KALEIDOSCOPE
Multi Academy Trust

Records Management Policy

Approved by:	Kaleidoscope Trust Board	**Date:**	April 2022
Next Review:	April 2024		

Contents

1. Introduction

Kaleidoscope Multi-Academy Trust (KMAT) recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the Trust.

Records provide evidence for protecting the legal rights and interests of the Trust and provide evidence for demonstrating performance and accountability. The aim of this policy is to provide a framework for managing the School's information to enable the School to:

- Make informed decisions;
- Be open and transparent;
- Respond appropriately to information requests;
- Protect records;
- Comply with the legislative requirements;
- Effectively work with its partners, and share information as required;
- Demonstrate accountability.

2. About this policy

All records created, held, and maintained by Kaleidoscope Multi-Academy Trust in the course of its duties are covered by this policy. This is irrespective of the format of the information, including, but not limited to:

- Paper records
- Electronic records (Word Documents, emails, PowerPoints, database, etc.)
- Photographs, videos, etc.
- Discs

Records are defined as all those documents which facilitate the business carried out by the school/Trust and which are thereafter retained (for a set period) to provide evidence of its transactions, activities or decisions.

3. Responsibilities

The Board of Trustees has a corporate responsibility to maintain records and record keeping systems in accordance with the regulatory environment.

The Chief Finance Officer (for Trust central records) and the Headteacher/Executive Headteacher/Head of School (for School records) have overall responsibility for this policy. They are also responsible for giving guidance for good records management practice to staff and for promoting compliance with this policy so that information can 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.

Individual staff, Governors and Trustees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the Trust's Records Management Policy and Guidelines.

4. Storage

Records must be appropriately stored with due regard for efficiency, cost-effectiveness, security, durability and access. Appropriate procedures and processes are in place to ensure the physical and intellectual security of records.

Storage conditions and handling processes should be designed to protect records from unauthorised access, loss, destruction, theft and disaster. This in line with the GDPR principles of data protection by design, and integrity and confidentiality.

The retention of records for longer than necessary is in breach of the General Data Protection Regulation 2016 (GDPR), and the duplication of records should be limited to optimise the use of space for storage purposes and to aid data accuracy.

5. Retention and Disposal

Information held for longer than is necessary carries additional risk and cost, therefore records and information shall only be retained when there is a business or legislative need to do so. Under the GDPR 2016 and the Data Protection Act 2018 (DPA 2018), personal data processed by an organisation must not be retained for longer than is necessary for its lawful purpose.

The retention of specific documents may be necessary to:

- Fulfil statutory or other regulatory requirements.
- Evidence events/agreements in the case of disputes.
- Meet operational needs.
- Ensure the preservation of documents of historic or other value.
- Evidence child protection matters.

The untimely destruction of documents could cause the school/Trust:

- Difficulty in defending litigious claims
- Operational problems
- Embarrassment
- Failure to comply with the Freedom of Information or Data Protection laws.

Conversely, the permanent retention of all documents where there is no business need or other legal basis to retain them, poses regulatory and security risks.

Appropriate secure disposal is accordingly implemented at the school/Trust in accordance with this policy for the following reasons:

- To comply with the records retention schedule in this policy and data protection principles;
- To comply with Article 5 of the GDPR which states that personal data must not be kept in an identifiable form for longer than is necessary
- To free-up storage space (there is evidence that the de-cluttering of office accommodation can be psychologically beneficial for employees.);
- To reduce the risk of fire (in the case of paper records);
- To lessen the risk of a data breach through data loss or unauthorised access.
- To increase the efficiency of the exercising of data subject rights

5.1. Retention Schedule

In line with all relevant legislative requirements, including the GDPR 2016 and DPA 2018, the Trust/schools will keep some forms of information for longer than others. Information will not be kept indefinitely, unless there are specific requirements.

This schedule is available in Appendix B has been adopted from the Information and Records Management Society's (IRMS) Toolkit for Schools (June 2019), which can be found here https://irms.org.uk/page/SchoolsToolkit.

5.2. Disposal

The school/Trust will either use an accredited confidential waste disposal provider or shred the information on site using a cross-cut shredder. Information on what should be deemed as confidential waste is detailed in Appendix B.

The disposal of school/Trust data, in either paper or electronic form, is conducted in a way that makes reconstruction highly unlikely.

Under no circumstances should paper documents containing personal data or confidential information be simply binned or deposited in refuse tips. To do so could result in the unauthorised disclosure of such information to third parties and render the Trust liable to enforcement action by the Information Commissioner's Office (ICO).

Wherever practicable and appropriately secure, disposal methods should encourage recycling. Electronic files are securely overwritten, in accordance with government guidance, and other media is shredded, incinerated or otherwise disintegrated for data.

A destruction log is kept of all data that is disposed of. The log includes the document type (e.g. Personal data), date of destruction, method and who authorised the destruction. Once data has been deleted, it is deemed to be a permanent deletion, irrespective of whether it could technically be reconstructed from a back-up.

5.3. Archiving

A small percentage of the school's records will be selected for permanent preservation as part of the school's or county archives. It is maintained as a resource to help inspire and equip current staff and pupils to understand and appreciate issues of identity, belonging and shared heritage; to prompt memories of school-life among many generations; and to serve as a research resource for all interested in the history of the school and the community it serves.

