South Grove Primary School

Records Management and Retention Schedule Policy

Date Governors Agreed:	08th October 2020		
Date to be reviewed:	October 2023		
Head Teacher:	J.Mattwood.	**Date:**	08.10.2020
Chair of Governors	C J Slade	**Date:**	08.10.2020

1. Introduction

The School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- The scope of the policy
- Responsibilities
- Relationships with existing policies

2. Scope of the policy

2.1 This policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.

2.2 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

2.3 A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the County Archives Service.

3 Responsibilities

3.1 The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Head Teacher.

3.2 The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

3.3 Individual staff and employees must ensure that records for which they are responsible and accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

4. Relationship with existing policies

This policy has been drawn up within the context of:

- Freedom of Information Policy
- Data Protection Policy (GDPR)
- And with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school

Managing Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System1. The pupil record should accompany the pupil to every school they attend and should 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 cover).

1. File covers for pupil records

It is strongly recommended that schools use a consistent file cover for the pupil record. 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 record looks tidy, and reflects the fact that it is the principal record containing all the information about an individual child.

2. Recording information

A pupil or their nominated representative Pupils have the legal right to see their file at any point during their education and even until the record is destroyed (when the pupil sis 25 years of age or 35 years from date of closure for pupils with Special Educational Needs). This is their right of subject access under the Education (Pupil Information) (England) Regulations 2005 and Data Protection Act 1998. It is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner.

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 which 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 the paper file:

- Surname
- Forename
- DOB
- Special Educational Needs yes/No (This is to enable the files of children with Special Educational Needs to be easily identified for longer retention).
- Emergency contact details
- Gender
- Preferred name
- Position in family

On the Data Collection from the following information is accessible:

- Ethnic origin (although this is 'sensitive' data under the Data Protection Act 1998, the Department for Education require statistics about ethnicity)
- Language of home (if other than English)
- Names of parents and/or guardians with home address and telephone number (and any additional relevant carers and their relationship to the child)
- Name of the School, and the date of admission and the date of leaving
- Any other agency involvement e.g. speech and language therapist, paediatrician

3 Items which should be included on the pupil record:

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 which 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 the 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.

3b. Items which should be included on the pupil record

• If the pupil has attended an early years setting, then the record of transfer should 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]
• Photography Consents
• 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 (should be stored in the file in a sealed envelope clearly marked as such)
• Child protection reports/disclosures (should 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 weeding 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)

3c. Transferring the pupil record to the secondary school

The pupil record should not be weeded 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 which may seem unnecessary to the person weeding the file 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.

Files should not be sent by post unless absolutely necessary. If 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.

Items which should be included on the pupil record:
• If the pupil has attended an early years setting, then the record of transfer should 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]
• Photography Consents
• 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 (should be stored in the file in a sealed envelope clearly marked as such)
• Child protection reports/disclosures (should 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 weeding 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)

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

The school which the pupil attended until statutory school leaving age (or the school where the pupil completed sixth form studies) is responsible for retaining the pupil record until the pupil reaches the age of 25 years. This retention is set in line with the Limitation Act 1980 which allows that a claim can be made against an organisation by a minor for up to 7 years from their 18th birthday.

5. Safe destruction of the pupil record

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

6. Transfer of a pupil record outside the EU area

If you are requested to transfer a pupil file outside the EU area because a pupil has moved into that area the Local Authority will be contacted for further advice.

7. Storage of pupil records

All pupil records should be kept securely at all times. Paper records, for example, should be kept in lockable storage areas with restricted access, and the contents should be secure within the file. Equally, electronic records should have appropriate security.

Access arrangements for pupil records should 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

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.

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

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 civil penalty of up to £500,000 from the Information Commissioner or it could end up on the front page of a newspaper. Confidential or sensitive information should only be sent by a secure encrypted e-mail system. Never put personal information (such as a pupil's name) in the subject line of an e-mail.

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.

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 1998.

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 should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.

E-mail systems are commonly used to store information which 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.
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. If you intend to monitor staff e-mail or telephone calls you should inform them how you intend to do this and who will carry out the monitoring.

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 which causes individuals to feel that they have lost control of their e-mail and their workload. Regular filing and deletion can prevent this 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. 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.

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 (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.
- Never write a whole e-mail 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 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).

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

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 which 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 me on xxxxxxxxx.

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

5. Filing e-mail Attachments only

Where the main purpose of the e-mail is to transfer documents, then the documents should 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 which 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, however, 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, and e-mail applications are not designed for keeping e-mail as a record in a storage area meeting records management storage standards.

E-mail that needs to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? 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 1998. 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.

An Information Security Policy should incorporate a Business Continuity Plan and should 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. Digital Information

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

a. Operate an effective back-up system

You should 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 backup 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 which 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 should also be stored in the safe.

b. Control the way data is stored within the school

Personal information should not be stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff should 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 should 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.

