Document title	**Records Management Policy & Guidelines**
Version	**4.0**

LIGHTHOUSE SCHOOLS PARTNERSHIP

RECORDS MANAGEMENT POLICY AND GUIDELINES

Statutory Policy

Policy Approved by the Trust Board	
Signed:  Name: Adele Haysom Chair of Board of Trustees	Date: 29 January 2025
Authorised for Issue	
Signed:  Name: Gary Lewis Chief Executive Officer (CEO)	Date: 29 January 2025

Document History

Version	Author/Owner	Drafted	Comments
1.0	Louise Malik	August 2018	Based on information sourced from and produced by the Information and Records Management Society (IRMS).
2.0	Louise Malik & Tracey Joyce	September 2020	Scheduled update with advice from One West and updated information from Information and Records Management Society (IRMS).
3.0	Louise Malik & Neill Bird	August 2022	Scheduled update with advice from One West
4.0	Beth Watts	Autumn 2024	Scheduled update with advice from One West

Review cycle	Biennial
Review date	Autumn Term 2026

This policy applies to all schools and employees within the Lighthouse Schools Partnership.

Contents

RECORDS MANAGEMENT POLICY

1. Introduction

The Lighthouse Schools Partnership recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the Trust.

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

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

2. Objectives

The objective of this policy if to define a framework for The Lighthouse Schools Partnership to manage data, information, and records.

3. Definitions

Data - Raw facts and figures that supply the basis for information.

Information - Data which has been collected, organised, ordered and given both meaning and context.

Record - Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations, or in the transaction of business.

Confidential Waste - See Appendix 1.

4. Scope

This policy applies to all employees of the Lighthouse Schools Partnership including contract, agency and temporary staff, volunteers and employees of partner organisations working on behalf of the Lighthouse Schools Partnership.

All records created, held, and maintained by The Lighthouse Schools Partnership in the course of its duties are covered by this policy. This is irrespective of the format of the information, including, but not limited to:

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

5. Responsibilities

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

The Chief Financial and Operating Officer (for Trust central records) and the Headteacher (for School records) have overall responsibility for this policy. They are also responsible for giving guidance for good records management practice and for promoting compliance with this policy so that information can be retrieved easily, appropriately and in a timely way.

All members of staff and employees are individually responsible for the records they create or hold. Individuals must ensure that records are accurate, maintained securely, and disposed of in accordance with this policy.

6. Creation & Storage

All School staff are responsible for creating and maintaining data, information and records in relation to their work, and storing them in a way which ensures that they can be identified and retrieved when required.

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

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

The retention of records for longer than necessary is in breach of the UKGDPR, and the duplication of records should be limited tooptimise the use of space for storage purposes and to aid data accuracy.

7. Retention and Disposal

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

The retention of specific documents may be necessary to:

- Fulfil statutory or other regulatory requirements.[1]
- Evidence events/agreements in the case of disputes.
- Meet operational needs.
- Ensure the preservation of documents of historic or other value.
- Evidence child protection matters.

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

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

Conversely, the permanent retention of all paper or electronic documents where there is no business needor other legal basis to retain them, poses regulatory and security risks, as well as being a breach of personal data.

Appropriate secure disposal is accordingly implemented at the school/Trust in accordance with the school's/Trust's retention schedule for the following reasons:

- To comply with Article 5 of the UKGDPR which states that personal data must not bekept in an identifiable form for longer than is necessary
- To free-up physical or digital storage space (there is evidence that the de-cluttering of officeaccommodation can be psychologically beneficial for employees.);
- To reduce the risk of fire (in the case of paper records);
- To lessen the risk of a data breach through data loss or unauthorised access.
- To increase the efficiency of the exercising of data subject rights

7.1 Retention Schedule

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

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

Definition of Retention Periods

Defining a retention period will be determined on one of the following three factors:

- Statutory requirements.
- Codes of Practice and guidance published by professional bodies.

[1] The Covid-19 Public Inquiry issued a Document Preservation Notice on 11th November 2022. This inquiry will cover all aspects of the country's response to the Covid-19 pandemic and requires organisations to preserve all documents relating to the pandemic and the following recovery period. For more information about the inquiry visit: https://covid19.public-inquiry.uk/.

- In the absence of the above, the retention period will be determined by the needs of the Council.

Defining the retention period based on organisation needs must be approved by the relevant senior manager and where necessary in consultation with the DPO.

Reviewing Retention Periods

Most retention periods will remain static and will relate to legal requirements to retain data. However, retention periods based on codes of practice and guidance published by professional bodies may vary. Any changes to known retention periods should be raised with the Data Protection Lead and where necessary the DPO.

Course of Action at the End of the Retention Period

When a record reaches the end of its retention period in most cases it will be deleted or destroyed. However, these are not the only courses of action that can be taken, and consideration must be made to the relevance of the data for other uses.

