RECORD MANAGEMENT POLICY

AND

ANNUAL REVIEW OF SCHOOL RECORDS AND SAFE DATA DESTRUCTION CHECKLIST

ODBST Level 1 Statutory Policy:	**ALL** Schools require this policy with **no changes** allowed to core text. No changes are necessary to personalise this with school name and branding, as this is a Trust level policy for use, without change, by all schools. LGBs will **note** adoption in LGB meetings. Review will take place at Trust level, and schools will be notified of updates and review dates as necessary.
Other related ODBST policies and procedures:	Data Protection Policy Freedom of Information
Committee responsible:	AEC
Approved by:	AEC
Date Approved:	October 2021
Review date:	Autumn term 2024

1 Introduction

1.1 The aim of this policy and the records retention schedule at Records Checklist for Safe Data Destruction log is to enable the Trust to comply with the commitments of the General Data Protection Regulation and other relevant statutory legislation such as audit requirements and Health and Safety requirements and integrates consideration of these and other compliance issues.

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

2 Objectives

2.1. Records management is defined as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

2.2. Records management helps to:

a. ensure that the Trust conducts itself in an efficient and accountable manner.

b. meet legislative and regulatory requirements.

c. support and document policy formation and decision-making.

d. facilitate the effective performance of activities and delivery of services throughout the Trust.

e. provide continuity in the event of a disaster.

f. protect the interests of the Trust in the event of litigation or otherwise.

g. establish and maintain the Trust's cultural identity and institutional memory.

3 Responsibilities

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

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

3.3. Each school within the Trust is individually responsible for the management of their records generated by its activities.

3.4. Individual members of staff should ensure that records, for which they are responsible, are maintained and disposed of in accordance with this policy.

4 **Records Management Good Practice**

4.1. When managing records, consider factors such as how your colleagues can access the files if necessary, how to ensure that records are kept for as long as necessary, whether records are duplicated (stored in paper and electronic format) and stored in the correct location. Some general guidelines which may help to meet these and other aims are:

a. avoid duplication - create records only where necessary,

b. name files, electronic and paper, in a way that is meaningful to you and your colleagues,

c. avoid long, complicated numbering or coding that may be easy to misfile,

d. have a filing system that can be accessed by all that have a right to, while also balancing it with appropriate security arrangements, i.e. computer passwords, locked filing cabinets,

e. store material appropriately,
f. do not overfill boxes or cabinets,
g. sort files regularly,
h. dispose of records in a timely manner and use confidential waste collection or shredding facilities where available.

4.2 The length of time records should be kept can vary depending on the type of documentation and legal constraints, for more details on how long to keep specific records see the Trust's Disposal Schedule.

4.3 Records should be held in files - these may be paper based or held electronically in shared directories, databases or document management systems. The files should be organised in a structured way and have some indication as to their contents and relevance. Where there are confidentially issues, files may be held in a secure storage area, on a computer or email box but bear in mind that colleagues should be able to access them in your absence.

4.4 Exactly what records you keep on file will vary according to the work you do, however reasons for keeping records include but are not exhausted to:
a. There is a legal requirement to keep the information,
b. The information is needed to carry out the Trust's everyday business,
c. The information is for financial purposes,
d. Information explaining why and how a particular decision was made,
e. The information is needed if a decision is challenged or is public`cly accountable.

4.5 For most data, there should be one lead copy. This will be the file of the person or department who has the lead on the topic concerned, for example, a schedule of consents for a school trip, which has been printed for the accompanying teacher. The electronic file should be kept and attached to the Evolve record. All other records/ copies should be destroyed. Other members of staff may also have a file on the same subject, but they should keep this only for so long as is needed for their personal reference.
4.6 If you create a folder on a shared drive or on your personal drive, you should take responsibility for maintaining the contents of that folder. Do not allow out-of-date material to accumulate in it. If a document is not accessed for eighteen months, it should probably be deleted from the drive unless it is the master file copy then it should be archived.
4.7 Documents and folders should have titles which are easily understood by all members of staff. Only use commonly understood abbreviations. Do not store multiple versions / copies of the same data.
4.8 Do not use your computer hard drive (c:// drive) to store information as this drive is not backed up. Use the R or U drives only. Use your personal drive only for information that is confidential or personal or does not need to be shared within the Trust. Use cloud storage such as Google Drive or Microsoft One Drive where available to do so.
4.9 Shared drives e.g. R drive should be used for current work to which your colleagues may need access. Do not password protect material unless your colleagues know the password so that the information can be accessed in your absence. The shared drive can be set up with folder permissions to allow a restricted group of people to have access.

