SECURE DISPOSAL
1.1.19	Accessibility Plan	There may be if the plan refers to specific pupils	Limitation Act 1980 (Section 2)	Life of plan + 6 years	SECURE DISPOSAL

1.2 Board of Directors, Members Meetings and Governing Body					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
	Board of Directors				
1.2.1	Board Meeting Minutes	Could be if the minutes refer to living individuals	Companies Act 2006 section 248	Minutes must be kept for at least 10 years from the date of the meeting	OFFER TO ARCHIVES
1.2.2	Board Decisions	Could be if the decisions refer to living individuals		Date of the meeting + a minimum of 10 years	OFFER TO ARCHIVES
1.2.3	Board Meeting: Annual Schedule of Business	No		Current year	SECURE DISPOSAL
1.2.4	Board Meeting: Procedures for conduct of meeting	No	Limitation Act 1980 (Section 2)	Date procedures superseded + 6 years	SECURE DISPOSAL
	Committees²				
1.2.5	Minutes relating to any committees set up by the Board of Directors	Could be if the minutes refer to living individuals		Date of the meeting + a minimum of 10 years	OFFER TO ARCHIVES
	General Members' Meeting				

² The board can establish any committee and determine the constitution, membership and proceedings that will apply.

1.2 Board of Directors, Members Meetings and Governing Body					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.2.6	Records relating to the management of General Members' Meetings	Could be if the minutes refer to living individuals	Companies Act 2006 section 248	Minutes must be kept for at least 10 years from the date of the meeting ³	OFFER TO ARCHIVES
1.2.7	Records relating to the management of the Annual General Meeting	Could be if the minutes refer to living individuals	Companies Act 2006 section 248	Minutes must be kept for at least 10 years from the date of the meeting ⁴	OFFER TO ARCHIVES
	Governors				
1.2.8	Agendas for Governing Body meetings	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 ⁵

³ The signed minutes must be kept securely together with the notice and agenda for the meeting and supporting documentation provided for consideration at the meeting. Documentation is generally filed in a dedicated minute book, which is usually in the form of a loose-leaf binder to which additional pages can be easily added.

⁴ The signed minutes must be kept securely together with the notice and agenda for the meeting and any supporting documentation provided for consideration at the meeting. Documentation is generally filed in a dedicated minute book.

⁵ 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.

1.2 Board of Directors, Members Meetings and Governing Body					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.2.9	Minutes of, and papers considered at, meetings of the Governing Body and its committees	May be data protection issues, if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			Life of Academy	
	Inspection Copies ⁶			Date of meeting + 3 years	SECURE DISPOSAL
1.2.10	Reports presented to the Governing Body	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 for the life of the Academy	SECURE DISPOSAL or retain with the signed set of minutes

⁶ These are the copies which the clerk to the Governor may wish to retain, so that requestors can view all the relevant information, without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

1.2 Board of Directors, Members Meetings and Governing Body

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.2.11	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
1.2.12	Trusts and Endowments managed by the Governing Body	No		PERMANENT	
1.2.13	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
1.2.14	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

1.2 Board of Directors, Members Meetings and Governing Body					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
	Statutory Registers⁷				
1.2.15	Register of Directors		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.16	Register of Directors' interests [this is not a statutory register]			Life of the Academy + 6 years	SECURE DISPOSAL
1.2.17	Register of Directors' residential addresses		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.18	Register of gifts, hospitality and entertainments		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.19	Register of members		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.20	Register of secretaries		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.21	Register of Trustees interests			Life of the Academy + 6 years	SECURE DISPOSAL
1.2.22	Declaration of Interests Statements [Governors] [this is not a statutory register]			Life of the Academy + 6 years	SECURE DISPOSAL

⁷ Academies are required by law to keep specific records, collectively known as statutory registers or the statutory books. The registers record information relating to the Academy's operations and structure, such as the current directors. Records should be kept up-to-date to reflect any changes that take place.