In most cases the requirement for further use of data will be identified prior to processing, however there may be occasion where a dataset is identified as having particular relevance to the needs of the organisation.

The following may occur to data after the period of use has expired: [delete where not applicable]

- Anonymisation for statistical needs.
- Transfer to an appropriate archive where it is in the public interest.
- Scientific or historical research purposes.

Appropriate safeguards must be put in place to ensure that wherever personal data is used beyond its original period of retention it is done so legally and in compliance with DPA 2018 and guidance from the Information Commissioner's Office (ICO).

7.2 Disposal

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

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

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

If records are accidentally destroyed or discovered, this should be reported as a data breach to the school / Trust Data Protection Lead, in line with the Data Breach Policy.

Wherever practicable and appropriately secure, disposal methods should encourage recycling.

Electronic files are securely overwritten, in accordance with government guidance, and other media is shredded, incinerated or otherwise disintegrated for data

A destruction log is kept of all data that is disposed of. The log includes thedocument type (e.g. Personal data), date of destruction, method and who authorised the destruction.

Once data has been deleted, it is deemed to be a permanent deletion, irrespective of whether it could technically be reconstructed from a back-up.

7.3 Archiving

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

8. Monitoring and Compliance

This policy is reviewed biennially.

Compliance with this policy shall be monitored through a review process undertaken by the person with overall responsibility for records management within the Trust.

This will be achieved by an annual survey to check if records are stored securely and can be accessed appropriately.

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

9. Relationship with existing policies

This policy and associated guidelines have been drawn up within the context of:

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

Appendix A - Records Management Guidelines

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

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

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

These are only guidelines and have no legal status, if you are in doubt about whether a piece of information should be included on the file please contact the Headteacher or the Chief Financial and Operating Officer for the Trust.

This guidance includes:

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

Managing Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System, whether they are held in paper form or in various electronic systems. The pupil record(s) must accompany the pupil to every school they attend and contain information that is accurate, objective and easy to access.

These guidelines are based on the assumption that the pupil record is a principal record and that all informationrelating to the pupil will be found in the file (although it may spread across more than onefile and may be held in a number of electronic systems).

1. File covers for paper pupil records

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

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

2. Recording information

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

3. Primary School records

3a. Opening a file

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

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

- Surname
- Forename
- DOB
- Unique Pupil Number

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

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

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

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

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

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

- Privacy Notice [if these are issued annually only the most recent need be on the file]
- Years Record
- Annual Written Report to Parents
- National Curriculum and Religious Education Locally Agreed Syllabus Record Sheets
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (must be stored in the file in a sealed envelope clearly marked as such)
- Child protection reports/disclosures (must be stored in the file in a sealed envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

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

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

3c. Transferring the pupil record to the secondary school

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

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

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

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

4. Secondary School records

Items that must be included on the pupil record:

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

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

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

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

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

6. Safe destruction of the pupil record

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

7. Transfer of a pupil record outside the of the Uk or EU area

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

8. Storage of pupil records

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

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

Good Practice for Managing E-mail

1. Introduction

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

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

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

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

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

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

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

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

d. E-mail is not necessarily deleted immediately.

E-mails can remain in a system for a period of time after you have deleted them. You must remember that although you may have deleted your copy of the e-mail, the recipients may

not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 2018 (DPA 2018). Once an email has left your system you have no control over where that data goes, who might have access to it or whether it ever gets fully deleted, so ensuring that only the minimum necessary data is sent to the right person is paramount.

e. E-mail can form a contractual obligation.

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

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

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

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

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

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

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

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

3. Creating and sending e-mail

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

Do I need to send this e-mail?

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

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

Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain e-mails. It is very important to consider whether the people who have been included in the email need to know the information. Indiscriminate sharing of information not only generates

unnecessary email traffic which may then fail to be disclosed as part of a subject access request, but may also breach data protection principles.

Always check whether you have used BCC when sending to multiple recipients. Unauthorised disclosure of email addresses constitutes a data breach and has led to the imposition of serious fines by the Information Commissioner's Office on organisations. If using mail merge

check that none of the fields have become corrupted, as this can lead to a mismatch of information and a consequent data breach.

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

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

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

Use a consistent method of defining a subject line

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

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

Ensure that the e-mail is clearly written

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

Sending attachments

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

Disclaimers

Adding a disclaimer to an e-mail may help to mitigates risk, such as sending information to the wrong recipient, or helps to clarify the school's position in relation to the information being e-mailed. Typically, they cover the fact that information may be confidential, the

intention of being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the school.

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

4. Managing received e-mails

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

a) Manage interruptions

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

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

b) Use rules and alerts

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

c) Using an out of office message

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

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

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

d) Receiving emails containing personal data

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

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

5. Filing e-mail

Attachments only

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

to a paper file. The e-mail can then be deleted.

