

Records Retention and Deletion Policy	
Policy Ref:	Gen 028
Status	
Purpose	
Committees	Trust Finance Business and Audit Committee
Other linked policies	Privacy Notice (Pupils), Privacy Notice (Workforce), Retention Schedule, Social Media Policy, Bring Your Own Device (BYOD) Policy, ICT Acceptable Use Policy, Off Site Working Policy, CCTV Policy, Privacy Notice (Governors), Special Category Data Policy, Information Policy, Remote Learning Policy
Issue date	June 2024
Review Date	June 2025

### Introduction

1. This records management policy (retention and deletion) contains recommended retention periods for the different record series created and maintained by schools across our Trust. The schedule refers to all information regardless of the media in which it is stored.
2. Some of the retention periods are governed by statute. Others are guidelines, following best practice, employed by schools throughout the United Kingdom. Every effort has been made to ensure that these retention periods are compliant with the requirements of the General Data Protection Regulation 2018 (GDPR), the Data Protection Act 2018 (DPA), Article 8, the Human Rights Act 1998, the Freedom of Information Act 2000 (FOI) and the Code of Practice on Records Management (under Section 46 of the FOI).
3. Managing records series using these retention guidelines will be deemed to be 'normal processing' under the terms of the legislation noted above. If those record series are to be kept for longer or shorter periods than the time scales held in this document, the reasons for any deviation must be recorded.
4. This policy will be reviewed by the **Trust Board** at intervals of **no less than three years**, or exceptionally, if required by changes in Data Protection, Freedom of Interest or other legislation, where relevant.

### Purpose

5. Across the Trust all schools need to create and maintain accurate records for them to function and carry out the tasks of educating and safeguarding pupils. This policy, for managing records across our schools has been drawn up in conformity with legislation, regulations affecting schools and best practice as promoted by the Information and Records Management Society of Great Britain.
6. As well as containing Record Retention tables (Gen 028A) this document sets out more general information and guidelines for recording, managing, storing and the disposal of data, whether they are held on paper or electronically (including on line), in order to assist staff, and our schools, to comply with the General Data Protection Regulation (EU) 2016/679 (GDPR) including as adopted by the United Kingdom as a result of its exit from the European Union ("UK GDPR"), General Data Protection Regulation (2018) and the Freedom of Information Act (2000). It should be read and used in conjunction with the following Trust and school policies.
7. It is expected that;
  - All information held by schools needs to be justifiable, by reference, to its purpose.
  - Schools must be transparent and accountable as to what data they hold.
  - Schools must understand and explain the reasons why they hold data.
  - Schools must be able to respond to Subject Access Requests.
  - Schools must be able to amend, delete or transfer data promptly upon any justified request.
  - Schools must be able to audit how personal data was collected and when and why.
  - Schools must hold sensitive data securely, accessed only by those with reason to view it and possess a policy as to why it is needed.

- Schools must have retention policies that reflect the importance of records relating to child sexual abuse to victims and survivors, and that they may take decades to seek access to such records.

### Disposal of data

8. Article 5(e) of the GDPR states that personal data should be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes... in order to safeguard the rights and freedoms of the data subject ('storage limitation')
9. Not all data needs to be destroyed. Each school, with the support of the GDPR team should determine whether records are to be selected for permanent preservation, or for destruction or to be transferred into a different format.
10. When information is no longer required, it should be disposed of. For confidential, sensitive or personal information, to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed.
11. Skips, 'regular' waste disposal and ribbon shredders are not secure.
12. Paper records should be cross-shredded, incinerated, or pulped.
13. CDs/DVDs/discs should be cut into pieces. Hard copy images, AV recordings and hard disks should be dismantled and destroyed. Where third party disposal companies are employed, a certificate of destruction must be obtained. Staff working for external provider should have been trained in the handling and destruction of confidential data.
14. If a school receives a request for records that have not yet been destroyed, even if they should have been destroyed, that record must still be made available to the requestor.
15. The Freedom of Information Act 2000 requires the school to maintain a list of all records that have been destroyed and who authorised their destruction. This record should be retained for 15 years. The appropriate members of staff (Data Lead) should record:
  - File reference and/or unique identifier
  - File title or brief description of contents
  - Number of files
  - Name of the authorising officer

