STEEL RIVER
ACADEMY TRUST

Record of Retention

TRANSFER OF CHILD PROTECTION FILES BETWEEN SCHOOLS / COLLEGES

(AS PER KEEPING CHILDREN SAFE IN EDUCATION, 2026)

Key document details

Author:	SG first/SM	**Approver:**	
Owner:	SRAT	**Version no.:**	3
Last review:	Sept 26	**Next review:**	Sept 27
Ratified:			

All young people involved with child protection services (Social Care or Police) at any time in their school life must have that information retained until the child reaches 35 years of age including pupils with Special Educational Needs. This means that the last education provider for the child will retain the file e.g. secondary phase or college. This is in line with best practice advice until further directive is given from the General Data Protection Regulations and the updated KCSIE, 2026

Current national frameworks—including the Information and Records Management Society (IRMS) Toolkit for Schools and statutory Children's Services retention schedules—outline distinct baseline timelines depending on record type. These include a standard retention guideline of 25 years of age for general education records, 35 years of age for pupils with Special Educational Needs (SEN), and up to 35 years from the formal closure of the case for statutory children's social care records.

Introduction

The purpose of this guidance is to provide clarity and consistency of practice regarding what information should be transferred onto the next school/provider and how this information should be transferred at each stage**.**

Stages

- Early years to early years transfer
- Early years to primary transfer
- Primary to secondary transfer
- Secondary to post 16 transfer
- In year transfer
- Managed move

Child Protection Files

- Child Protection files are records maintained by the setting, detailing a history of all concerns, incidents, involvement with agencies (including social care, early help and intervention) and communication with any professionals relating to concerns about the welfare of the child. Chronologies must include relevant, high-risk flags generated by the school's digital monitoring software. Where a file contains records of peer-on-peer abuse, the transferring DSL must explicitly brief the receiving DSL on risk management strategies to ensure a safe transition
- A child's file must follow them to every setting that they are educated in to ensure that incidents are not dealt with in isolation and that education professionals making decisions about children have all the information available to them. This should happen until the child is 18 years old and they are accessing further education. Please be aware that some special school settings will go up to 19 years of age. This procedure must be followed regardless of the kind of establishment the child attends e.g., state school, academy, free school or college.

- Child protection files should contain information that is accurate, factual and objective. The information as well as the organisation of the file should be easy to understand and follow. The child's voice should be thematic throughout.
- Each child protection file should contain a full and thorough chronology and a summary of significant events throughout your involvement with the child.
- **Keeping Children Safe in Education (2026) advises that all child protection files must, in their entirety, be transferred to the new school and a receipt for the file must be returned to the transferring school. This file must be transferred separately to the child's school file and secure transit ensured.**

  For example, if a child protection referral was made in Year 1 to Children's Services Social Care and no action was taken by Social Care and no other concerns were raised during the primary phase, then this child protection file would still be transferred to the new school as a record of involvement.

  Another example may be a child protection referral made in Year 5, a Section 47 carried out and child made subject to a child protection plan. The Core group is continuing at point of transfer to new school. It is the responsibility of the Designated Safeguarding Lead to contact the Social Worker and inform of change of school and contact the Designated Safeguarding Lead at the new school to arrange for them to attend the core group. The file should be transferred to the new school.

- The school/college must keep the chronology for one year only of a child protection file to ensure they have sufficient knowledge of the case and their involvement, should the case go to review or court and their involvement in the case be sought or the case is subject to individual or multi agency review
- All Designated Safeguarding Leads receiving current (live) files or closed files must keep all contents enclosed and not remove any material.
- Files will be destroyed only when the young person reaches 35 years of age including pupils with Special Educational Needs
- All receipts confirming file transfer must be kept until the child's 35th birthday including pupils with Special Educational Needs
- It is recommended that all schools distinguish a separate system for archiving and retaining information with regards to children's concerns and vulnerability. This retention guidance we would recommend is adhered to, with those children who have had a statutory plan. It would be GOOD PRACTICE for schools to maintain consistency in the management of transferring information regarding children who have had statutory plans.
- The sharing of information in this way does not remove the need for a thorough handover. It is GOOD PRACTICE that for all cases where children transfer or move schools that the Designated Safeguarding Lead's share information and communicate effectively about ANY vulnerable children. The DFE Information Sharing Advice for Practitioners advises that information can be shared where it can be evidenced to be in the best interests of children.
- All Designated Safeguarding Leads are responsible for the organisation, maintenance and transfer of all child protection files.

