Records Management and Retention Policy

Ratified at Finance & Staffing Sub Committee

Committee on (date): **October 2023**

Review: (2 year): **October 2025**

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 school. Records provide evidence for protecting the legal right 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:

- Scope
- Responsibilities
- Relationships with existing policies

1. **Scope of the Policy**

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

1.2 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.

1.3 A small percentage of the school's records will be selected for permanent preservation as part of the institutions archives and for historical research. This should be done in liaison with the Leicester City Council's archives service.

2. **Responsibilities**

2.1 The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with the overall responsibility is the Headteacher of the School.

2.2 A copy of the Information Management Toolkit for Schools (IRMS) being a comprehensive guidance and is located in the policy folder for ease of access. However, should there still be some uncertainty, the Headteacher for the 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, appropriate 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.

2.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of securely and safely.

3. **Relationships with existing policies**

This policy has been drawn up within the context of:

- Information Management Toolkit for Schools (IRMS)
- Freedom of Information Publication Scheme
- Data Protection Policy
- E-safety Policy (covering unacceptable ICT use)
- And with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school
- Appendix 1 – Information Management Best Practice Guidance

Monitoring and Review

The effectiveness of this policy will be monitored and evaluated by the Headteacher and will be reviewed on a biennial basis.

INFORMATION MANAGEMENT BEST PRACTICE GUIDANCE

Contents

Pupil Records

Managing Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System. 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 to 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 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

Pupils have a right of access to their educational record and so do their parents under the Education (Pupil Information) (England) Regulations 2005. Under the Data Protection Act 1998 (DPA) (Revising GDPR 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 should be accurately recorded, objective in nature and expressed in a professional manner.

3. Primary School records

3a) Opening a file

This applies 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 cover 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 (although this is 'sensitive' data under the DPA, the Department for Education (DfE) require statistics about ethnicity
- Language of home (if other than English – This needs to be recorded for the Census – Mother Tongue)
- Religion (although this is 'sensitive ' data under the DPA, the school has good reasons for collecting this information)
- Any allergies or other medical conditions that it is important to be aware of (although this is 'sensitive' data under the DPA, the school has good reasons for collecting this information)
- 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

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 record of major incidents is recorded onto the Local Authority (LA) Accident and Incident recording computer programme.

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 date.

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 accompany 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 audition purposes.

Electronic documents that relate to the pupil file also need to be transferred, or, if duplicated in a master paper file, destroyed.

4. Secondary School records

N/A

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

For pupils who have left with no trace the school shall seek guidance from the LA Educational Welfare Service for guidance.

6. Safe destruction of the pupil record

As most pupils' records are transferred to their secondary school, this leaves only pupils who have left with no trace; in this circumstance it will be necessary to seek guidance from the LA Educational Welfare Service before any destruction of pupil records and then this would be in line with the safe disposal of records guidelines.

7. Transfer of a pupil record outside the EU area

If requested to transfer a pupil file outside the EU area because a pupil has moved into that area, please contact the LA for further advice.

8. 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 arrangement 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.

See the school's Information Access and Password Security Policy.

Information Audits

1. What is an information audit?

An information audit is a form of records survey encompassing:

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

The information audit is designed to help organisations complete an information asset register (identifying vital records and assigning protective marking). The terminology grows out of the concept "knowledge information" which involves the capture of knowledge in whatever form it is held, including encouraging people to document the information they would previously have held in their heads.

It is now generally accepted that information is an organisation's greatest asset and that it should be managed in the same way as the organisation's more tangible assets such as staff, buildings and money.

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

2. What are the benefits of the information audit?

The information audit is designed to allow organisations to discover the information they are creating, holding, receiving and using and therefore to manage that information in order to get the most effective business use from it. For a school the concept is much more concerned with accessibility of information. The information audit allows the school to identify the personal information it creates and stores to allow correct management under the DPA.

NB. Under the DPA the school is classed as a "Data Controller" in its own right.

Information a school creates and uses to make the decisions which affect people's daily lives may well become subject to the Freedom of Information Act 2000 (FOIA) and should use the model publication scheme for schools.

An information audit collects the information necessary to formulate and implement an efficient records management programme and to ensure compliance with legislation.