5 Confidential Records

5.1 These records should be labelled as 'Confidential' or 'Commercial in Confidence' and be clear as to who within the organisation should be able to access and use these records. It is also good practice for the record to hold an intended publication date, as few records remain confidential for their entire life-span.

5.2 N.B. Labelling a record 'Confidential' does not exempt the record from being admissible under the Freedom of Information Act 2000. Further information can be obtained from the Trust's Freedom of Information Policy

5.3 Information being supplied in confidence should be stamped, marked, or include a statement that it is confidential or being supplied in confidence, and be treated in a consistent confidential manner.

5.4 The following guidelines should be followed for confidential records:

a. Store confidential records in secure filing cabinets.

b. Cabinets should always be kept locked when not in use, not located in a public area, and access to the confidential records should be restricted only to those employees that require the information; c. Confidential records should never be left in a public open area such as an in-tray or on a desk. The record should be returned to the cabinet when not in use;

d. Confidential records must be destroyed by confidential waste disposal or shredding only;

e. For electronic records, store confidential records in separate directories or files and restrict access to these directories or files;

f. Laptops that hold confidential information must be Trust owned and encrypted by IT Services; Confidential information should not be copied to non-Trust equipment;

6 E-Mails & Attachments

6.1 E-mails may be disclosed in response to a Freedom of Information or Subject Access Request and in legal cases. Electronic messages can be legally binding, and we may be held liable for defamatory statements in e-mails. For these reasons, do not put anything in e- mails that you would not say in other forms of communication. If an e-mail contains important information or an important decision, it should be added to the relevant file/folder either electronically or a hard copy. An email can be saved electronically using 'File – Save as - File'.

6.2 The majority of emails produced are trivial; it is therefore, a drain on Trust resources to store them on our system and can cause a delay in responding to a subject request because of the additional time caused in searching through them. Keep information about people for no longer than necessary; this includes e-mails to and from or about people. You should delete e-mails as soon as possible and should not allow a backlog to accumulate as this then becomes difficult to manage. Emails should also be deleted from your deleted items folder and/or recycle bin.

6.3 Because e-mail is a record you need to know that you can find it quickly and easily if you must disclose it because of a Freedom of Information or Subject Access Request.

6.4 E-mails need to be treated just like other records you deal with. You wouldn't leave paper mail piled up permanently in your in tray, so you should treat your inbox in the same way. When you receive an e-mail act on it as soon as possible and then delete it. If it needs to be kept, then file it.

6.5 If an e-mail is needed to record official business procedure, note that paper printouts of e-mails don't hold the same legal weight as e-mails filed electronically

6.6 Sensitive documents such as SEN documents, should be scanned and sent by secure Email. Postal services (even Special Delivery) may not guarantee security of delivery and receipt by the intended recipient.

6.7 Avoid sending documents as attachments. Instead send a link or tell people where the document can be found. This ensures documents are less likely to get lost and everyone looks at the most up to date copy so there is no confusion over which version is the correct or latest one.

6.8 Do not use a pupil's full name in an email header. This information could be easily visible if a screen is left on in the background.

7 Archive and Disposal

7.1 Documents should be archived in accordance with the Retention Schedule in Appendix A

7.2 You may wish to archive electronic files this should be done by creating an archive sub- folder on a Trust network drive. Within the archive sub-folder, you can then create a folder named 'do not dispose' and numerous folders with the naming convention as the date of destruction. This will make it easier to dispose of the archived records when they reach their destruction date.

7.3 Before you begin to archive you will need to use items that are suitable for storing items long term such as archive cardboard boxes, paper files, plastic-ended treasury tags etc. as over time metal components may damage the files.

7.4 Documents and files need to be prepared prior to being put into the archive storage box. Files should be removed from lever arch files and placed into card wallets/files and all metal removed. The documentation should be reviewed to remove and destroy any paperwork that is not required to be stored, i.e. personal notes, duplicate items etc.