### Transfer of records to archives

16. A school archive is different from official school records. A school archive preserves data where there is a legitimate interest in holding that information e.g. to commemorate a significant event in the life of the school. It can take on many characteristics and serve many purposes--but it neither compliments nor replaces the official record-keeping systems.
17. Where records have been identified as being worthy of permanent preservation, due to their historical or social value, they may be retained on site or transferred to the Local Authority Record Office (see local guidance Find an archive | The National Archives).
18. Where a school decides to maintain an onsite archive, the school should consult with their Data Protection Officer to implement the following steps:
  - Establish what information needs to be archived

- Select someone to serve as the archivist. This may be an additional function within an established role, to work alongside both the Data Protection Officer and Data Lead officer (where applicable).
- Select a physical location to house the collection, and determine what equipment and supplies are needed to accomplish the project for the first year and on a continuing basis e.g. safe storage, shelving
- Remember that archives can include electronic data e.g. schools may have digital photographs which are no longer displayed on their website or social media pages. Consider not only holding and cataloguing this data in a secure driver, but making potential requestors aware of its presence, through a dedicated website.
- Come to an agreement with the Local Authority Record Office, in order for the collected materials could be turned over if the school archives should be discontinued.

### Transfer of Records to other Media

19. Where lengthy retention periods have been allocated to records, schools should consider converting paper records to other media (e.g. digital or virtual, 'cloud' based). The lifespan of the media, and the ability to migrate data, should be documented in a Digital Continuity Policy. A scanning risk assessment is recommended to ensure the procedure is adequate.
20. Further information about digital continuity can be found on the National Archives website who also provide guidance on assessing and managing digital continuity risks and a digital continuity checklist. Schools that believe that they need to retain digital records over a long period on devices, software systems or in formats that may become inaccessible due to developments in technology should seek further advice from the Data Protection Officer and their IT support staff.

### Transfer of Records to other Settings and 'Last Known School'

21. When a child leaves the school, all pupil records should be transferred in a secure manner, to the child's new school. If the records contain sensitive information (e.g. Child Protection records), proof of receipt must be obtained and logged by the school's Data Lead.
22. Keeping Children Safe in Education 2022 (KCSiE) states that "where children leave the school or college, the designated safeguarding lead should ensure their child protection file is transferred to the new school or college as soon as possible, and within 5 days for an in-year transfer or within the first 5 days of the start of a new term to allow the new school or college to have support in place for when the child arrives. The designated safeguarding lead should ensure secure transit, and confirmation of receipt should be obtained. For schools, this should be transferred separately from the main pupil file."
23. All copies of data held by the school that the child has departed should then be deleted, or retained in line with the retention schedule below, including all paper records and data stored electronically. Generally, a record should be kept for tracking and auditing purposes only. Schools should be aware that where electronic systems are used, sending a pupil file to the next setting does not mean that their own copy of the file is deleted, so action should be taken to delete or archive copies retained where they are no longer required by the school that the pupil has left.
24. There are four main categories of pupil records that need to be transferred to other settings:

#### Management Information System (MIS) data

Data held on the MIS is extracted by the school using the Common Transfer File mechanism as specified in The Education (Pupil Information) (England) Regulations 2006 Statutory Instrument (SI) and in subsequent amendments (2005, 2008, 2016, 2018, 2019). The Department for Education specifies what data is to be included in the CTF file in technical specification documentation. This should mean that the majority of information held on the MIS is transferred using the CTF method. However, it is important to note that **not all personal data is transferred, only the data sets specified in the CTF schema**. If the MIS has been used to store

additional information (documents such as copies of end of year reports or letters) schools must take proactive action to ensure these are sent separately and securely. Traditionally, this sort of documentation was held in a pupil 'buff' file, but as schools have turned to digital ways of working, these are frequently stored by attaching them to the digital MIS record.