3. Information audit process

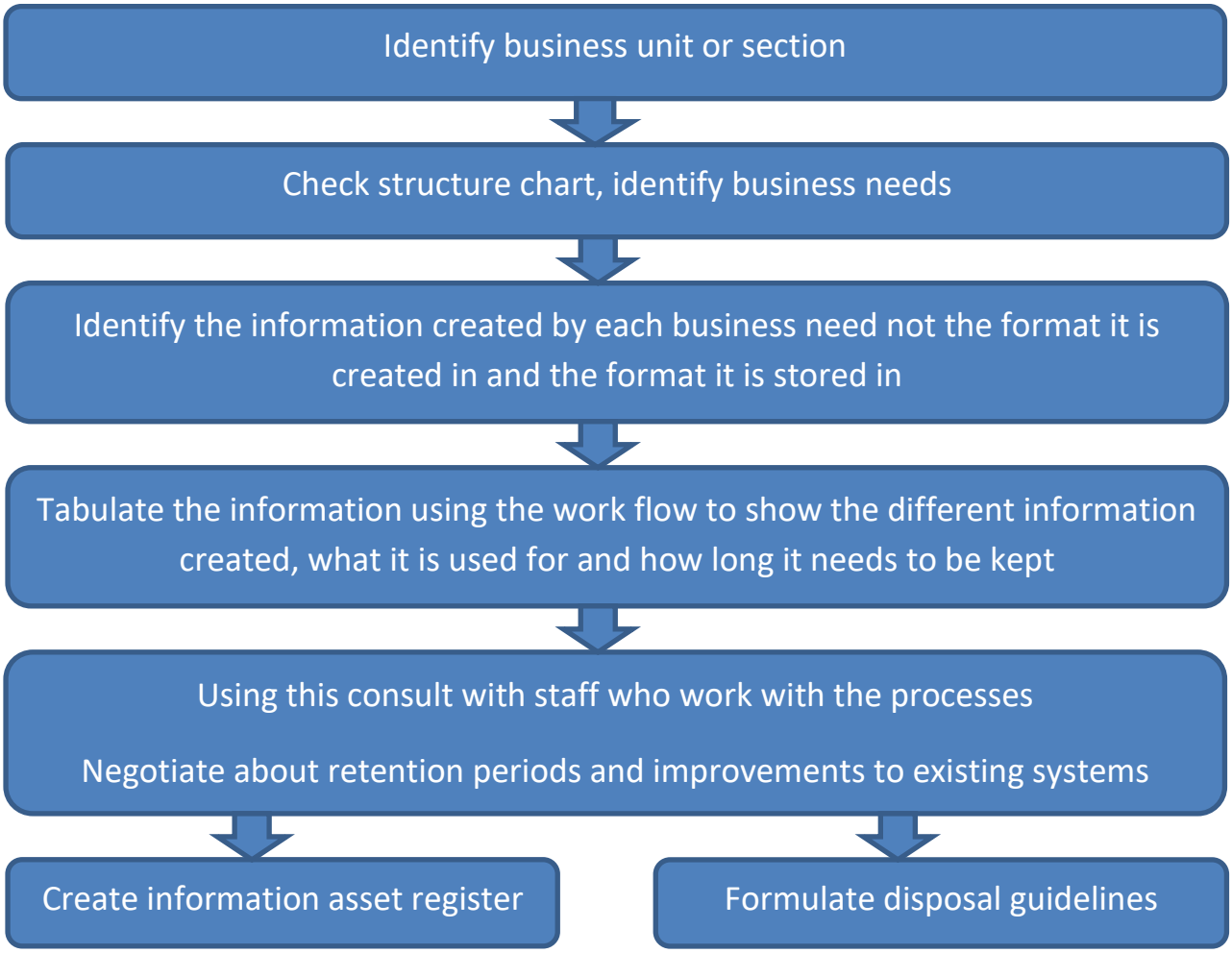
The information audit works on the premise that all information is created for a purpose (business need) and the information created and stored is to support that business need.

The information audit works through a work-flow process [see flow chart below] identifying which information is created at which point in the process, what it is used for, how long it is needed, whether or not it should be captured as part of the "vital" record of the school (i.e. whether it is a working document or a final policy or report) and whether it needs to be protectively marked.

The information audit can be conducted in a number of ways:

- Interviewing key staff from the key areas to identify the information and information flows etc.
- Sending out questionnaires to key staff to identify the information and information flows etc., although these may be less likely to be returned as staff are busy and see a questionnaire as low priority
- A mixture of the above

Information Audit



Seek leadership buy-in to ensure that staff know what is expected. After all, they work with the information so they are best placed to identify it and any requirements. This will also help all staff understand their information responsibilities and should help ensure questionnaires are completed and returned on time.

Once this process has been completed the information audit should contain a list of business needs, the kind of information created to meet that business need, the format in which it is stored, how long it needs to be kept, vital records status and any protective marking. Where local copies have been recorded by the information audit it might also be useful to stipulate who is responsible for retaining the master document/record (e.g. local copies of minutes of a meeting may be kept by individual members of the school leadership on a temporary basis but the Headteacher will usually be responsible, as Chair of that meeting for the master set of minutes).