- Information should always be retained, stored and transferred in the best of interests of children. If in doubt you must seek support on an individual case by case basis.

Transferring files

- The transferring of files should be organised between the designated leads of each setting. Effective handovers and good discussion of the individual case will ensure a positive transition for every child.
- The transfer of the file should take place within 5 school days of the child's attendance at the new setting being confirmed. In all circumstances the sooner the handover can occur the better. Handovers should only occur once the destination of the child is certain and confirmed.
- Wherever possible files should be transferred by hand or recorded delivery. The receipt of the handover should be kept by both parties. If a signed receipt is not returned by the receiving school within 10 school days of file transfer, the transferring DSL must actively escalate and follow up until written confirmation is obtained
- For early years settings, parents should be advised regarding the transfer of the child protection file, however lack of parental consent should not prevent the file from being transferred where it is in the best interests of the child to share information with a new setting.
- For post 16 providers information should be passed over in the same way initially through a verbal discussion and handover and then the transfer of the physical file.
- Where the destination of the child is uncertain or unconfirmed, the original setting should make every effort to ascertain where the child has moved to and consider initiating their missing from education procedures in the event that the child cannot be located. For post 16 every attempt should be made by the original setting to confirm the pupil's education or employment intentions.

Pupils who are dual registered or educated off-site

- Where a pupil is dual registered or educated off site, the setting that maintains the most contact with the pupil should maintain the child protection file.
- Both settings need to liaise closely with each other to ensure positive communication is maintained and incidents that occur are shared and dealt with effectively and communicated between the settings.
- A decision should be made between the settings about how the chronology is kept up to date and shared and how information will be shared and presented at both child protection conferences/reviews and core groups.
- In any circumstance where a child may have access to other settings e.g. breakfast/after school clubs, consideration must be made to ensuring effective communication between the settings to share information and concerns.

Archiving

Child Protection files need to be stored in their entirety in hard copy or electronically with appropriate levels of security and access until the child's 35th birthday (Secondary/College settings). The decision of the storage of the files needs to be made by the school via the governing body.

In schools who use CPOMS or similar electronic recording software systems, the system archives the files once electronic transfer has occurred or in their final education setting at statutory leaving age. The files will be archived within the system till the retention date identified within the retention scheduled agreed by governing body and the provider. (The Child's 35th birthday inclusive of files of children with SEN)

Access to files

A pupil or their nominated representative have the legal right to see their file at any point during their education and even until the record is destroyed (when the pupil is 35 years old including for pupils with special educational needs) This is their right of subject to Access under the Data Protection Act 2018/GDPR.

It is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner. Information that is sensitive in nature, involves other pupils or staff should be redacted if a pupil wishes to view their file. (Please also see **appendix 1** for more detail)

Responsibility for the pupil record once the pupil leaves the school

The primary school is responsible for securely transferring the entire child protection file to the child's next education provider (e.g., secondary phase or academy) within 5 school days of confirmed attendance.
Once the transfer is complete, the final school the pupil attends until statutory school leaving age (or post-16 studies) bears the ultimate responsibility for retaining the record until the young person reaches 35 years of age. This extended timeline applies to all children, including those with Special Educational Needs (SEN). It adheres to best practice advice under the General Data Protection Regulation (GDPR) and Keeping Children Safe in Education (KCSIE) 2026, heavily exceeding the standard 6-to-7-year limitation windows outlined in the Limitation Act 1980.
Primary School Retention Exception: Following a successful transfer, the primary school will safely destroy the main file copy but must retain the case chronology for exactly one year, alongside the signed file transfer receipt which must be kept until the child's 35th birthday.

Safe Destruction of the pupil record

When child protection records reach their destruction date (such as the primary school's copy of a chronology after one year post-transfer, or a final record at age 35), they must be disposed of in accordance with secure data destruction guidelines.
Physical documents must be securely shredded (cross-shredded on-site) or disposed of by an approved, confidential waste contractor who provides a formal Certificate of Destruction. Electronic files (such as records held on CPOMS) must be permanently and securely deleted from all servers and backups.