1.3 Funding and Finance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
	Strategic Finance				
1.3.1	Statement of financial activities for the year	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.2	Financial planning	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.3	Value for money statement	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.4	Records relating to the management of VAT	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.5	Whole of government accounts returns	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.6	Borrowing powers	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.7	Budget plan	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.8	Charging and remissions policy	No		Date policy superseded + 3 years	SECURE DISPOSAL
	Audit Arrangements				
1.3.9	Audit Committee and appointment of responsible officers	No		Life of the Academy	SECURE DISPOSAL
1.3.10	Independent Auditor's report on regularity	No		Financial year report relates to + 6 years	SECURE DISPOSAL
1.3.11	Independent Auditor's report on financial statements	No		Financial year report relates to + 6 years	SECURE DISPOSAL

1.3 Funding and Finance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
	Funding Agreements				
1.3.12	Funding Agreement with Secretary of State and supplemental funding agreements ⁸	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.13	Funding Agreement – Termination of the funding agreement ⁹			Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.14	Funding Records – Capital Grant	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.15	Funding Records – Earmarked Annual Grant (EAG)	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.16	Funding Records – General Annual Grant (GAG)	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.17	Per pupil funding records	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.18	Exclusions agreement ¹⁰	No		Date of last payment of funding + 6 years	SECURE DISPOSAL

⁸ Where there is multi-Academy governance.

⁹ Either party may give not less than 7 financial years' written notice to terminate the Agreement, such notice to expire on 31 August. Or, where the Academy has significant financial issues or is insolvent, the Agreement can be terminated by the Secretary of State to take effect on the date of the notice.

¹⁰ The Academy can enter into an arrangement with a Local Authority (LA), so that payment will flow between the Academy and the LA, in the same way as it would do were the Academy a maintained school. The Academy can enter into an arrangement with a Local Authority (LA), so that payment will flow between the Academy and the LA, in the same way as it would do were the Academy a maintained school.

1.3 Funding and Finance					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.19	Funding records ¹¹	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.20	Gift Aid and Tax Relief	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.21	Records relating to loans	No		Date of last payment on loan + 6 years if the loan is under £10,000 or date of last payment on loan + 12 years if the loan is over £10,000	SECURE DISPOSAL
	Payroll and Pensions				
1.3.22	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL

¹¹ Funding agreement which says that the Academy can receive donations and can only charge where the law allows maintained schools to charge [see Charging and Remission Policy].

1.3 Funding and Finance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.23	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	Regulation 15 Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)	From the end of the year in which the accounts were signed for a minimum of 6 years	SECURE DISPOSAL
1.3.24	Management of the Teachers' Pension Scheme	Yes		Date of last payment on the pension + 6 years	SECURE DISPOSAL
1.3.25	Records relating to pension registrations	Yes		Date of last payment on the pension + 6 years	SECURE DISPOSAL
1.3.26	Payroll records	Yes		Date payroll run + 6 years	SECURE DISPOSAL
	Risk Management and Insurance				
1.3.27	Insurance policies	No		Date the policy expires + 6 years	SECURE DISPOSAL
1.3.28	Records relating to the settlement of insurance claims	No		Date claim settled + 6 years	SECURE DISPOSAL
1.3.29	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL
	Endowment Funds and Investments				
1.3.30	Investment policies	No		Life of the investment + 6 years	SECURE DISPOSAL

1.3 Funding and Finance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.31	Management of Endowment Funds	No		Life of the fund + 6 years	
	Accounts and Statements				
1.3.32	Annual accounts	No		Current year + 6 years	STANDARD DISPOSAL
1.3.33	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
1.3.34	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
1.3.35	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
1.3.36	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.37	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL

1.3 Funding and Finance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.38	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL
	Contract Management				
1.3.39	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
1.3.40	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
1.3.41	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL
	Asset Management				
1.3.42	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
1.3.43	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL
1.3.44	Records relating to the leasing of shared facilities, such as sports centres	No		Current year + 6 years	SECURE DISPOSAL
1.3.45	Land and building valuations	No		Date valuation superseded + 6 years	SECURE DISPOSAL