7.5 The first step to archiving your documents is to create an inventory. The best way to do this is by using a standard template detailing all the relevant information of the archive box contents.

8 Policy Circulation

8.1 This Policy will be published on the Trust's website and included in the Trust's Policy Monitoring Schedule.

8.2 The Trustees are responsible for overseeing, reviewing and organising the revision of this Policy.

{Insert your school logo}

ANNUAL REVIEW OF SCHOOL RECORDS AND SAFE DATA DESTRUCTION CHECKLIST

A. Summary of areas reviewed:

Contents

A. Aims

This checklist has been produced based on the "Information Management Toolkit for Schools" (IMTIS) dated 1 February 2016 and developed and published by the Information Record Management Society ("IRMS").

This checklist has been produced in accordance with the guidance produced by the DFE in April 2018 in the "GDPR Toolkit for Schools" and is in accordance with the Data Protection rules and Freedom of Information Act (2000) legislation.

This is a checklist developed to enable School Business Managers, Clerks, SENCO and other School Staff to carry out an efficient annual review and safe destruction of school records and information.

Where there is legal statute behind a requirement this is detailed in the IMTIS document.

B. Safe Destruction of Data

(i) Disposal of records that have reached the end of the minimum retention period allocated

The fifth data protection principle as per the data protection rules (updated for GDPR) 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 school, the leadership 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 school review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the school for research or litigation purposes.

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

(ii) Safe destruction of records

All records containing personal information, or sensitive policy information should be made either unreadable or non-reconstructable.

- 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.

Third party contractors should be certified to the following:

o BSEN15713 – secure destruction of confidential material o BS7858 – staff security vetting

o ISO 9001 – service quality

o ISO 14001 – environmental management standard

o ISO 27001 – information security Additionally, membership of the following organisations and associations are recommended:

o BSIA – British Security Industry Association

o FACT - Federation Against Copyright Theft

o FTA – Freight Transport Association

o FORS - Fleet Operator Recognition Scheme

o NAID – National Association for Information Destruction

o SafeContractor – health and safety assessment scheme

o UKSSA – UK Security Shredding Association

Third party contractors provide a short chain of custody, which significantly reduces the risk of a data breach. Accredited contractors will meet requirements for environmental conditions, the physical security of vehicles and facilities, and they will shred to a minimum of DIN3. Shredding contractors should be trained in the handling of confidential records. Their premises, policies, processes and accreditations should be regularly audited to ensure compliance to requirements.

(It is vital to ensure shredded material cannot be put back together. The European standard, DIN 32757, is the standard for paper shredding. There are six levels, ranging from DIN1 to DIN6. The higher the number the higher the standard of shredding and the smaller the shred size. DIN 1 - 2 provides the least level of security, with DIN 5 - 6 being used mainly by central government and the military. DIN 3 - 4 is recommended for public authority records, including school records.)

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

(iii) 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 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
- Method of disposal

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

If you have any queries in completing this checklist, please contact:

The Data Protection Officer
The Oxford Diocesan Bucks Schools Trust
Moat Farm
Marsh Lane
Stoke Mandeville
Bucks
HP22 5UZ

1. 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						
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.1.1	Agendas for Governing Body meetings	potential	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	Principal Set (signed)	potential	There may be data protection issues if the meeting is dealing with confidential issues relating to staff	PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service	
	Records relating to Governor visits	potential		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	potential	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	YES	No	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.

	1.1 Governing Body (continued…)					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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 made to and investigated by the governing body or head teacher	yes	Yes	Major complaints: current year + 6 years. If negligence involved then: current year + 15 years If child protection or safeguarding issues are involved then: current year + 40 years	SECURE DISPOSAL	
1.1.10	Annual Reports created under the requirements of the Education (Governor'sAnnual Reports)(England) (Amendment) Regulations 2002		No	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	
1.1.12	Records relating to the election of parent and staff governors not appointed by the governors	yes	Yes	Date of election + 6 months	SECURE DISPOSAL	