Escalation Protocol

Where a school discovers that a child protection file was in existence but was not transferred or identified to the school, the matter should be brought to the attention of the Local Authority as soon as possible. **(**see **escalation protocol)**

Appendix 1

Subject Access Requests (SARs) and Redaction Framework
Under the Data Protection Act 2018 and UK GDPR, any child (or a parent or guardian acting on behalf of a child who lacks the maturity to understand their data rights) has a legal right to request access to their safeguarding records. Because Steel River Academy Trust (SRAT)consists of academies, access to these records is governed strictly by UK data protection legislation through the Subject Access Request (SAR) process. While local authority-maintained schools may additionally process generic student data under specific local education regulations, SRAT assesses all requests for sensitive child protection files directly against the strict statutory exemptions provided by UK data protection law to ensure the welfare of the child remains paramount.

1. The Threshold of "Best Interests" and Exemptions from Disclosure

Neither the child nor the parent has an automatic or absolute right to see child protection files. In accordance with **Keeping Children Safe in Education (KCSIE)** and the **Data Protection Act 2018**, the welfare of the child is paramount. The Trust must withhold or redact specific information if disclosing it meets any of the following statutory exemptions:

- **Serious Harm Exemption:** Disclosure is likely to cause serious harm to the physical or mental health or condition of the child or another individual.
- **Abuse or Exploitation Risks:** Disclosure could reveal that the child or another person has been the subject of, or is at risk of, child abuse, and providing the information is deemed contrary to the best interests of the child.
- **Prejudice to Law Enforcement:** Disclosure is likely to prejudice an active or ongoing criminal investigation, police inquiry, or statutory court proceeding.
- **Third-Party Confidentiality:** Disclosure would reveal information about another identifiable individual, including members of the public, neighbours, or professionals

who shared a safeguarding concern in confidence (unless that individual has consented or it is reasonable to dispense with consent).

2. Mandatory Dual-Vetting Protocol & Statutory Timelines

A Designated Safeguarding Lead (DSL) must never release a child protection file in isolation. Upon receipt of a formal SAR, **the statutory timeframe of one calendar month begins immediately and cannot be paused or suspended.** The DSL must immediately initiate the following dual-vetting process:

- **Log with the SRAT Data Protection Officer (DPO):** Contact the DPO immediately to register the request, establish the statutory deadline, and determine if the complexity of the redactions justifies a formal two-month extension under UK GDPR rules.
- **Consult Multi-Agency Partners:** Promptly consult the child's allocated Social Worker (for active Child Protection, Child in Need, or Looked After Children cases) or the Local Authority Children's Services Information Governance Officer. This consultation must be used to identify if disclosure would trigger a serious harm exemption or disrupt an active police/social care intervention, **but it does not halt the statutory completion clock.**

3. Practical Redaction Checklist for DSLs

Before any document, chronology, or digital record (e.g., CPOMS printout) is exposed to an applicant, the DSL must conduct a rigorous, line-by-line redaction review using the following criteria:

- **Remove Third-Party Identifiers:** Black out names, phone numbers, and addresses of neighbours, community members, or anonymous callers who reported concerns.
- **Protect Peer Data:** Permanently erase any references to other pupils, including peer-on-peer abuse configurations, names of friends, or co-involved children.
- **Apply the Serious Harm Test to Opinions:** Do not redact professional safeguarding opinions or entries simply because they contain sensitive speculation; opinions must be disclosed **unless** the DPO and DSL determine that disclosure is likely to cause serious physical or mental harm to an individual.
- **Verify Digital Metadata:** Ensure that electronic exports do not accidentally leak hidden metadata, system notes, or the names of staff members who are protected under specific risk assessments.

All redactions must be made using permanent digital redaction software or irreversible black ink on physical copies before scanning. The use of standard digital highlighters or erasable digital overlays is **strictly prohibited**.

Supporting Documents

http://irms.org.uk/page/SchoolsToolkit

https://www.farrer.co.uk/News/Briefings/CPU-Update---High-Court-Rules-on-Retention-Period-for-Child-Protection-Information/

http://www.proceduresonline.com/barnet/fs/t_retention_records.html

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2