#### Safeguarding/Child Protection records

Schools frequently use vendor edtech products to hold and transfer these records. Many of these products include the functionality to electronically transfer a copy of (and obtain receipt for) pupil records directly to the next school, where the same product is also used by the receiving school. Where this is not possible, these products should have the functionality to download a pupil record for it to them be transferred electronically or printed out and delivered to the new school. Paper records should be dealt with carefully to ensure that these are safely received by the new school.

Some safeguarding edtech products enable schools to use the same system to record behavioural and other information in the same log. Schools should ensure that safeguarding/child protection records are clearly identified as such so that the receiving school can quickly identify this information. The school should consider if information such as behaviour notes needs to be transferred to the next setting, or whether it should be deleted if no longer required or relevant (e.g. a child's toileting routine may be very relevant when younger, or merits/demerits re but does not need to be part of a permanent safeguarding record).

#### Special Educational Needs records

It is becoming more common for schools to use vendor edtech products to manage these records. Whether stored in such edtech products, on school IT systems/cloud storage or on paper, the SEND co-ordinator must ensure that a complete record is compiled and passed securely to the next school.

#### Pupil 'buff' files

For many schools, in recent years, the traditional pupil buff files have dwindled in relevance and importance as schools have increasingly moved to digital storage. Schools are left with either sending or receiving folders which are very light and seemingly irrelevant. However, there will be documentation, whether on paper or electronic (on the server, in emails, in the MIS) that should be sent to the next setting that the pupil will attend. The Education (Pupil Information) (England) Regulations 2005 state that this "Educational Record" should be transferred to the next setting within 15 school days of confirmation that a pupil is registered at another school. There may be a significant amount of material that is not contained in the CTF file, safeguarding or SEND records that should be transferred to the next setting. Schools may have inadvertently not adapted their records transfer practices as management of these records have moved from a paper 'buff' file to digital format and so this should be noted where relevant on the retention schedule below.

25. Schools may wish to retain some minimal 'skeleton' data about pupils' admission, departure and next destination (where known) in order to respond to any requests for information about these pupils and for the school's historical archive. They may also wish to retain records relating to safeguarding/child protection or SEND records, even though there is no legislative requirement to do so (i.e. to have their own copy of evidence in case of any later legal action). If schools intend to create and maintain skeleton records or retain copies of records, this should be noted on the retention policy. In some instances, schools may have a legitimate interest in retaining a copy of more detailed pupil records for a longer time period. If the school does retain pupil records, then they should be prepared to justify this retention and will need to consider if a Data Protection Impact Assessment should be completed for any extended retention of records once a pupil has left the school.
26. Responsibility for maintaining the pupil record passes to the 'last known school'.
27. The school is the final or last known school if:
  - secondary phase and the pupil left at 16 years old or for post-16 or independent education, or;
  - at any point the pupil left for elective home education, they are missing from education, or have

left the UK, or have died.

28. Schools should note that tertiary colleges are not included in the definition above. This means that for pupils that leave your setting for a tertiary college, the college may not want the pupil file to be forwarded to them. If this applies to your school, you should discuss with the college what pupil records they wish to receive. They must receive the child protection file, as per the requirements of KCSiE above.
29. The Pupil Record should be retained as a whole for 25 years from the date of birth of the pupil, after which time, if no longer required, it can be deleted or destroyed.
30. SEN and other support service records can be retained for a longer period of 31 years to enable defence in a “failure to provide a sufficient education” case.
31. If a school wishes to retain data for analysis or statistical purposes, it should be done in an anonymised fashion.

### Management Information System (MIS)

32. The majority of pupil records and some staff records are held on the school MIS. Managing data retention on the MIS can be complex because different data sets held on the MIS have different retention requirements. For example, information relating to emergency contacts is only required when a pupil or staff is a member of the school, and this information can be deleted quickly once they have left, whereas information relating to school meal and other financial transactions will need to be retained for six years (plus current) in line with financial retention requirements.
33. **Until 18 August 2024, legislation states that pupil admissions records and attendance records needed to be retained for three years from the date of entry, but from 19 August 2024, this information must be retained for six years.** School staff have limited time and resources to manage these differing retention periods and should work with their MIS provider to request support on how to efficiently delete data sets from a record without deleting the entire record (or deleting all data sets except those that are required as part of the ‘skeleton’ record for long term retention). Where this is not possible, schools may make a policy decision to retain the entirety of a record for the longest applicable retention period for a data set within the MIS (usually current plus six years). The school should set out how records will be retained in the MIS in the relevant section of the Retention Table at Gen 028A.