1.1.13	Records relating to the appointment of co-opted governors	yes		Provided that the decision has been recorded in the minutes, the records relating to the appointment can be destroyed once the co-opted governor has finished their term of office (except where there have been allegations concerning children). In this case retain for 25 years	SECURE DISPOSAL	
1.1.14	Records relating to the election of chair and vice chair	yes		Once the decision has been recorded in the minutes, the records relating to the election can be destroyed	SECURE DISPOSAL	
1.1.15	Scheme of delegation and terms of reference for committees	no		Until superseded or whilst relevant [Schools may wish to retain these records for reference purposes in case decisions need to be justified]	These could be offered to the archives if appropriate	
1.1.16	Meeting schedule	no		Current year	STANDARD DISPOSAL	
1.1.17	Agendas - additional copies	No		Date of meeting	STANDARD DISPOSAL	
1.1.18	Records relating to Governor Monitoring Visits			Date of the visit + 3 years	SECURE DISPOSAL	
1.1.19	Annual reports required by the DFE			Date of report + 10 years	SECURE DISPOSAL	
1.1.20	All records relating to the conversion of schools to Academy status			For the life of the organisation	Consult local archives before disposal	
1.1.21	Correspondence sent and received by the governing body or head teacher	potential		General correspondence should be retained for current year + 3 years	SECURE DISPOSAL	
1.1.22	Action plans created and administered by the governing body			Until superseded or whilst relevant	SECURE DISPOSAL	
1.1.23	Policy documents created and administered by the governing body.			Until superseded [The school should consider keeping all policies relating to safeguarding, child protection or other pupil related issues such as exclusion until the IICSA has issued its recommendations		
1.1.13	All records relating to the conversion of schools to Academy status			For the life of the organisation	Consult local archives before disposal	
	1.2 Governor Management					

1.2.1	Records relating to the appointment of a clerk to the governing body			Date on which clerk appointment ceases + 6 years	SECURE DISPOSAL	
1.2.2	Records relating to the terms of office of serving governors, including evidence of appointment	Yes		Date appointment ceases + 6 years		
1.2.3	Records relating to governor declaration against disqualification criteria	yes		Date appointment ceases + 6 years	SECURE DISPOSAL	
1.2.4	Register of business interests	yes		Date appointment ceases + 6 years	SECURE DISPOSAL	
1.2.5	Governors Code of Conduct			This is expected to be a dynamic document; one copy of each version should be kept for the life of the organisation		
1.2.6	Records relating to the training required and received by Governors	yes		Date Governor steps down + 6 years	SECURE DISPOSAL	
1.2.7	Records relating to the induction program for new governors	yes		Date appointment ceases + 6 years	SECURE DISPOSAL	
1.2.8	Records relating to DBS checks carried out on clerk and members of the governing body	yes		Date of DBS check + 6 months	SECURE DISPOSAL	
1.2.9	Governor personnel files	yes		Date appointment ceases + 6 years	SECURE DISPOSAL	

	1.2 Head Teacher and Senior Management Team					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.2.1	Log books of activity in the school 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 annually, or as required if not destroyed	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	Potential	Yes	These should be held on the individual's personnel record. If not then termination of employment + 6 years	SECURE DISPOSAL	
1.2.7	School Development Plans		No	Life of the plan + 3 years	SECURE DISPOSAL	

	1.3 Admissions Process					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy		No	Life of the policy + 3 years then review	SECURE DISPOSAL	
1.3.2	Admissions – if the admission is successful		Yes	Date of admission + 1 year	SECURE DISPOSAL	
1.3.3	Admissions – if the appeal is unsuccessful		Yes	Resolution of case + 1 year	SECURE DISPOSAL	
1.3.4	Register of Admissions		Yes	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.[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	Current year + 1 year	SECURE DISPOSAL	

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					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.4.1	General file series which does not fit under any other category.		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 School should consider keeping a copy for its own archive.	
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	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	
1.4.7	School Privacy Notice which is sent to parents as part of GDPR compliance	Yes		Until superseded + 6 years		
1.4.8	Consents relating to school activities as part of GDPR compliance (for example, consent to be sent circulars or mailings)	Yes		Consent will last whilst the pupil attends the school, it can therefore be destroyed when the pupil leaves	SECURE DISPOSAL	
1.5.9	Walking bus registers	Yes		Date of register + 6 years	SECURE DISPOSAL	