6. Monitoring and Compliance

This policy is reviewed bi-annually. Compliance with this policy shall be monitored through a review process undertaken by the person with overall responsibility for records management within the Trust. This will be supported by an annual compliance checks which will include if records are stored securely and can be accessed appropriately.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the Headteacher/Executive Headteacher/Head of School, in consultation with our Data Protection Officer, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

7. Recording of complaints

Complaints will be recorded in writing and monitored termly in accordance with the Trust's complaints policy. Recording will begin at the point when a broad concern has become a specific issue that cannot be resolved instantly, but needs investigation. Recording at the earliest stages need only be a basic record with the date, name and nature of the complaint. The record will detail whether the complaints were resolved at the preliminary stage or whether they had to proceed to the formal stages of the procedure.

8. Links to existing policies

This policy and associated guidelines have been drawn up within the context of, and should be read in conjunction with the following policies:

- Freedom of Information policy
- Data Protection policy
- Other policies, legislation or regulations (including audit, equalities and diversity and business ethics) affecting the Trust.

Appendix A - Records Management Guidelines

These guidelines are intended to help provide consistency of practice in the way in which school/Trust records are managed. These will assist schools about how pupil records should be managed and what kind of information should be included in the file.

It is hoped that the guidelines will develop further following suggestions and comments from those members of staff in schools who have the most contact with pupil records.

These guidelines apply to information created and stored in both physical and electronic format.

These are only guidelines and have no legal status, if you are in doubt about whether a piece of information should be included on the file please contact the Headteacher/Executive Headteacher/Head of School or the Central Team of the Trust.

This guidance includes:

- Managing Pupil Records
- Good Practice for Managing E-mail
- Information Security and Business Continuity
- Safe disposal of records which have reached the end of their administrative life
- Digital Continuity
- Appropriate Storage for Physical Records
- Retention Guidelines

Managing Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System, whether they are held in paper form or in various electronic systems. The pupil record(s) must accompany the pupil to every school they attend and contain information that is accurate, objective and easy to access. These guidelines are based on the assumption that the pupil record is a principal record and that all information relating to the pupil will be found in the file (although it may spread across more than one file and may be held in a number of electronic systems).

1. File covers for paper pupil records

It is strongly recommended that schools use a consistent file cover for any paper based pupil records. This assists secondary schools to ensure consistency of practice when receiving records from a number of different primary schools. If, for example, primary schools have many different file covers for their files, the secondary school that the pupil files are transferred to will then be holding different levels of information for pupils coming from different primary schools.

Using pre-printed file ensures all the necessary information is collated and the paper record looks tidy, and reflects the fact that it is the principal record containing all the information about an individual child.

2. Recording information

Under the Data Protection Act 2018 (DPA 2018) a pupil or their nominated representative has a right to see information held about them. This right exists until the point that the file is destroyed. Therefore, it is important to remember that all information must be accurately recorded, objective in nature and expressed in a professional manner. Whilst the right to request access always exists, the ICO do not expect organisations to try to retrieve information that has been permanently deleted with no intention of ever accessing it again. If it has been archived or simply moved to 'deleted items' then this may be in scope.

3. Primary School records

3a. Opening a file

These guidelines apply to information created and stored in both physical and electronic format.

The pupil record starts its life when a file is opened for each new pupil as they begin school. This is the file that will follow the pupil for the rest of his/her school career. If pre-printed file covers are not being used then the following information should appear on the front of any paper file:

- Surname
- Forename
- DOB
- Unique Pupil Number

The file cover should also contain a note of the date when the file was opened and the date when the file is closed if it is felt to be appropriate.

Inside the front cover the following information should be easily accessible:

- The name of the pupil's doctor
- Emergency contact details
- Gender
- Preferred name
- Position in family
- Ethnic origin
- Language of home (if other than English)
- Religion
- Any allergies or other medical conditions that it is important to be aware of
- Names of adults who hold parental responsibility with home address and telephone number (and any additional relevant carers and their relationship to the child)
- Name of the school, admission number and the date of admission and the date of leaving.
- Any other agency involvement e.g. speech and language therapist, paediatrician

It is essential that these files, which contain personal information, are managed against the information security guidelines set out in this document.

3b. Items that must be included on the pupil record:

- If the pupil has attended an early years setting, then the record of transfer must be included on the pupil file
- Admission form (application form)

- Privacy Notice
- Years Record
- 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 (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (must be stored in the file in a sealed envelope clearly marked as such)
- Child protection reports/disclosures (must be stored in the file in a sealed envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

The following records should be stored separately to the pupil record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary clearing of the files before they are transferred on to another school.

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)
- Photography consent forms

3c. Transferring the pupil record to the secondary school

The pupil record should not be removed from the pupil's record before transfer to the secondary school unless any records with a short retention period have been placed in the file. It is important to remember that the information that may seem unnecessary may be a vital piece of information required at a later stage.

Primary schools do not need to keep copies of any records in the pupil record except if there is an ongoing legal action when the pupil leaves the school. Custody of and responsibility for the records passes to the school the pupil transfers to.