### Records relating to Child Sexual Abuse

32. Records relating to child sexual abuse should be retained for 75 years, in line with the recommendations arising from the outcome of the Independent Inquiry into Child Sexual Abuse (IICSA). The Inquiry stated that these records should be retained for such a long period in recognition of the importance of these records to victims, but that they should be regularly reviewed during that extended retention period. Where records are held digitally, schools will particularly need to consider digital continuity where:
  - they hold relevant records for staff or governors, or
  - they are the ‘last known school’ responsible for this long retention period for any relevant pupil records.
33. Where there is evidence, or allegations of child sexual abuse, then it will almost certainly be appropriate to retain the entire pupil, staff or other record as a whole, not just the parts of the record that pertain to the abuse. Staff whose duties include reviewing or digitising records should be trained to understand the importance of any evidence or allegations of child sexual abuse that they may happen to uncover, whether that was what they were looking for and the importance of them bringing these to the attention of school leadership and/or preserving these records.
34. The Inquiry report also recommends that the UK government directs the Information Commissioner’s Office (ICO) to introduce a Code of Practice on retention of and access to records known to relate to child sexual abuse. This Policy will be updated in line with any Code of Practice from the ICO. The report states that such a code

should set out that institutions should have:

- retention policies that reflect the importance of such records to victims and survivors, and that they may take decades to seek to access such records;
- clear and accessible procedures for victims and survivors of child sexual abuse to access such records;
- policies, procedures and training for staff responding to requests to ensure that they recognise the long-term impact of child sexual abuse and engage with the applicant with empathy.

#### Retention of Records relating to Staff

35. As stated above regarding the long-term retention of minimal pupil records, schools may wish to retain very basic 'skeleton' records about staff that have worked in the school beyond the normal retention of the whole personnel/HR file. This information may include the staff name, role, contract start and end dates. This may be useful for schools who may need to respond to requests for information from/regarding staff, in the event of it being needed for litigation or other legal purpose and as part of their historical archive. If schools intend to create and maintain these records, this should be noted on the retention policy.

#### Academisation

36. Where maintained schools academise during periods specified in this document, the new Academy shall hold all School Records (including those relating to former pupil and employees), on trust for the Council from the Transfer Date.

#### Responsibility and Monitoring

37. The Headteacher/Principal and/or officer tasked with the role of Data Lead, hold primary and day to day responsibility, for implementing this policy. The Data Protection Office, in conjunction with the school, is responsible for monitoring its use and effectiveness and resolving any queries with regards the interpretation of the policy. The Data Protection Officer will consider the suitability and adequacy of this policy and will pass any amendments or alterations directly to the Headteacher/Principal.

38. All permissions to access data are granted by the Headteacher and recorded in the member of staff's personnel file.

39. All teaching and office staff are given training and guidance on accessing and managing school records, to ensure compliance with the time scales laid out under the retention schedule. All members of staff, with access to records, are expected to;

- a. Manage their current record keeping systems using the Retention Policy.
- b. Only dispose of records in accordance with the requirements outlined in this policy, if authorised to do so.
- c. Ensure that any proposed divergence from the records retention schedule and disposal policies is authorised and documented by the Headteacher/Principal.

40. This policy does not form part of any employee's contract of employment and is not intended to have a contractual effect. However, it does reflect the school's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the school but any changes will be notified to employees within one month of the date on which the change is intended to take effect. The school may also vary any parts of the procedure, including time limits, as appropriate.

41. This policy will be reviewed by the board of trustees on an annual basis.

42. Changes to this policy will be communicated with the relevant stakeholders.

#### Outline Retention Schedule

43. Derbyshire County Council's GDPR for Schools service uses an adapted version of the IRMS pro forma retention schedule (Please see Gen 028A). This offers a comprehensive and thorough review of all possible data that may be held by a school – the outline schedule, however, provides an initial overview of how the data retention policy can be applied to the records held by a school;

End