2. Human Resources

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

	2.1 Recruitment					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.1.1	All records leading up to the appointment of a new headteacher	Yes	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	Yes	Application forms, references and other documents – for the duration of the employee's employment + 6 months	SECURE DISPOSAL	
2.13	All records leading up to the appointment of a new member of staff – successful candidate	Yes	Yes	All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 years	SECURE DISPOSAL	
2.1.4	Pre-employment vetting information – DBS Checks	Yes	No	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	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	Yes	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					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.2.1	Staff Personal File	yes	Yes	Termination of Employment + 6 years	SECURE DISPOSAL	
2.2.2	Timesheets	yes	Yes	Current year + 6 years	SECURE DISPOSAL	
2.2.3	Annual appraisal/ assessment records	yes	Yes	Current year + 5 years	SECURE DISPOSAL	
2.2.4	School Privacy Notice which is part of GDPR compliance			Until superseded + 6 years		

	2.3 Management of Disciplinary and Grievance Processes					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	yes	Yes	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded	
2.3.2	Disciplinary Proceedings		Yes			
	oral warning			Date of warning + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]	
	written warning – level 1			Date of warning + 6 months		
	written warning – level 2			Date of warning + 12 months		
	final warning			Date of warning + 18 months		
	case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL	

	2.4 Health and Safety					
Ref	**Basic file description**	**Statutory provisions**	**Data Protection Issues/personal information**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.4.1	Health and Safety Policy Statements		No	Life of policy + 3 years	SECURE DISPOSAL	
2.4.2	Health and Safety Risk Assessments		No	Life of risk assessment + 3 years	SECURE DISPOSAL	
2.4.3	Recordsrelatingto accident/ injury at work		Yes	Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL	
2.4.4	Accident Reporting		Yes			
	Adults Accident reporting records relating to individuals who are over 18 years of age at the time of the incident	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980 Social Security (Claims and Payments) Regulations 1979. SI 1979 No 628 Social Security (Claims and Payments) Regulations SI 1987 No 1968 Revokes all but Part 1 of SI 1979 No 628 Social Security Administration Act 1992 Section 8. Social Security (Claims and Payments) Amendment (No 30 Regulations 1993 SI 1993 No 2113 Allows the information to be kept electronically	yes	Date of the incident + 6 years The Accident Book – BI 510 - 3 years after last entry in the book This includes the new format to be used from 1/1/04 This means that, if it takes 5 years to complete, the book must be retained for a further 3 years from the last entry Completed pages must be kept secure with restricted access. Data Protection Act 2018 and GDP	SECURE DISPOSAL	

	Children Accident reporting records relating to individuals who are under 18 years of age at the time of the incident	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980 Social Security (Claims and Payments) Regulations 1979. SI 1979 No 628 Social Security (Claims and Payments) Regulations SI 1987 No 1968 Revokes all but Part 1 of SI 1979 No 628 Social Security Administration Act 1992 Section 8. Social Security (Claims and Payments) Amendment (No 30 Regulations 1993 SI 1993 No 2113 Allows the information to be kept electronically		DOB of the child + 25 years The Accident Book – BI 510 - 3 years after last entry in the book This includes the new format to be used from 1/1/04 This means that, if it takes 5 years to complete, the book must be retained for a further 3 years from the last entry Completed pages must be kept secure with restricted access. Data Protection Act 2018 and GDPR	SECURE DISPOSAL	
2.4.5	Records relating to any reportable death, injury, disease or dangerous occurrence (RIDDOR). For more information see http://www.hse.gov.uk/RIDDOR/	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 SI 2013 No 1471 Regulation 12(2)	Yes	Date of incident + 3 years provided that all records relating to the incident are held on personnel file [see 2.4.2 above]	SECURE DISPOSAL	
2.4.6	Control of Substances Hazardous to Health (COSHH)	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)	No	Date of incident + 40 years	SECURE DISPOSAL	
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	No	Last action + 40 years	SECURE DISPOSAL	