Paper files should not be sent by post unless absolutely necessary. If paper files are sent by post, they should be sent by registered post with an accompanying list of the files. The secondary school should sign a copy of the list to say that they have received the files and return that to the primary school. Where appropriate, records can be delivered by hand with signed confirmation for tracking and auditing purposes.

Electronic documents that relate to the pupil file also need to be transferred, or, if duplicated in a master paper file, destroyed. For the transfer of safeguarding records between KMAT schools the receiving school should request the records electronically via the SAFEGUARD system.

4. Secondary School records

Items that must be included on the pupil record:

- If the pupil has attended an early years setting, then the record of transfer must be included on the pupil file
- Admission form (application form)
- Privacy Notice [if these are issued annually only the most recent need be on the file]
- Years Record
- 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 (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (must be stored in the file in a sealed envelope clearly marked as such)
- Child protection reports/disclosures (must be stored in the file in a sealed envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

The following records should be stored separately to the pupil record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary clearing of the files once the pupil leaves the school.

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)
- Photography consent forms

5. Responsibility for the pupil record once the pupil leaves the school

The school that the pupil attended until statutory school leaving age is responsible for retaining the pupil record until the pupil reaches the age of 25 years. [See the retention schedule for further information]. However, during the period of the Independent Inquiry into Sexual Abuse (IICSA), you must not destroy any safeguarding or child protection records that may be of relevance to the inquiry.

6. Safe destruction of the pupil record

The pupil record must be disposed of in accordance with the safe disposal of records guidelines.

7. Transfer of a pupil record outside the of the UK or EEA area

If you are requested to transfer a pupil file outside of the UK or the EEA area because a pupil has moved into that area, please contact the DPO (office@kaleidoscopemat.co.uk) for further advice.

8. Storage of pupil records

All pupil records must be kept securely at all times. Paper records, for example, must be kept in lockable storage areas with restricted access, and the contents must be secure within the file. Equally, electronic records must have appropriate security and restricted access. Safeguarding records in particular must have restricted permissions, and information must only be shared on a "need to know basis".

Access arrangements for pupil records must ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it.

Good Practice for Managing E-mail

1. Introduction

These guidelines are intended to assist school staff to manage their e-mail in the most effective way, and must be used in conjunction with your school's policies on the use of ICT.

Information about how your e-mail application works is not included in this document.

2. Eight Things You Need to Know About E-mail

a. E-mail has replaced telephone calls and memos.

As communicating by e-mail is quick and easy, many people have replaced telephone conversations and memos with e-mail discussions. However, the language in which e-mail is written is often less formal and more open to misinterpretation than a written memo or a formal letter. Remember that e-mail should be laid out and formulated to your school's standards for written communications.

b. E-mail is not always a secure medium to send confidential information.

c. You need to think about information security when you send confidential information by e-mail. The consequences of an e-mail containing sensitive information being sent to an unauthorised person could be a significant fine from the Information Commissioner's Office, and reputational damage - for example publication of the error in the press, social media or on the Information Commissioner's website. Confidential, personal or sensitive information must be encrypted as content prior to putting it into an e-mail or sent using a secure email system. Never put personal information (such as a pupil's name) in the subject line of an e-mail. Beware of emails "popping up" if you have your screen on display, for instance in the classroom. E-mail is disclosable under the access to information regimes.

All school e-mail is disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public.

d. E-mail is not necessarily deleted immediately.

E-mails can remain in a system for a period of time after you have deleted them. You must remember that although you may have deleted your copy of the e-mail, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 2018 (DPA 2018). Once an email has left your system you have no control over where that data goes, who might have access to it or whether it ever gets fully deleted, so ensuring that only the minimum necessary data is sent to the right person is paramount.

e. E-mail can form a contractual obligation.

Agreements entered into by e-mail can form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff must not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.

f. E-mail systems are commonly used to store information that should be stored somewhere else.

All attachments in e-mail should be saved into any appropriate electronic filing system or printed out and placed on paper files.

g. Employers must be careful how they monitor e-mail

Any employer has a right to monitor the use of e-mail provided it has informed members of staff that it may do so. Monitoring the content of e-mail messages is a more sensitive matter and if you intend to do this you will need to be able to prove that you have the consent of staff or another lawful basis for doing so. If you intend to monitor staff e-mail or telephone calls you must inform them how you intend to do this and who will carry out the monitoring.

The Information Commissioner's Employment Practices Code is an excellent guide to this subject.

h. E-mail is one of the most common causes of stress in the work-place

Whilst e-mail can be used to bully or harass people, it is more often the sheer volume of e-mail that causes individuals to feel that they have lost control of their e-mail and their workload. Regular filing, archiving and deletion can prevent this from happening.

3. Creating and sending e-mail

Here are some steps to consider when sending e-mail.

Do I need to send this e-mail?

Ask yourself whether this transaction needs to be done by e-mail? It may be that it is more appropriate to use the telephone or to check with someone face to face.

To whom do I need to send this e-mail?

Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain e-mails. It is very important to consider whether the people who have been included in the email need to know the information. Indiscriminate sharing of information not only generates unnecessary email traffic which may then fail to be disclosed as part of a Subject Access Request (SAR), but may also breach data protection principles.

