Records Management and Retention Policy

The Stour Federation

Date of publication: May 2025 Review date: May 2028

1. ABOUT THIS POLICY

The Stour Federation recognises that by efficiently managing our records, we will be able to comply with our legal and regulatory obligations, and to contribute to the effective overall management of our school. Maintaining good records helps us to provide the evidence needed to protect the legal rights and interests of our school, and for us to demonstrate our performance and accountability.

This policy provides the framework through which we will effectively manage our records.

It covers:

- Scope.
- Responsibilities.
- Safe destruction of records.
- Freedom of Information Act 2000.
- Relationships with existing policies.

2. SCOPE

This policy applies to all records created, received or maintained by permanent and temporary staff of each school in the course of carrying out its functions. Also, by any agents, contractors, consultants or third parties acting on behalf of the school.

Records are defined as all documents which facilitate the business carried out by each school and which are thereafter retained to provide evidence of transactions or activities. These records may be created, received or maintained in hard copy or electrical format e.g. paper documents, scanned documents, emails, audio and video recordings, text messages, notes of telephone and spreadsheets, documents, presentations, etc.

3. LEGISLATION AND GUIDANCE

This policy meets the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000 (FOIA 2000). It is based on the IRMS Toolkit For Schools, the Department of Education – Data Protection Toolkit for Schools, Department of Education – Annual Review of School Records and Safe Destruction Checklist, and guidance published by the Information Commissioner's Office (ICO) on the GDPR.

4. RESPONSIBILITIES

The Trust follows guidance from the Department for Education regarding the record keeping and retention information for academies and academy trusts.

4.1 Governance

The Trust Board and Local Academy Councils have a statutory responsibility to maintain the school's records and record keeping systems in accordance with the regulatory framework of the

school.

4.2 Responsible Persons

The CEO (Data Protection Lead) and Headteachers (Data Champions) will provide guidance on good records management practices within each school and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way.

The Data Protection Lead and Data Champions will monitor compliance with this policy by ensuring that the 'Annual Review of School Records Checklist' is completed at least annually.

4.3 All Staff

It is the responsibility for all members of staff to ensure that our school does not keep personal information for longer than is necessary for the purpose or purposes for which it was collected.
Our school will manage and document its records disposal process in line with the guidance provided by the IRMS Toolkit for Schools.

It is the responsibility of all members of the school to ensure that they:

- Manage school records consistently in accordance with school's policies and procedures.
- Properly document their actions and decisions.
- Hold personal information securely.
- Only share personal information appropriately and do not disclose it to an unauthorised third party.
- Dispose of records securely in accordance with the guidance set out in the Information and Records Management Society's toolkit for schools. https://irms.org.uk/page/SchoolsToolkit.

Staff who do not comply with this policy may face disciplinary action.

This policy does not form part of any employee's contract of employment and may be amended at any time.

5. SAFE DESTRUCTION OF RECORDS

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

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

Any other records will be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways.

Do not put records containing personal information with the regular waste or in a skip.

Where an external provider is used, where possible, all records will 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 will be trained in the handling of confidential documents.

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

PLEASE NOTE: 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.

6. FREEDOM OF INFORMATION ACT 2000

The Freedom of Information Act 2000 requires us to maintain a list of records which have been destroyed and who authorised their destruction.

When destroying either a substantial amount of information or information which is of a particularly sensitive or important nature, members of staff should record at least:

- The information that has been destroyed.
- The volume of the information that has been destroyed.
- Who provided authorisation to destroy the information.
- The date the information was destroyed.

By following this guidance and completing the Annual Checklist, we will ensure that our school is compliant with the Data Protection rules and the Freedom of Information Act 2000.

7. RELATIONSHIP WITH EXISTING POLICIES

This policy is linked to our:

- Data Protection Policy.
- Information Security Policy.

Retention FAQs from the School Data Protection Officer

What are we required to do under the CTF process?
When a child leaves your school to go to another school the information you hold about them should generally follow them to their next educational establishment.

All maintained schools are required to send certain information in the form of a Common Transfer File (CTF). Academies and independent schools are not legally required to follow the CTF process but it is recommended that they do.