1.3 Funding and Finance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.46	Disposal of assets	No		Date asset disposed of + 6 years	SECURE DISPOSAL
1.3.47	Community School leases for land	No		Date lease expires + 6 years	SECURE DISPOSAL
1.3.48	Commercial transfer arrangements	No		Date of transfer + 6 years	SECURE DISPOSAL
1.3.49	Transfer of land to the Academy Trust	No		Life of land ownership then transfer to new owner	SECURE DISPOSAL
1.3.50	Transfers of freehold land	No		Life of land ownership then transfer to new owner	SECURE DISPOSAL
	School Fund				
1.3.51	School Fund – Cheque books	No		Current year + 6 years	SECURE DISPOSAL
1.3.52	School Fund – Paying in books	No		Current year + 6 years	SECURE DISPOSAL
1.3.53	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
1.3.54	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
1.3.55	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
1.3.56	School Fund – Bank statements	No		Current year + 6 years	SECURE DISPOSAL

1.3 Funding and Finance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.57	School Fund – Journey books	No		Current year + 6 years	SECURE DISPOSAL
	School Meals¹²				
1.3.58	Free school meals registers	Yes		Current year + 6 years	SECURE DISPOSAL
1.3.59	School meals registers	Yes		Current year + 3 years	SECURE DISPOSAL
1.3.60	School meals summary sheets	No		Current year + 3 years	SECURE DISPOSAL

As a charity, an Academy is not permitted to trade and make a profit. It is, however, possible to set up a subsidiary trading company, which can sell products or services and Gift Aid profits back to the Academy. If the Academy operates a subsidiary company, it is expected that these records will be managed in line with standard business practice.

1.4 Policies, Frameworks and Overarching Requirements

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.4.1	Data Protection Policy, including data protection notification	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.2	Freedom of Information Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL

¹² Unless it would be unreasonable to do so, school lunches should be provided when they are requested by, or on behalf of, any pupil. A school lunch must be provided free of charge to any pupil entitled to free school lunches. From September 2014, free school lunches must be provided to all KS1 pupils.

1.4 Policies, Frameworks and Overarching Requirements

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.4.3	Information Security Breach Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.4	Special Educational Needs Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.5	Complaints Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.6	Risk and Control Framework	No		Life of framework + 6 years	SECURE DISPOSAL
1.4.7	Rules and Bylaws	No		Date rules or bylaws superseded + 6 years	SECURE DISPOSAL
1.4.9	Home School Agreements ¹³	No		Date agreement revised + 6 years	SECURE DISPOSAL
1.4.10	Equality Information and Objectives (public sector equality duty) Statement for publication	No		Date of statement + 6 years	SECURE DISPOSAL

¹³ This should be drawn up in consultation with parents and should apply to all pupils.

2. Human Resources

2.1 Recruitment ¹⁷					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
2.1.1	All records leading up to the appointment of a new Head Teacher	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 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 ¹⁴	No	DBS Update Service Employer Guide June 2014	The organisation should take a copy of the DBS certificate when it is shown to them by the individual and should be added to the Staff Personal File	SECURE DISPOSAL
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 added to the Staff Personal File	SECURE DISPOSAL

¹⁴ Academies are bound by the legislation that applies to independent schools NOT maintained schools.

2.1 Recruitment17					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom ¹⁵	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, 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	SECURE DISPOSAL
2.1.7	Records relating to the employment of overseas teachers	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	SECURE DISPOSAL
2.1.8	Records relating to the TUPE process	Yes		Date last member of staff transfers or leaves the organisation + 6 years	SECURE DISPOSAL

¹⁵ Employers are required to take a “clear copy” of the documents which they are shown as part of this process.

2.2 Operational Staff Management

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
2.2.1	Staff Personal File, including employment contract and staff training records	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
2.2.4	Records relating to the agreement of pay and conditions	No		Date pay and conditions superseded + 6 years	SECURE DISPOSAL
2.2.5	Training needs analysis	No		Current year + 1 year	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes

	Basic file description	Data Protection Issues			
2.3.1	Allegation which is child protection in nature against a member of staff, including where the allegation is unfounded ¹⁶	Yes	“Keeping children safe in education Statutory guidance for schools and colleges”; “Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children”	Until the person’s normal retirement age or 10 years from the date of the allegation, whichever is longer, then REVIEW	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	<ul style="list-style-type: none"> Oral warning 			Date of warning ²¹ + 6 months	SECURE DISPOSAL ¹⁷
	<ul style="list-style-type: none"> Written warning – level 1 			Date of warning + 6 months	SECURE DISPOSAL ¹⁸
	<ul style="list-style-type: none"> Written warning – level 2 			Date of warning + 12 months	SECURE DISPOSAL ¹⁹
	<ul style="list-style-type: none"> Final warning 			Date of warning + 18 months	SECURE DISPOSAL ²⁰

¹⁶ This review took place when 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.