Always check whether you have used BCC when sending to multiple recipients. Unauthorised disclosure of email addresses constitutes a data breach and has led to the imposition of serious fines by the Information Commissioner's Office on organisations. If using mail merge check that none of the fields have become corrupted, as this can lead to a mismatch of information and a consequent data breach.

When sending emails containing personal or sensitive data always respond to an authorised, approved address. All emails that are used for official business must be sent from an official business domain address.

In the case that any personal data in an email is going to another company address, you must ensure that that company has the ability to handle this personal data as a Data Controller or Data Processor as defined in the Data Protection Act 2018.

In the case that any personal data in an email is going to an email address outside of the UK or EU/EEA, you must ensure that authority to do so has been sought from the requisite data owner.

Use a consistent method of defining a subject line

Having a clearly defined subject line helps the recipient to sort the e-mail on receipt.

A clear subject line also assists in filing all e-mails relating to individual projects in one place. For example, the subject line might be the name of the policy, or the file reference number.

Ensure that the e-mail is clearly written

- Do not use text language or informal language in school e-mails.
- Always sign off with a name, position and contact details.
- Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
- Avoid writing in capital letters. This can be interpreted as shouting.
- Always spell check an e-mail before you send it. Do not use the urgent 'flag' unless it is absolutely necessary, recipients will not respond to the urgent 'flag' if they perceive that you use it routinely.
- If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.

Sending attachments

Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list can cause resource problems on your network. Where possible put the attachment in an appropriate area on a shared drive and send the link round to the members of staff who need to access it.

Disclaimers

Adding a disclaimer to an e-mail may help to mitigates risk, such as sending information to the wrong recipient, or helps to clarify the school's position in relation to the information being e-mailed. Typically, they cover the fact that information may be confidential, the intention of being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the school.

There is some debate about how enforceable disclaimers are. Legal advice should be sought when using or drafting a disclaimer for your organisation to ensure it meets your specific needs. If an email has been sent to the wrong address, you will need to follow the breach procedure if personal data has been wrongly disclosed.

4. Managing received e-mails

This section contains some hints and tips about how to manage incoming e-mails.

a) Manage interruptions

Incoming e-mail can be an irritating distraction. The following tips can help manage the interruptions.

- Turn off any alert that informs you e-mail has been received
- Plan times to check e-mail into the day (using an out of office message to tell senders when you will be looking at your e-mail can assist with this).

b) Use rules and alerts

- By using rules and alerts members of staff can manage their inbox into theme-based folders. For example:
- E-mails relating to a specific subject or project can be diverted to a named project folder
- E-mails from individuals can be diverted to a specific folder
- Warn senders that you will assume that if you are copied in to an e-mail, the message is for information only and requires no response from you.
- Internally, use a list of defined words to indicate in the subject line what is expected of recipients (for example: “For Action:”, “FYI:”, etc.)
- Use electronic calendars to invite people to meetings rather than sending e-mails asking them to attend
- Set up a delay on the email, which will allow you the chosen amount of time to rectify any errors, before it leaves your outbox.

c) Using an out of office message

If you check your e-mail at stated periods during the day you can use an automated response to incoming e-mail that tells the recipient when they might expect a reply. A sample message might read as follows:

Thank you for your e-mail. I will be checking my e-mail at three times today, 8:30am, 1:30pm and 3:30pm. If you require an immediate response to your e-mail please telephone xxxxxxx on xxxxxxx.

This gives the sender the option to contact someone by phone if they need an immediate response.

d) Receiving emails containing personal data

Any received emails containing personal data must be handled appropriately as per the Data Protection Policy and Data Protection Act 2018.

If any personal data has been received from another organisation you must ensure that the organisation had the authority to send this and that your school has the authority to receive it with consent from all of the Data Subjects referred to.

5. Filing e-mail

Attachments only

Where the main purpose of the e-mail is to transfer documents, then the documents must be saved into the appropriate place in an electronic filing system or printed out and added to a paper file. The e-mail can then be deleted.

E-mail text and attachments

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. The best way to do this and retain information that makes up the audit trail, is to save the e-mail in .msg format. This can be done either by clicking and dragging the e-mail into the appropriate folder in an application such as MS
Outlook, or by using the “save as” function to save the e-mail in an electronic filing system.

If the e-mail needs to be re-sent it will automatically open into MS Outlook.

Where appropriate the e-mail and the attachments can be printed out to be stored on a paper file. Please note that a printout does not capture all the audit information which storing the e-mail in .msg format will.

E-mail text only

If the text in the body of the e-mail requires filing, the same method can be used as that outlined above. This will retain information for audit trail purposes.

Alternatively the e-mail can be saved in .html or .txt format. This will save all the text in the e-mail and a limited amount of the audit information. The e-mail cannot be re-sent if it is saved in this format.

The technical details about how to undertake all of these functions are available in application Help functions.

How long to keep e-mails?

E-mail is primarily a communications tool. E-mail applications are not designed for keeping records or providing a storage area that meets records management storage standards. Emails are subject to different retention periods to other documents which if saved elsewhere may be saved for longer periods.

E-mail that needs to be kept must be identified by content; for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these e-mails will then correspond with the classes of records according to content in the retention schedule for schools found elsewhere in the Records Management Tool Kit for Schools.