Once the information audit can be formulated like this then the person completing the audit needs to consult with the staff actually involved in the processes to ensure that this is an accurate reflection of what happens. At this point some negotiation may need to take place if there are anomalies. The purpose of the information audit is to identify where processes can be improved, not merely to document what happens at present.

Example:

Bursar				
Business Function: Payment of Invoices				
Record	**Format**	**Retention/Disposal Period**	**Vital Record Status**	**Protective Marking**
Invoice	**Paper**	**Payment plus 6 years (Audit)**	**Not important**	**Not protectively marked**
Payment authorisation	**Electronic**			
Payment made	**Electronic**			
Acknowledgement	**Paper**			

Once the information audit is felt to be accurate then the information can be tabulated into an information asset register if it is appropriate. This enables all members of staff to see what information is created, by which business process, where it should be filed and how it should be managed. This helps with business continuity in the case of an emergency as members of staff are encouraged to consider what information they would need to carry on with their work.

The results of the information audit should be presented to leadership for comments and final approval. This will provide the audit with leadership endorsement.

Finally any information audit is only a snapshot in time and is only as good as the information which is provided by those taking part. Therefore in order for information systems to be kept up-to-date, including capturing information created by new and

developing technologies, formats and to take account of new functions, and legislation the audit results should be regularly reviewed and updated.
Information Survey Form – located in the IRMS toolkit.

1. Name of school:

2. Department and contact details:

3. Interviewee/person completing form:

4. What is the information series called?

5. Purpose of information:

3a. Day to day responsibility:

6. What is the format? (tick as appropriate)

☐ Paper ☐ Film ☐ Electronic

6a. If electronic:

☐ CD ☐ Tape ☐ Floppy
☐ Hard drive ☐ Server ☐ Cloud storage
☐ Other

7. What other Sections / Teams have access to them?

8. Finding aids:

9. How many individual records in the series?

9a. If paper or film – type of storage:

9b. Linear metreage / cms /megabytes:

9c. Annual growth:

10. How often are they accessed?

☐ Less than once a month
☐ At least once a month but not every week
☐ At least once a week but not every day
☐ Daily

11. How long do you need to keep this information?

☐ Less than 1 year ☐ Less than 2 years
☐ 2 to 6 years ☐ 6 to 10 years
☐ 10 to 25 years ☐ 25 to 50 years
☐ 50 to 100 years ☐ Archived for research

12. State the reason for the retention period:

13. Does a duplicate exist? ☐ Yes ☐ No ☐ Don't know

13a. If yes, where?

13b. In what form? ☐ Paper ☐ Film ☐ Electronic

13c. If electronic, what format? ☐ CD ☐ Tape ☐ Floppy
☐ Hard drive ☐ Server ☐ Other

14. The loss of certain information through fire or some other disaster would have serious consequences for the school's operations.

Does this information fall into this category? ☐ Yes ☐ No ☐ Don't know

14a. If yes please explain why:

15. Any other comments? (Use reverse of form if necessary.)

Please refer to the retention schedule at the end of this document.

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 school's policies on the use of ICT.

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 FOIA and DPA legislation. Be aware that anything you write in an e-mail 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 FOIA or the DPA.

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. (The Information Commissioner's Employment Practice Codes guide best practice).

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 caused 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 send 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 e-mails containing personal or sensitive data; always respond to an authorised, approved address. All e-mails 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 to 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.

Manage interruption
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).

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
- 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.

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 …….

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 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 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 in the IRMS 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 DPA. Taking measures to protect your records can ensure that:

- The school can demonstrate compliance with the law and avoid data loss incidents;
- In the event of a major incident, the 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)

I. Digital information

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

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 LA 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 which is located in another part of the premises. The premises must also be physically secure and any hard copy supporting data regarding the location of records should also be stored in the safe.

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, and portable hard drives or even on CD.

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 e-mail and calendars. In addition staff should always lock their PCs when they are away from the desk to prevent unauthorised use.

Manage the location of server equipment
Ensure that the server environment is managed to prevent access by unauthorised people.

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 back-up is not the first time you need to retrieve data from it.

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

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.

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.

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 filing 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 form 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.

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 DPA. 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.

5. Responding to incidents

In the event of an incident 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.

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 and the school has 72 hours to do so (GDPR 2018).

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.

School Closures and Record Keeping

When a school closes, records management is often low on the list of priorities. School closures are often imposed on schools, therefore, at the time where records management needs to be considered the staff at the school will be on different parts of the change management cycle.

The school will have records which will need to be assessed and either:

a) Securely disposed of; or

b) Stored securely until they reach the end of the statutory retention period; or
c) Transferred to another organisation (for example the LA, or where appropriate, the successor body such as an Academy); or
d) Transferred to the appropriate county Record Office.