¹⁷ If warnings are placed on personal files, then they must be weeded from the file.

¹⁸ If warnings are placed on personal files, then they must be weeded from the file.

¹⁹ If warnings are placed on personal files, then they must be weeded from the file.

²⁰ If warnings are placed on personal files, then they must be weeded from the file.

2.3 Management of Disciplinary and Grievance Processes

	Basic file description	Data Protection Issues			
	<ul style="list-style-type: none"> 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 Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of 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 Health and Safety

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
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	The official Accident Book must be retained for 3 years after the last entry in the book. The book may be in paper or electronic format The incident reporting form may be retained as below	
	<ul style="list-style-type: none"> Adults 			Date of incident + 6 years	SECURE DISPOSAL
	<ul style="list-style-type: none"> Children 			Date of birth of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No		Current year + 10 years then REVIEW	SECURE DISPOSAL
2.4.6	Process of monitoring of areas where employees and persons are likely to have come into 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 come into contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire precautions log books	No		Current year + 6 years	SECURE DISPOSAL
2.4.9	Fire risk assessments	No	Fire Service Order 2005	Life of the risk assessment + 6 years	SECURE DISPOSAL

2.4 Health and Safety					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
2.4.10	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL

3. Management of the Academy

3.1 Admissions					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
3.1.1	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
3.1.2	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 + 6 years	SECURE DISPOSAL

3.1 Admissions					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
3.1.3	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
3.1.4	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 6 years after the date on which the entry was made ²¹	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
3.1.5	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL

²¹ [Data protection in schools - Record keeping and management - Guidance - GOV.UK](https://www.gov.uk/guidance/data-protection-in-schools-record-keeping-and-management)

3.1 Admissions

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
3.1.6	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
3.1.7	Supplementary information form, including additional information such as religion and medical conditions	Yes			
	<ul style="list-style-type: none"> For successful admissions 			This information should be added to the pupil file	SECURE DISPOSAL
	<ul style="list-style-type: none"> For unsuccessful admissions 			Until appeals process completed	SECURE DISPOSAL

3.2 Head Teacher and Senior Management Team					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
3.2.1	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
3.2.2	Minutes of Senior Management Team meetings and 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
3.2.3	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
3.2.4	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
3.2.5	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
3.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL

3.3 Operational Administration					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
3.3.1	Management of complaints	Yes		Date complaint resolved + 3 years	SECURE DISPOSAL
3.3.2	Records relating to the management of contracts with external providers	No		Date of last payment on contract + 6 years	SECURE DISPOSAL
3.3.3	Records relating to the management of software licences	No		Date licence expires + 6 years	SECURE DISPOSAL
3.3.4	General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
3.3.5	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
3.3.6	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
3.3.7	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
3.3.8	Visitors' books and signing in sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
3.3.9	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

4. Property Management

This section covers the management of buildings and property.

4.1 Property Management					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
4.1.1	Title deeds of properties belonging to the school	No		These should follow the property, unless the property has been registered with the Land Registry	
4.1.2	Plans of property belonging 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
4.1.5	Business continuity and disaster recovery plans	No		Date the plan superseded + 3 years	SECURE DISPOSAL

4.2 Maintenance					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of 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