These e-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

Information Security and Business Continuity

Information Security and Business Continuity are both important activities in ensuring good information management and are vital for compliance with the Data Protection Act 2018 (DPA 2018). Taking measures to protect your records can ensure that:

- Your school can demonstrate compliance with the law and avoid data loss incidents;
- In the event of a major incident, your school should be able to stay open and will at least have access to its key administrative and teaching records, which may be key in being able to contact parents or staff in an emergency.

Information Security must incorporate a Business Continuity Plan and deal with records held in all media across all school systems:

- Electronic (including but not limited to databases, word processed documents and spreadsheets, scanned images)
- Hard copy (including but not limited to paper files, plans)

1. <u>Digital Information</u>

In order to mitigate the loss of electronic information a school needs to:

a. Operate an effective back-up system

You must undertake regular backups of all information held electronically to enable restoration of the data in the event of an environmental or data corruption incident.

Where possible these backups should be stored in a different building to the servers and if possible off the main school site. This is to prevent loss of data, reduce risk in case of theft or the possibility of the backups becoming temporarily inaccessible. Options for the management of back-up facilities include:

- Use of an off-site, central back up service (usually operated by the local authority or other provider). This involves a back-up being taken remotely over a secure network (usually overnight) and stored in encrypted format in premises other than the school.
- Storage in a data safe in another part of the school premises

The back-up may be stored in a fireproof safe that is located in another part of the premises. These premises must also be physically secure and any hard copy supporting data regarding the location of records must also be stored in the safe.

b. Control the way data is stored within the school

Personal information must not be stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff must be advised not to hold personal information about students or other staff on mobile storage devices including but not limited to memory sticks, phones, iPads, portable hard drives or even on CD.

c. Maintain strict control of passwords

Ensure that the data is subject to a robust password protection regime, ideally with users changing their passwords every 30 days. Discourage password sharing strongly and seek alternative ways for users to share data – like shared network drives or proxy access to email and calendars. In addition staff must always lock their PCs when they are away from the desk to prevent unauthorised use.

d. Manage the location of server equipment

Ensure that the server environment is managed to prevent access by unauthorised people.

e. Ensure that business continuity plans are tested

Test restore processes on a regular basis to ensure that the first time you identify a problem with the backup is not the first time you need to retrieve data from it.

For advice on preserving information security when using email see the fact-sheet on good practice for managing email.

2. Hard Copy Information and Records

Records that are not stored on the school's servers are at greater risk of damage by fire and flood as well as risk of loss and of unauthorised access. Consideration should be given to scanning records where possible so that an electronic record is kept, although it is understood that some original paper records will need to be retained.

a. Fire and flood

The cost of restoring records damaged by water can be high but a large percentage may be saved, fire is much more destructive of records. In order to limit the amount of damage which a fire or flood can do to paper records, all vital information must be stored in filing cabinets, drawers or cupboards. Metal filing cabinets are a good first level barrier against fire and water.

Vital records must not be left on open shelves or on desks as these records will almost certainly be completely destroyed in the event of fire and will be seriously damaged (possibly beyond repair) in the event of a flood. The bottom shelves of a storage cupboard must be raised at least 2 inches from the ground. Physical records must not be stored on the floor. All such records need to be secured in a locked location.

b. Unauthorised access, theft or loss

Staff should be encouraged not to take personal data on staff or students out of the school unless there is no other alternative. Records held within the school must be in lockable cabinets. Consider restricting access to offices in which personal information is being worked on or stored. All archive or records storage areas must be lockable and have restricted access.

Where paper files are checked out from a central system, log the location of the file and the borrower, creating an audit trail.

For the best ways of disposing of sensitive, personal information see Safe Disposal.

c. Clear Desk Policy

A clear desk policy is the best way to avoid unauthorised access to physical records that contain sensitive or personal information and will protect physical records from fire and/ or flood damage.

A clear desk policy involves the removal of the physical records that contain sensitive personal information to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all its contents.

3. Disclosure

Staff must be made aware of the importance of ensuring that personal information is only disclosed to people who are entitled to receive it. Ensure that where you intend to share personal information with a third party that you have considered the requirements of the Data Protection Act. Be careful of giving out personal information over the telephone; invite the caller to put the request in writing, supplying a return address that can be verified.

Where appropriate you should develop a data sharing protocol with the third parties with whom you regularly share data. The Data Protection Officer can provide advice where there is any doubt about data sharing to ensure that a lawful basis for sharing personal data applies.

Staff must be aware that under GDPR, the school is obliged to have contracts in place with parties who process data on the school's behalf. This is a far reaching requirement, and would include for example, IT contractors, work experience placements or school photography companies.

4. Risk Analysis

Individual schools must undertake a business risk analysis to identify all records that are vital to school management and these records must be stored in the most secure manner. Reference materials or resources that are easily replaced are more suitable for storage on open shelves or desks.

The development of an information asset/risk register can assist with this process.