E-mail text and attachments

Where the text of the e-mail adds to the context or value of the attached documents it may be necessary to keep the whole e-mail. The best way to do this and retain information that makes up the audit trail, is to save the e-mail in .msg format. This can be done either by clicking and dragging the e-mail into the appropriate folder in an application such as MS Outlook, or by using the "save as" function to save the e-mail in an electronic filing system.

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

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

E-mail text only

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

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

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

How long to keep e-mails?

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

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

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

Information Security & Business Continuity

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

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

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

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

1. Digital Information

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

a. Operate an effective back-up system

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

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

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

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

b. Control the way data is stored within the school

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

c. Maintain strict control of passwords

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

d. Manage the location of server equipment

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

e. Ensure that business continuity plans are tested

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

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

2. Hard Copy Information and Records

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

a. Fire and flood

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

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

b. Unauthorised access, theft or loss

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

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

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

c. Clear Desk Policy

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

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

3. Disclosure

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

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

Staff must be aware that under GDPR, the school is obliged to have contracts in place with parties who process data on the school's behalf.

This is a far-reaching requirement, and would include for example, IT contractors, work experience placements or school photography companies.

4. Risk Analysis

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

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

5. Responding to Incidents

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

a. Major Data Loss/Information Security Breach

Schools must ensure that all staff are aware of the procedures for a potential data breach in the Data Protection Policy. The school may need to be ready to pull together an incident response team to manage the situation. Schools should consider assigning a specific member of staff to deal with press/media enquiries. In the event of a potential data breach the schools Data Protection Lead and/or Headteacher must inform the Trust immediately. Any breach must be reported to ICO within 72 hours where it is likely that there is a risk to someone's rights and freedoms. Individuals must also be notified where the breach is likely to result in a high risk to their rights and freedoms.

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

b. Fire/Flood Incident

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

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

Further Information and Guidance

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

Local Authority Resilience Forums

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

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

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

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

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

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

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

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

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

2. Safe destruction of records

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

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

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

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

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

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

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

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

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

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

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

3. Transfer of records to the Archives

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

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

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

4. Transfer of information to other media

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

Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media. It is essential to have procedures in place so that conversion is done in a standard way. This means that organisations can prove that the

electronic version is a genuine original and could not have been tampered with in any way. Reference should be made to 'British Standard 10008:2008 'Evidential weight and legal admissibility of electronic information' when preparing such procedures.

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

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

Digital Continuity

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

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

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

1. The Purpose of Digital Continuity Statements

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

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

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

2. Allocation of Resources

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

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

3. Storage of records

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

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

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

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

4. Migration of Electronic Data

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

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

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

5. Degradation of Electronic Documents

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

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

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

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

6. Internationally Recognised File Formats

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

7. Digital Continuity Statement

Each digital continuity statement must include the following information:

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

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

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

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

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

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

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

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

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

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

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

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

This should be agreed with the appropriate technical staff.

g. Retention of all software specification information and licence information

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

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

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

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

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

8. Review of Digital Continuity Statements

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

Appropriate Storage for Physical Records

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

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

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

Environmental Damage - Fire

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

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

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

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

Environmental Damage - Water

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

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

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

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

Environmental Damage – Sunlight

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

Environmental Damage – High Levels of Humidity

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

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

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

Environmental Damage – Insect/Rodent Infestation

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

Retention Guidelines

1. The purpose of the retention guidelines

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

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

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

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

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

2. Benefits of a retention schedule

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

- Managing records against the retention schedule is deemed to be "normal processing" under the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000. Members of staff must be aware that once a Freedom of Information request is received or a legal hold imposed then records disposal relating to the request or legal hold must be stopped.
- Members of staff can be confident about safe disposal information at the appropriate time.
- Information that is subject to Freedom of Information and Data Protection legislation will be available when required. The school is not maintaining and storing information unnecessarily.

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.

The retention schedule attached as Appendix A contains recommended retention periods for the different record series created and maintained by schools in the course of their business. The schedule refers to all information regardless of the media in which it is stored.

Some of the retention periods are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000.

Managing record series using these retention guidelines will be deemed to be "normal processing" under the legislation mentioned above. If record series are to be kept for longer or shorter periods than laid out in this document the reasons for this need to be documented.

Using the Retention Schedule

The Retention Schedule is divided into eight sections:

1. Management of the School

2. Human Resources

3. Financial Management of the School

4. Property Management

5. Pupil Management

6. Curriculum Management

7. Extra-Curricular Activities

8. Central Government and Local Authority

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

Appendix B – Retention Schedule

Please see the PDF document, **Retention Schedule,** that accompanies this policy.

Appendix C - What is Confidential Waste?

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

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

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

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

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

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

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

- Information which Lighthouse Schools Partnership would be affected by any loss of, or unauthorised access to.

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

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

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