2.4.8	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation Maintenance records or controls, safety features and PPE ---------- Dose assessment and recording	The Ionising Radiation Regulations 2017. SI 2017 No 1075 Regulation 11 As amended by SI 2018 No 390 Personal Protective Equipment (Enforcement) Regulations 2018	No	2 years from the date on which the examination was made and that the record includes the condition of the equipment at the time of the examination. ---------- To keep the records made and maintained (or a copy of these records) until the person to whom the record relates has or would have attained the age of 75 years, but in any event for at least 30 years from when the record was made	SECURE DISPOSAL	
2.4.9	Fire Precautions logbooks		No	Current year + 6 years	SECURE DISPOSAL	
2.4.10	Health and safety file to show current state of building, including all alterations (wiring, plumbing, building works, etc.), to be passed on in the case of change of ownership			Pass to new owner on sale or transfer of building		

	2.5 Payroll and Pensions					
Ref	**Basic file description**	**Statutory provisions**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.5.1	Maternity pay records		Yes	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	
2.5.3	Absence record	Yes	Yes	Current Year + 3 years	SECURE DISPOSAL	
2.5.4	Batches	Taxes Management Act 1970 Income and Corporation Taxes 1988	Yes	Current Year + 6 years	SECURE DISPOSAL	
2.5.5	Car mileage output	Taxes Management Act 1970 Income and Corporation Taxes 1988	Yes	Current year + 6 years	SECURE DISPOSAL	

2.5.7	Insurance	Taxes Management Act 1970 Income and Corporation Taxes 1988	Yes	Current year + 6 years	SECURE DISPOSAL	
2.5.8	National Insurance – schedule of payments	Taxes Management Act 1970 Income and Corporation Taxes 1988	yes	Current year + 6 years	SECURE DISPOSAL	
2.5.9	Overtime Taxes	Management Act 1970 Income and Corporation Taxes 1988	yes	Current year + 3 years	SECURE DISPOSAL	
2.5.10	Payroll awards		yes	Current year + 6 years	SECURE DISPOSAL	
2.5.11	Payroll – gross/net weekly or monthly	Taxes Management Act 1970 Income and Corporation Taxes 1988	Yes	Current year + 6 years	SECURE DISPOSAL	
2.5.12	Payroll reports	Taxes Management Act 1970 Income and Corporation Taxes 1988	yes	Current year + 6 years	SECURE DISPOSAL	
2.5.13	Pension payroll	Taxes Management Act 1970 Income and Corporation Taxes 1988	yes	Current year + 6 years	SECURE DISPOSAL	
2.5.14	Personal bank details	If employment ceases then end of employment + 6 years		Until superseded + 3 years	SECURE DISPOSAL	
2.5.15	Sickness records			Current year + 3 years	SECURE DISPOSAL	
2.5.16	Superannuation adjustments or reports	Taxes Management Act 1970 Income and Corporation Taxes 1988	yes	Current year + 6 years	SECURE DISPOSAL	

2.5.17	Tax forms P6/P11/ P11D/P35/P45/P46/ P48	The minimum requirement - as stated in Inland Revenue Booklet 490 - is for at least 3 years after the end of the tax year to which they apply. Originals must be retained in paper/ electronic format. It is a corporate decision to retain for current year + 6 years. Employees should retain records for 22 months after current tax year		Current year + 6 years	SECURE DISPOSAL	
2.5.18	Time sheets/clock cards/flextime		yes	Current year + 3 years	SECURE DISPOSAL	

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

3. Financial Management of the School

	3.1 Risk Management and Insurance					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.1.1	Employer's Liability Insurance Certificate		No	Closure of the school + 40 years	SECURE DISPOSAL	

	3.2 Asset Management					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.2.1	Inventories of furniture 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

Ref	Basic file description	Personal information	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
3.3.1	Annual Accounts		No	Current year + 6 years	STANDARD DISPOSAL	
3.3.2	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	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					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.4.1	All records relating to the management of contracts under seal		No	Last payment on the contract + 12 years	SECURE DISPOSAL	
3.4.2	All records relating to the management of contracts under signature		No	Last payment on the contract + 6 years	SECURE DISPOSAL	
3.4.3	Records relating to the monitoring of contracts		No	Current year + 6 or 12 years	SECURE DISPOSAL	

	3.5 School Fund					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
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					
Ref	**Basic file description**	**Personal Information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.6.1	Free School Meals Registers	Yes	Yes	Current year + 6 years	SECURE DISPOSAL	
3.6.2	School Meals Registers	Yes	Yes	Current year + 3 years	SECURE DISPOSAL	
3.6.3	School Meals Summary Sheets	Yes	No	Current year + 3 years	SECURE DISPOSAL	

4. Property Management

This section covers the management of buildings and property.