5. Responding to Incidents

In the event of an incident involving the loss of information or records the school should refer to the Data Protection Policy. The school may need to be ready to pull together an incident response team to manage the situation. Schools should consider assigning a specific member of staff to deal with press/media enquiries.

a. Major Data Loss/Information Security Breach

Schools must ensure that all staff are aware of the procedures for a potential data breach in the Data Protection Policy. The school may need to be ready to pull together an incident response team to manage the situation. Schools should consider assigning a specific member of staff to deal with press/media enquiries. In the event of a potential data breach the schools Data Protection Lead and/or Headteacher/Executive Headteacher/Head of School must inform the Trust immediately. Any breach must be reported to ICO within 72

hours where it is likely that there is a risk to someone's rights and freedoms. Individuals must also be notified where the breach is likely to result in a high risk to their rights and freedoms.

Do not put off informing the necessary individuals/organisations so as not to delay informing the Information Commissioner's Office if the incident is serious enough to justify notification. It is better to have notified the Information Commissioner before someone makes a complaint. If in doubt the schools Data Protection Lead and/or Headteacher/Executive Headteacher/Head of School must inform the Trust immediately.

b. Fire/Flood Incident

You should create a team of people who are trained to deal with a fire/flood incident. This will include the provision of an equipment box and the appropriate protective clothing.

The team and equipment should be reviewed on a regular basis.

Further Information and Guidance

UCISA Toolkit https://www.ucisa.ac.uk/representation/activities/ist/samples

Local Authority Resilience Forums

Cabinet Office Guidance http://www.cabinetoffice.gov.uk/content/business-continuity

Safe disposal of records that have reached the end of their administrative life

NB: Please be aware that this guidance applies to all types of record, whether they are in paper or digital format.

1. Disposal of records that have reached the end of the minimum retention period allocated

Principles of the GDPR provides that: Personal data shall not be kept for longer than is necessary for that purpose or those purposes.

Anonymised/pseudonymised data, can be retained, but this means that it would no longer be possible to identify any individual via any means at any point in time. In each organisation, local records managers must ensure that records that are no longer required for business use are reviewed as soon as possible under the criteria set out so that only the appropriate records are destroyed.

The local review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the organisation for research or litigation purposes.

Refer to the Retention Guidelines at the end of this guidance.

Whatever decisions are made they need to be documented as part of the records management policy within the organisation.

2. Safe destruction of records

All records containing personal information, or sensitive policy information must be made either unreadable or unreconstructable.

- Paper records must be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks must be cut into pieces
- Audio / Video Tapes and Fax Rolls must be dismantled and shredded
- Hard Disks must be dismantled and sanded

Any other records must be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in with the regular waste or a skip unless there is no other alternative.

There are companies who can provide confidential waste bins and other services that can be purchased to ensure that records are disposed of in an appropriate way.

Where an external provider is used it is recommended that all records are shredded on-site and a risk assessment is undertaken about supervision requirements, and appropriate checks undertaken for safeguarding purposes. The organisation must also be able to prove that the records have been destroyed by the company who must provide a Certificate of Destruction. Staff working for the external provider must have been trained in the handling of confidential documents. A contract must be in place with any processor.

The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.

It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed, and a request for the records has been received, they MUST still be provided.

Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by a Senior Manager and the destruction recorded. Records must be shredded as soon as the record has been documented as being destroyed.

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction. Members of staff must record at least:

- File reference (or other unique identifier);
- File title (or brief description);
- Number of files and date range
- The name of the authorising officer
- Date action taken

Following this guidance will ensure that the school is compliant with the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000.

3. Transfer of records to the Archives

Where records have been identified as being worthy of permanent preservation arrangements must be made to transfer the records to the County Archives Service.

The school must contact the local record office if there is a requirement to permanently archive the records, and the records will continue to be managed via the DPA 1998 and the FoIA 2000.

If you would like to retain archive records in a special archive room in the school for use with pupils and parents please contact the local record office for specialist advice.

4. Transfer of information to other media

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

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

5. Recording of all archiving, permanent destruction and digitisation of records

Sample appendices are provided for the recording of all records to be used. These records could be kept in an Excel spreadsheet or other database format.

Digital Continuity

The long term preservation of digital records is more complex than the retention of physical records. A large number of organisations create data in electronic format that needs to be retained for longer than 7 years. If this data is not retained in accessible formats the organisation will be unable to defend any legal challenge that may arise.

In order to ensure that digital records are retained in a way that ensures they can be retrieved in an accessible format when they are required, all records that are required to be retained for longer than 6 years must be part of a digital continuity statement.

The average life of a computer system can be as little as 5 years, however, as digital continuity is resource intensive, only records which are required to be retained for 6 years (in line with the Limitation Act 1980) or longer must be subject to digital continuity statements.

1. The Purpose of Digital Continuity Statements

A digital continuity statement will not need to be applied to all the records created by the school. The retention schedule must indicate the records that need to be subject to a digital continuity statement. Any record that needs to be preserved for longer than 6 years needs to be subject to a digital continuity statement.

Appropriate records need to be identified as early in their lifecycle as possible so that the relevant standards can be applied to them and conversely any records that do not need to be included in the policy should also be identified in the early part of the lifecycle.

Digital continuity statements must only be applied to principal copy records.

2. Allocation of Resources

Responsibility for the management of the digital continuity strategy, including the completion of the digital continuity statements must rest with one named post holder in the school.

This will ensure that each information assets is “vetted” for inclusion in the strategy and that resources are not allocated to records that should not be included in the strategy.