4.3 Fleet Management					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
4.3.1	The process of acquisition and disposal of vehicles through lease or purchase, e.g., contracts/leases, quotes, approvals	N	Limitation Act 1980 (Section 2)	Disposal of the vehicle + 6 years	SECURE DISPOSAL
4.3.2	The process of managing allocation and maintenance of vehicles, e.g., lists of who was driving the vehicles and when, maintenance	N	Limitation Act 1980 (Section 2)	Disposal of the vehicle + 6 years	SECURE DISPOSAL
4.3.3	Service logs and vehicle logs	N	Limitation Act 1980 (Section 2)	Life of the vehicle, then either to be retained for 6 years by school or to be returned to lease company	SECURE DISPOSAL
4.3.4	GPS tracking data relating to the vehicles	N	Limitation Act 1980 (Section 2)	Date of journey + 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 Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of 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		
	<ul style="list-style-type: none"> Primary 			Retain whilst the child remains at the primary school	<p>The file should follow the pupil when they leave the primary school. This will include:</p> <ul style="list-style-type: none"> To another primary school To a secondary school To a pupil referral unit <p>If the pupil dies whilst at primary school, the file should be returned to the LA to be retained for the statutory retention period.</p> <p>If the pupil transfers to an independent school, transfers to home schooling or leaves the country, the file should be returned to the LA to be retained for the statutory retention period.</p> <p>Primary schools do not ordinarily</p>

5.1 Pupil's Educational Record					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
					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 LA, as it is more likely that the pupil will request the record from the LA
	<ul style="list-style-type: none"> Secondary 		Limitation Act 1980 (Section 2)	Date of birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Records relating to the management of exclusions	Yes		Date of birth of the pupil involved + 25 years	SECURE DISPOSAL
5.1.3	Management of examination registrations	Yes		The examination board will usually mandate how long these records need to be retained	
5.1.4	Examination results – pupil copies	Yes			
	<ul style="list-style-type: none"> Public 			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board
	<ul style="list-style-type: none"> Internal 			This information should be added to the pupil file	

5.1 Pupil's Educational Record					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
5.1.5	Child protection information held on pupil file	Yes	“Keeping children safe in education Statutory guidance”; “Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children”	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
5.1.6	Child protection information held in separate files	Yes	“Keeping children safe in education Statutory guidance”; “Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children” “The Report of the Independent Inquiry into Child Sexual Abuse (IICSA) recommendation on access to records. ”	Date of birth 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 LA Social Services record If the file relates to child sexual abuse, retain until the child's 75 th birthday	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 Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of 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 6 years after the date on which the entry was made	SECURE DISPOSAL
5.2.2	Correspondence relating to authorised absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of 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 in order 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 – this should be documented
-------	---	-----	---------------------------------	---------------------------------------	--

5.3 Special Educational Needs					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
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 Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of 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 –	Yes			

	<ul style="list-style-type: none"> Results 			<p>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</p> <p>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</p>	SECURE DISPOSAL
	<ul style="list-style-type: none"> 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 Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of 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	It may be appropriate to review these records at the end of each year and allocate a further retention period, or, SECURE DISPOSAL
6.2.3	Class record books	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
6.2.4	Mark books	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
6.2.5	Record of homework set	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
6.2.6	Pupils' work	No		Where possible, 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. Extracurricular Activities

7.1 Educational Visits outside the Classroom

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
--	------------------------	------------------------	----------------------	--------------------------------	--

7.1.1	Records created by schools in order 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 in order 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 ²²	Yes		Conclusion of the trip	Although the consent forms could be retained for date of birth + 25 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 Educational Visits outside the Classroom

²² One-off or blanket consent: The Department for Education (DfE) has prepared a one-off consent form to be signed by the parent on enrolment of their child in a school. This form is intended to cover all types of visits and activities where parental consent is required. The form is available on the DfE website for establishments to adopt adapt, as appropriate, at www.gov.uk/government/publications/consent-for-school-trips-and-other-off-site-activities. A similar form could be used for other establishments, such as Early Years Foundation Stage (EYFS) providers and youth groups, or at the start of programmes for young people.

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	Date of birth 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	
7.1.5	Records relating to residential trips	Yes		Date of birth of youngest pupil involved + 25 years	SECURE DISPOSAL

7.2 Walking Bus					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of 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]

8. Central Government and Local Authority

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

8.1 Local Authority					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of 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

8.2 Central Government					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of 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