	4.1 Property Management					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues/personal information**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
4.1.1	Title deeds of properties belonging to the school	no	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					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues/ personal information**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
4.2.1	All records relating to the maintenance of the school carried out by contractors		No	These should be retained whilst the building belongs to the school and should be passed on to any new owners if the building is leased or sold. See 2.4.10	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 These should be retained whilst the building belongs to the school and should be passed on to any new owners if the building is leased or sold. See 2.4.10	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					
Ref	**Basic file description**	**Personal data**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	yes	Yes			
	Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. [2]	
	Secondary			Date of Birth of the pupil + 25 years	SECURE DISPOSAL	
5.1.2	Examination Results – Pupil Copies	yes	Yes			
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.	

[2] This will include: (i) to another primary school (ii) to a secondary school (iii) to a pupil referral unit (iv) 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

	Internal			This information should be added to the pupil file		
5.1.3	Child Protection information held on pupil file	yes		If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded	
5.1.4	Child protection information held in separate files			DOB of the child + 25 years then review. No files should be kept by the infant or primary school on the child's transfer to secondary or to another school. All child protection records should be transferred with the child when the exit the school.	SECURE DISPOSAL – these records MUST be shredded	

	5.2 Attendance					
Ref	**Basic file description**	**Personal data**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.2.1	Attendance Registers	yes	Yes	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL	
5.2.2	Correspondence relating to authorized absence			Current academic year + 2 years	SECURE DISPOSAL	

	5.3 Special Educational Needs					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.3.1	Special Educational Needs files, reviews and Individual Education Plans		Yes	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. 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	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	

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

7. Extra Curriculum Management

7.1 Educational Visits outside the Classroom					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom–Primary Schools	No	Date of visit + 14 years	SECURE DISPOSAL	
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Date of visit + 10 years	SECURE DISPOSAL	
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes	Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.	

7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	DOB of the pupil involved in the incident+25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils		

	7.2 Walking Bus					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
7.2.1	Walking Bus Registers	Yes	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					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
7.3.1	Day Books	Yes	Current year + 2 years then review		
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes	Whilst child is attending school and then destroy		
7.3.3	Referral forms	Yes	While the referral is current		
7.3.4	Contact data sheets	Yes	Current year then review, if contact is no longer active then destroy		
7.3.5	Contact database entries	Yes	Current year then review, if contact is no longer active then destroy		
7.3.6	Group Registers	Yes	Current year + 2 years		

8. Central Government and Local Authority

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

	8.2 Central Government					
Ref	**Basic file description**	**Personal information**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
8.2.1	OFSTED reports and papers		No	Life of the report then REVIEW	SECURE DISPOSAL	
8.2.2	Returns made to central government		No	Current year + 6 years	SECURE DISPOSAL	
8.2.3	Circulars and other information sent from central government		No	Operational use	SECURE DISPOSAL	

Appendix A – List of School Records and Data safely destroyed

The following sheet can be completed or alternatively documented in a spreadsheet.

Ref Number	File/Record Title	Description	Reference or Cataloguing Information	Number of Files Destroyed	Method of destruction	Confirm (i) Safely destroyed (ii) In accordance with Data Retention Guidelines Tick (√)	Authorized by:
e.g.	*School Invoices*	*Copies of purchase invoices dated 2011/12*	*Folders marked "Purchase Invoices 2011/12" 1 to 3*	*3 Folders*	*Shredding*	√	
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							

Appendix B

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 in which records are stored should be secured against intruders and have controlled access to the working space. Storage areas should be regularly monitored and checked for any damage or emerging risks, especially during holiday periods.

Hazards
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, fireproof cabinets may need to be considered. However, fireproof cabinets are expensive and very heavy, so they should only be used in special circumstances. Core records should be identified so that they may receive priority salvage or protection in the event of an incident affecting the storage area. Records which are stored on desks, shelves or in cupboards which do not have doors will suffer more damage than those which are stored in cupboards/cabinets which have closefitting 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 at this height). 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, 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.