3. Storage of records

Where possible records subject to a digital continuity statement should be “archived” to dedicated server space that is being backed up regularly.

Where this is not possible the records should be transferred to high quality CD/DVD, if they are to be included with paper documentation in a paper file or onto an external hard drive that is clearly marked and stored appropriately. Records stored on these forms of storage media must be checked regularly for data degradation.

Flash drives (also known as memory sticks) must not be used to store any records that are subject to a digital continuity statement. This storage media is prone to corruption and can be easily lost or stolen. Flash drives should always be encrypted.

Storage methods must be reviewed on a regular basis to ensure that new technology and storage methods are assessed and where appropriate added to the digital continuity policy.

4. Migration of Electronic Data

Migration of electronic data must be considered where the data contained within the system is likely to be required for longer than the life of the system. Where possible system specifications should state the accepted file formats for the storage of records within the system.

If data migration facilities are not included as part of the specification, then the system may have to be retained in its entirety for the whole retention period of the records it contains. This is not ideal as it may mean that members of staff have to look on a number of different systems to collate information on an individual or project.

Software formats should be reviewed on an annual basis to ensure usability and to avoid obsolescence.

5. Degradation of Electronic Documents

In the same way as physical records can degrade if held in the wrong environmental conditions, electronic records can degrade or become corrupted. Whilst it is relatively easy to spot if physical records are becoming unusable it is harder to identify whether an electronic record has become corrupted, or if the storage medium is becoming unstable.

When electronic records are transferred from the main system to an external storage device, the data must be backed up and two safe copies of the data must be made.

The data on the original device and the back-ups must be checked periodically to ensure that it is still accessible. Additional back-ups of the data must be made at least once a year and more frequently if appropriate.

Where possible digital records should be archived within a current system, for example, a designated server where “archived” material is stored or designated storage areas within collaborative working tools such as SharePoint.

6. Internationally Recognised File Formats

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

7. Digital Continuity Statement

Each digital continuity statement must include the following information:

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

The statement must contain a description of the business purpose for the information assets and any statutory requirements including the retention period for the records. This must also include a brief description of the consequences of any loss of data.

By doing this the records owner will be able to show why and for how long the information assets needs to be kept. As digital continuity can be resource intensive, it is important that the resources are allocated to the information assets that require them.

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

The statement must name the post-holder who holds responsibility for long term data preservation and the post holder responsible for the information assets. The statement must be updated whenever there is a restructure that changes where the responsibility for long term data preservation is held.

If the responsibility is not clearly assigned there is the danger that it may disappear as part of a restructure process rather than be reassigned to a different post.

c. Description of the information assets to be covered by the digital continuity statement

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

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

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

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

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

This should be agreed with the appropriate technical staff.

g. Retention of all software specification information and licence information

Where it is not possible for the data created by a bespoke computer system to be converted to the supported file formats, the system itself will need to be mothballed. The statement must contain a complete system specification for the software that has been used and any licence information that will allow the system to be retained in its entirety.

If this information is not retained it is possible that the data contained within the system may become inaccessible with the result that the data is unusable with all the ensuing consequences.

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

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

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

8. Review of Digital Continuity Statements

The Digital Continuity Statements must be reviewed on a bi-annual (or more frequently if required) basis to ensure that the statement keeps pace with the development in technology.

Appropriate Storage for Physical Records

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

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

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

Environmental Damage - Fire

Records can be damaged beyond repair by fire. Smoke and water damage will also occur to records which have been in a fire, although generally records damaged by smoke or water can be repaired.

Core records must be kept in safes, cabinets or cupboards. Metal filing cabinets will usually suffice, but for important core records, fire proof cabinets may need to be considered.

Fireproof cabinets are expensive and very heavy so they should only be used in when strictly necessary.

Records that are stored on desks or in cupboards that do not have doors will suffer more damage than those that are stored in cupboards/cabinets that have close fitting doors.

Environmental Damage - Water

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

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

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

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

Environmental Damage – Sunlight

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

Environmental Damage – High Levels of Humidity

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

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

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

Environmental Damage – Insect/Rodent Infestation

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

Retention Guidelines

1. The purpose of the retention guidelines

Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule listing the record series that the school creates in the course of its business. Retention guidelines are also required to comply with GDPR principle (e) storage limitation and documentation requirements.

The retention schedule lays down the length of time which the record needs to be retained and the action that must be taken when it is of no further administrative use.

The retention schedule lays down the basis for normal processing under both the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000.

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

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

2. Benefits of a retention schedule

There are a number of benefits that arise from the use of a complete retention schedule:

- Managing records against the retention schedule is deemed to be "normal processing" under the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000. Members of staff must be aware that once a Freedom of Information request is received or a legal hold imposed then records disposal relating to the request or legal hold must be stopped.
- Members of staff can be confident about safe disposal information at the appropriate time.

- Information that is subject to Freedom of Information and Data Protection legislation will be available when required. The school is not maintaining and storing information unnecessarily.

2. Maintaining and amending the retention schedule

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

The retention schedule attached as Appendix A contains recommended retention periods for the different record series created and maintained by schools 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 Data Protection Act 2018 (DPA 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 laid out in this document the reasons for this need to be documented.