A detailed description of what is included in a CTF, the required format of a CTF and the required means of sending a CTF, can be found in the Department of Education's latest guidance, which can be found here.

The law which covers the CTF process states that a CTF must be sent to the child's new educational establishment within 15 school days of the child no longer being registered at your school or if the child is registered at two schools, within 15 school days of the child being registered at their new school. Schools do not always need to wait until a child is registered at their new school before sending the CTF.

We would recommend that you send your CTFs once you are reasonably certain that the pupil will be attending their new school.

Alongside the CTF, you are also required to send their educational record to the child's new school. This must also be done within 15 school days of the child no longer being registered at your school.

If a child leaves your school and you are unsure of their next destination the CTF process should be followed, and your pupil's information should be sent to your local authority instead.

What is in a pupil's educational record?
The definition of a child's educational record is very broad. It refers to information and documents which have been generated by or on behalf of the school's teachers and governors.

As such a child's educational record will include but is not limited to the following:

- Data collection sheets.
- Annual reports to parents.
- SEND Information, plans, records or reports.
- Child protection/safeguarding information.
- Details of complaints made by parents or pupils.
- Exam results.
- Any information from the child's previous school.
- Any information relating to exclusions.

When pupil's leave your school for a new establishment, you are required to send all of the above information to their next school.

Technically, a child's educational record would also include – photo consent forms, consents for

trips, pupil work, photographs, newsletters, old data collection sheets, etc.

Legislation does not make a distinction of what part of a pupil's educational record should be sent to the child's new school and what should not. However, we would advise that only the information which you consider of value to progressing the child's education or building a picture of the child's circumstances and needs should be sent to their new school.

What do we do with pupil information that did not go to the child's new school?
Broadly, information that does not go with the child to their new school should either be retained or securely destroyed.

Retention periods describe the *minimum* amount of time information is required/recommended to be retained for. If circumstances require you to retain information for longer, you are able to do so as long as you are able to justify why you have decided to retain the information.

Pages 67-76 of the DFE's guidance on Data Protection provides good contextual examples of the considerations that you may make when deciding to hold on to certain pieces of information.

What does good records management look like?
This will be dependent on your individual setting, but typically it will involve something similar to the below process:

- School leaders are responsible for ensuring that records are appropriately managed throughout each school.
- Individual members of staff are aware of: the information they hold, what information they are required to destroy/retain, and how the school requires them to dispose of this information.
- There is an organised process for ensuring that information is reviewed or destroyed when appropriate. For most schools, this is a general review of the information held in their organisation at the end of the academic year, including documents to be sent to children's new schools.
- The school's archive facilities are organised, clearly labelled and have appropriately secure, restricted access.
- The school documents the information that they have destroyed. Recording the information that you have destroyed will help school's evidence that they monitor retention periods appropriately. This practice will also help you when responding to SARs or FOI requests.

Can we delete old pupil information from our MIS?
The principles of retention and safe destruction also apply to information held electronically. You should ask your IT services provider how you can delete historic information from your MIS system.

When you review historic information on your MIS and in hard copy, please bear in mind the Independent Inquiry into Historic Child Sexual Abuse (IICSA).

IICSA has placed a hold on all documents relating **directly or indirectly to the sexual abuse of children or to child protection and care**. This information should be retained and not deleted until the conclusion of the inquiry.

Please refer to the 'Records Keeping' section in 'Keeping Children Safe in Education' for further details about how to keep and store this information.

How do we safely destroy information?
The GDPR does not prescribe a single method of secure destruction.

Instead, you should take 'appropriate steps' to ensure the security of your information. What will be considered to be appropriate will be dependent on the size of your organisation and the nature and volume of the sensitive information you are seeking to destroy.

For information to be considered 'securely destroyed', it should be made permanently unreadable and unable to be reconstructed. The process of destruction should also ensure that the information being destroyed remains confidential throughout its destruction.

The same principle of secure destruction applies to both 'hard-copy' and digital information.

A lot of our schools engage third parties to destroy paper records on their behalf. This can be both onsite and offsite destruction.