2. Hard Copy Information and Records

Records which 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.

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 should be stored in filing cabinets, drawers or cupboards. Metal filing cabinets are a good first level barrier against fire and water.

Where possible vital records should 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 should be raised at least 2 inches from the ground. Physical records should not be stored on the floor.

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 should 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 should 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 which 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 which 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 should 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 which can be verified.

Where appropriate you may wish to develop a data sharing protocol with the third parties with whom you regularly share data.

4. Risk Analysis

Individual schools should undertake a business risk analysis to identify which records are vital to school management and these records should be stored in the most secure manner. Reference materials or resources which could be 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.

6. Responding to Incidents

In the event of an incident involving the loss of information or records the school should 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

You should have a process which must be used by all members of staff if there is a major data loss or information security breach. This will involve appointing a named member of staff to liaise with the Information Commissioner's Office if an information security breach needs to be reported.

Do not put off 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 to him.

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.

Safe disposal of records which 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
The fifth data protection principle9 states that:

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

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.

2. Safe destruction of records

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

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

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

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

1. Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

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.

2. 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 should be shredded as soon as the record has been documented as being destroyed.

Freedom of Information Act 2000 (FoIA 2000)

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction10. Members of staff should 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 1998 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 should be made to transfer the records to the County Archives Service. The school should contact the local record office if there is a requirement to permanently archive the records, and the records will continue to be managed via the DPA 1998 and the FoIA 2000.

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 should 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.

Schedule of Records transferred by [Name of School]
to [Name of Organisation/Record Office]

- Signed:
- Name:
- Designation:
- Organisation:
- Signed:
- Name:
- Designation:
- Organisation:
- Please return to the Records Manager for retention.

Proforma of individual records to be converted to electronic media

- Date completed
- Signed
- Name
- Designation
- Date completed
- Signed
- Name
- Designation

Please contact [enter appropriate person] on [insert contact number] before destroying any records. The destruction of records must be authorised by your line manager.

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 which needs to be retained for longer than 7 years. If this data is not retained in accessible formats the organisation will be unable to defend any legal challenge which may arise.

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

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

8.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 should indicate which records need to be subject to a digital continuity statement. Any record which needs to be preserved for longer than 6 years needs to be subject to a digital continuity statement.

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

8.2 Allocation of Resources

Responsibility for the management of the digital continuity strategy, including the completion of the digital continuity statements should rest with one named post holder. This will ensure that each information assets is "vetted" for inclusion in the strategy and that resources are not allocated to records which should not be included in the strategy.

8.3 Storage of records

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

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

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

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

8.4 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.

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

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

8.6 Internationally Recognised File Formats

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

8.7 Exemplar Digital Continuity Strategy Statement

An exemplar digital continuity strategy statement can be found in the **Information Management Toolkit for Schools**.

8.8 Review of Digital Continuity Policy

The Digital Continuity Policy should be reviewed on a bi-annual (or more frequently if required) basis to ensure that the policy 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 should be regularly monitored and checked for any damage or emerging risks, especially during holiday periods.
The following are hazards which need to be considered before approving areas where physical records can be stored.

Environmental Damage – Fire

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

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

However, fireproof cabinets are expensive and very heavy so they should only be used in special circumstances.

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

Environmental Damage – Water

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

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

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

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

Environmental Damage – Sunlight

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

Environmental Damage – High Levels of Humidity

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

The temperature in record storage areas should not exceed 18oC and the relative

humidity should be between 45% and 65%.

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

Environmental Damage – Insect/Rodent Infestation

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

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 which the school creates in the course of its business. The retention schedule lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use.

The retention schedule lays down the basis for normal processing under both the Data Protection Act 1998 and the Freedom of Information Act 2000.

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 which 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 1998 and the Freedom of Information Act 2000. Members of staff should be aware that once a Freedom of Information request is received or a legal hold imposed then records disposal 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 which is subject to Freedom of Information and Data Protection legislation will be available when required. The school is not maintaining and storing information unnecessarily.

3. 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.

This retention schedule 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 1998 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.

This schedule should be reviewed on a regular basis.

Using the Retention Schedule

The Retention Schedule is divided into five 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

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

Monitoring and Review

This policy has been reviewed and approved by the Head Teacher and Governors. The Records Management and Retention Schedule Policy will be reviewed and updated as necessary or every two years.