It is the responsibility of each LA to manage the records of closed schools until they have reached the end of their administrative life and to arrange for their disposal when required.

There may be a number of different reasons why schools close which may affect where school records need to be stored.

- If a school has been closed and the site is being sold or reallocated to another use then the LA should take responsibility for the records from the date the school closes
- If two schools have merged and function as one school, it will be necessary for the new school to retain any records originating from the two schools for the appropriate time.
- If a secondary school closes and subsequently becomes an Academy, the records relating to the pupils who are transferring to the Academy will be transferred. If the Academy is retaining the current buildings, then all records relating to the maintenance of the buildings should also be transferred. All other records become the responsibility of the LA.

However, some LAs have decided that the responsibility for managing the records of the school prior to it receiving Academy status is to be transferred to the Academy. Each LA should seek legal advice before making any decision about the management of records relating to schools which have become Academies.

Sorting out records, when a building has to be vacated, is time consuming especially if records management has not been a priority in the past. Sufficient time to ensure that the records have been properly sorted, listed and boxed before transfer to the LA must be allowed as part of the project timescales for the school closure. Proper resources must be allocated to this to ensure that the job can be completed before the school closes. It is much more difficult to sort records which have been boxed haphazardly in a hurry in the few days before the school closes.

It is important to bear in mind that when a school closes the staff teams may well feel a real sense of bereavement and this will affect the way in which they view the work which has to be done before the school closes. Sorting out records is usually low on the priority list, but nonetheless needs to be tacked. Managers will need to consider this when allocating the different elements of the task.

It is suggested that project to sort out records could be managed in the following steps.

a) As soon as notification is received that the school is to be closed, a thorough review of all the records on the premises needs to take place. Agreement needs to be reached with the LA about where the records which need to be stored until they can

be disposed of will be sent and who in the LA will be taking responsibility for them. This may include transfer to a records management service or to the County Record Office.

b) The next step is to identify what should happen to all different records by using the retention guidelines found below. This will include safe disposal, transfer to the LA and transfer to the County Record Office.
c) The records can then be sorted in preparation for disposal or transfer.

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

NB: 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 principle 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.

Refer to the Retention Guidelines at the end of the document.

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 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.

a) 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.

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

   The FOIA requires the school to maintain a list of records which have been destroyed and who authorised their destruction. Members of staff should record at least:
   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 DPA and the FOIA.

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 and FOIA.

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 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 recording of records below, these formats 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]

Date	Description / Volume

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

Unique Identifier	Full Name	Date of Birth	Type of Record	Date to be Digitised (once known)

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.

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 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 life cycle 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.

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 (Headteacher). 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.

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.

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 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.

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.

7. Digital Continuity Strategy Statement

See school’s separate Digital Continuity Strategy Statement.

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.

Retention Guidelines

1. The purpose of the retention guidelines

Under the FOIA, 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 DPA and the FOIA.

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 DPA and the FOIA. 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.

Using the retention schedule
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 DPA and the FOIA.

Managing records 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.

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 LA

Management of the School

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

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

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

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

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

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

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

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

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

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

2. Human Resources

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

2.1 Recruitment					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.1.1	All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.1.3	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file	
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	

2.2 Operational Staff Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/ assessment records	Yes		Current year + 5 years	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	oral warning			Date of warning[6] + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
	written warning – level 1			Date of warning + 6 months	
	written warning – level 2			Date of warning + 12 months	
	final warning			Date of warning + 18 months	
	case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

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

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

3. Financial Management of the School

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

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

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

3.3 Accounts and Statements Including Budget Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
3.3.3	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL

3.4 Contract Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL

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

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

4. Property Management

This section covers the management of buildings and property.

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

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

5. Pupil Management

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

5.1 Pupil's Educational Record					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • to another primary school • to a secondary school • to a pupil referral unit • If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
	Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes			
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
	Internal			This information should be added to the pupil file	

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

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

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

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

6. Curriculum Management

6.1 Statistics and Management Information					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records –	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 Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.2.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.2	Timetable	No		Current year + 1 year	
6.2.3	Class Record Books	No		Current year + 1 year	
6.2.4	Mark Books	No		Current year + 1 year	
6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL

7. Extra Curricular Activities

7.1 Educational Visits outside the Classroom					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

7.2 Walking Bus					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.2.1	Walking Bus Registers	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]

7.3 Family Liaison Officers and Home School Liaison Assistants					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.3.1	Day Books	Yes		Current year + 2 years then review	
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	
7.3.3	Referral forms	Yes		While the referral is current	
7.3.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	
7.3.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
7.3.6	Group Registers	Yes		Current year + 2 years	

8. Central Government and Local Authority

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

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

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