Using the Retention Schedule

The Retention Schedule is divided into eight sections:

1. Management of the School
2. Human Resources
3. Financial Management of the School
4. Property Management
5. Pupil Management
6. Curriculum Management
7. Extra-Curricular Activities
8. Central Government and Local Authority

There are sub headings under each section to help guide you to the retention period you are looking for.

Trustee Board Chair 4/4/22

Appendix B – Retention Schedule

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 guarantee[3]. The Academy Trust may also be a charitable trust.

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	*Companies Act 2006 section 355*	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	*Companies Act 2006 section 355*	Life of Written Scheme of Delegation + 10 years	SECURE DISPOSAL

[3] 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	*Companies Act 2006 section 355*	Date of report + 10 years	SECURE DISPOSAL
1.1.12	Annual Report and Accounts	No	*Companies Act 2006 section 355*	Date of report + 10 years	SECURE DISPOSAL
1.1.13	Annual Return	No	*Companies Act 2006 section 355*	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

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
	Committees[4]				
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				

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

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[5]	OFFER TO ARCHIVES
1.2.7	Records relating to the management of the Annual General Meeting[6]	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[7]	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[8]

[5] 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.

[6] Not all Academies are required to hold an Annual General Meeting for the Members – the requirement will be stated in the Constitution.

[7] 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, which is usually in the form of a loose-leaf binder to which additional pages can be easily added.

[8] 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.

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[9]			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

[9] 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

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 Registers[10]				
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

[10] 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[11]	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.13	Funding Agreement – Termination of the funding agreement[12]			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[13]	No		Date of last payment of funding + 6 years	SECURE DISPOSAL

[11] Where there is multi-Academy governance.

[12] 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.

[13] 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[14]	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

[14] 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 Meals[15]				
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.

	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

[15] 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[16]	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

[16] 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[18]	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

[17] Academies do not necessarily have to employ people with qualified teacher status; only the SEN and designated LAC teacher must be qualified. [18] Academies are bound by the legislation that applies to independent schools NOT maintained schools.

2.1 Recruitment[17]					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[19]	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

[19] 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

Management of Disciplinary and Grievance Processes					
	Basic file description	**Data Protection Issues**			**administrative life**
2.3.1	Allegation which is child protection in nature against a member of staff, including where the allegation is unfounded[20]	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation, whichever is longer, then REVIEW	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	□ Oral warning			Date of warning[21] + 6 months	SECURE DISPOSAL[22]
	□ Written warning – level 1			Date of warning + 6 months	SECURE DISPOSAL[23]
	□ Written warning – level 2			Date of warning + 12 months	SECURE DISPOSAL[24]
	□ Final warning			Date of warning + 18 months	SECURE DISPOSAL[25]

[20] 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.

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

[22] If warnings are placed on personal files, then they must be weeded from the file. [23] If warnings are placed on personal files, then they must be weeded from the file. [24] If warnings are placed on personal files, then they must be weeded from the file. [25] 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**			**administrative life**
	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	
	Adults Children			Date of incident + 6 years Date of birth of the child + 25 years	SECURE DISPOSAL 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 + 1 year	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 3 years after the date on which the entry was made[26]	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

[26] School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities October 2014 p6.

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			
	□ For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	□ 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		
	□ Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when they leave the primary school. This will include: □ To another primary school □ To a secondary school □ To a pupil referral unit If the pupil dies whilst at primary school, the file should be returned to the LA to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country, the file should be returned to the LA to be retained for the statutory retention period. Primary schools do not ordinarily

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

5.1 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 for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file	SECURE DISPOSAL – these records MUST be shredded
5.1.6	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	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	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 3 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			
	□ Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	□ Examination papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value added and contextual data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self-evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2 Implementation of Curriculum					
	Basic file description	**Data 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

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[27]	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

[27] 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 and

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**
7.1.4	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]

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.

8.Central Government and Local Authority (LA)

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

Appendix C - What is Confidential Waste?

(1) Any record* which details <u>personal</u> information - *what is personal information?*

- Relates to and identifies a living person
- Could help someone identify a person when used with other information
- Is an expression of opinion about an individual
- Indicates our intentions towards an individual

Such as: Name, Address, Date of Birth, Email, Phone numbers, Location data, IP addresses

(2) Any record* which details <u>special categories of personal data</u> - *what are special categories of personal data?*

- Racial and/or Ethnic Origin
- Political Opinions
- Religious Beliefs (or other beliefs of a similar nature)
- Trade Union membership
- Biometric Information e.g. Photos
- Mental or Physical Health condition
- Sexual life and Orientation

Criminal Records are afforded similar protections to special category data and are similarly sensitive *Such as: Safeguarding, Accident/First Aid, Equalities information, Legal record.*

(3) Any record* which details <u>business/commercially sensitive</u> information - *what is business/commercially sensitive information?*

- Information which Kaleidoscope Multi-Academy Trust (KMAT) would be affected by any loss of, or unauthorised access to.

Such as: Contracts, opinions on service delivery, tender information.

If you have any doubt, then please treat the information as Confidential

** A Record can be in many formats – e.g. Paper, Post-it notes, Disks, CDs, Tapes, Posters, Emails, etc.*