GOVERNING BODY

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Agenda for Governing body meetings	Yes/No		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL
Minutes of Governing body				
• Principal Set (signed			PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
• Inspection copies			Date of meeting + 3 years	If these meeting contain any sensitive, personal information they must be shredded
Reports presented to Governing body	Yes/No		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
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 meeting + a minimum of 6 years	SECURE DISPOSAL
Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes
Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
Records relating to complaints dealt with by the Governing Body	Yes		Date of resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendments) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

MANAGEMENT

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Log books of activity in the school maintained by the Head Teacher	Yes/No		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
Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	Yes/No		Date of the meeting + 3 years then review	SECURE DISPOSAL
Reports created by the Head Teacher of the Management Team	Yes/No		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes/No		Current academic year + 6 years then review	SECURE DISPOSAL
Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes/No		Date of correspondence + 3 years then review	SECURE DISPOSAL
Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

PUPILS

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Admission Registers	Yes		Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry then consider transfer to Archives
Attendance Registers	Yes		Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any back-up copies should be destroyed at the same time]
Pupil files	Yes			
• *Primary*			Retain whilst the child remains at the primary school	Transfer to the secondary school(or other primary school) when the child leaves the school
• *Secondary*		Limitation Act 1980 (Section 2)	Date of birth of the pupil + 25 years	SECURE DISPOSAL
Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL
Special Educational Needs files, reviews and Individual Education Plans	Yes		Date of birth of the pupil + 25 years	SECURE DISPOSAL
Correspondence Relating to Authorised Absence and issues	No		Date of absence + 2 years	SECURE DISPOSAL
Examinations results	Yes			
• *Public*	No		Year of examinations + 6 years	SECURE DISPOSAL
• *Internal examination results*	Yes		Current year + 5 years	SECURE DISPOSAL
Statement maintained under the Education Act 1996 Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
Parental permission slips for school trips – where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL
Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE DISPOSAL

CURRICULUM

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Curriculum development	No		Current year + 6 years	SECURE DISPOSAL

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
School syllabus	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
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
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
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
Examinations results	Yes		Current year + 6 years	SECURE DISPOSAL
SATS records	Yes		Current year + 6 years	SECURE DISPOSAL

PERSONNEL

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
All records leading up to the appointment of a new member of staff – unsuccessful candidate	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
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 and all other information retained for 6 months	SECURE DISPOSAL
Pre-employment vetting information – DBS Checks	No	DBS guidelines	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	SECURE DISPOSAL
Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff’s personal file	
Pre-employment vetting information – Evidence proving the right to work in the UK	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
Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
Annual appraisal / assessment records	Yes		Current year + 5 years	SECURE DISPOSAL
Disciplinary proceedings	Yes			

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Allegation of a child protection nature against a member of staff including where the allegation is unfounded	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 of 10 years from the date of the allegation whichever is the longer then REVIEW. [Allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
• *oral warning*			Date of warning + 6 months	SECURE DISPOSAL [if warnings are placed on personal files then they must be weeded from the file]
• *written warning – level 1*			Date of warning + 6 months	SECURE DISPOSAL [if warnings are placed on personal files then they must be weeded from the file]
• *written warning – level 2*			Date of warning + 12 months	SECURE DISPOSAL [if warnings are placed on personal files then they must be weeded from the file]
• *final warning*			Date of warning + 18 months	SECURE DISPOSAL [if warnings are placed on personal files then they must be weeded from the file]
• *case not found*			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL
Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1996/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

HEALTH & SAFETY

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Health & Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
Health & Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
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

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
• *Adults*			Date of incident + 6 years	SECURE DISPOSAL
• *Children*			DOB of the child + 25 years	SECURE DISPOSAL
Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL
Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 2012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL

ADMINISTRATIVE

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Employer's Liability insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL
Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL
School brochure / Prospectus			Current year + 3 years	SECURE DISPOSAL
Circulars (staff, parents, pupils)			Current year +1 year	SECURE DISPOSAL
Newsletter / ephemera			Current year +1 year	SECURE DISPOSAL
Visitor's book			Current year + 2 years	SECURE DISPOSAL
PTA, Old pupils' Associations			Current year + 6 years	SECURE DISPOSAL

FINANCE

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Annual Accounts	No		Current year + 6 years	SECURE DISPOSAL
Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
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
Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL
All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL
School Fund – Cheque books	No		Current year + 6 years	SECURE DISPOSAL
School Fund – Paying in books	No		Current year + 6 years	SECURE DISPOSAL
School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
School Fund – Bank statements	No		Current year + 6 years	SECURE DISPOSAL
School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL
Free School Meal Registers	Yes		Current year + 6 years	SECURE DISPOSAL
School Meal Registers	Yes		Current year + 3 years	SECURE DISPOSAL
School Meal Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL
Petty Cash Books	No		Current year + 6 years	SECURE DISPOSAL

PROPERTY

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Title deeds of properties belonging to the school	No		Permanent	These should follow the property unless the property has been registered with the Land Registry
Plans of property belonging to the school	No		Retain whilst the building belongs to the school	Pass to new owner if the building is leased or sold
Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL
All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
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

LOCAL AUTHORITY

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

DFe

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
OFSTED reports and papers	No		Life of the report and then REVIEW	SECURE DISPOSAL
Returns	No		Current year + 6 years	SECURE DISPOSAL
Circulars from Dfe	No		Operational use	SECURE DISPOSAL