Below is a checklist of requirements that may help you to decide whether the service you have chosen provides a sufficient level of security:

- Your shredding company should provide you with a Certificate of Destruction which you can retain for your own records.
- You should have a contract in place with your shredding company which contains the specified data protection terms discussed in - Bulletin 8, Bulletin 8.5 and Bulletin 16. The terms contained in this contract will require that your shredding company keep information safe in transit, that their employees will keep any information confidential, etc.
- There are various standards of shredding ranging from a DIN 1 – 6. The higher the DIN number the more thorough the shredding is considered to be. DIN 3 – 4 is considered to be appropriate for school information.
- The British Standard Institution and the International Standards Organisation provide the following certifications which your secure shredding company should have:
    - BSEN15713 – secure destruction of confidential material.
    - BS7858 – staff security vetting.
    - ISO 9001 – service quality.
    - ISO 14001 – environmental management standards.
    - ISO 27001 – information security

Similarly, there are a number of ways in which electronic information can be deleted and not all of them will mean that the information cannot be recovered. It is important that you consult with your IT services provider about the best means of destruction for you.

More information regarding the standards of destruction for digital information can be found here and here.

Can we continue to display images of old students?
A lot of the images of your students will be processed on the lawful basis of consent. One of the main changes implemented by the GDPR is that individuals can now withdraw their consent at any time.

Furthermore, most of your consent forms will advise individuals that the consent to use their images will only be valid whilst they are still a pupil/member of staff at your school.

If consent is withdrawn or expires when a child leaves your school, in most circumstances you will not be able to continue to use the data in the same way as you had done before.

This means that it is important that images used within the school and externally are regularly reviewed, and marketing material is updated at regular intervals.

There may be scope to retain some images of former pupils in your school archive.

Remember - the GDPR only applies to data which can lead to the identification of a living individual, as such it may be arguable that very old images of students/individuals may no longer be considered as data subject to the GDPR.

Rules of Thumb
Below are some rules of thumb which may act as a good starting point when you manage the records in your school. We would always recommend that a detailed review is conducted and information is judged on a case by case basis.

As always, please refer to the IRMS Toolkit for Schools for detailed guidance on retention periods.

Location in the School	Typical documents	Suggested Retention Period
The Classroom	Pupil work, safeguarding + SEND information, Pupil Images, Classroom Apps.	Information in the classroom should **follow the child through the school**or should be sent to a central location so it can be stored/destroyed as appropriate – e.g. to the office to be added to the pupil file. All other information should be destroyed when no longer needed – e.g. at the end of the academic year.
Finance	Invoices, Account Statements, Inventories, Contracts.	Most information is stored for a minimum of **7 years (current year + 6 years**). However, some retention periods are shorter e.g. school meals registers can be destroyed after **4 years.**

Human Resources	Staff personnel files, Pensions and Payroll information, Staff Disciplinary information, Absence and sickness information.	Most information should be kept on staff personnel file, which is stored for the **duration of employee's appointment + 6 Years.** Information relating to child sexual abuse should be stored **until the conclusion of the IICSA.** Information pertaining to staff disciplinary matters may have some shorter suggested retention periods – **3 – 18 Months.** Pension and Payroll information – **4 – 7 years**.
Health and Safety	Accident Book, Risk Assessments, Logs.	**3 Years** since the: last entry, date of assessment, creation of log or incident nook.
The Office	Consent Forms, Registers, Signing-Books, Parent Pay, School Trip Information.	Consent Forms = **End of the school trip, whilst the child is in attendance at the school.** Attendance Registers = **3 years** following last entry into the register. School Trip Information = **End of the school trip,** or**25 years** following the trip if there has been an incident on the trip**.** Data Collection Sheets = **whilst current** (should be updated at least annually).
SLT	SEND Information, School Records, Safeguarding Information – Paper files and electrically – CPOMs/My Concern, Governing Body	Primary School – follow the child as they move school. Secondary School – follow the child as they move

	Records, Governor Hub.	school, if the child end's school career at school **D.O.B + 25 years**.