

Pupil Records Policy

Approved By	Director of Operations	Date:	09/02/2026
Author	Director of Safeguarding and Attendance	Date:	01/11/2025
Board Ratification	N/A	Date:	N/A
Joint Negotiating Council (JNC) consultation (where applicable)	N/A		
Last reviewed on:	09/02/2026		
Next review due by:	30/01/2027		

1. Statement of Intent

This policy sets out how the Respect Collaboration Trust creates, manages, stores, transfers and retains student records across all schools. It ensures statutory compliance (Data Protection Act 2018 and UK GDPR), supports safeguarding responsibilities under Keeping Children Safe in Education (KCSIE), and aligns with the Department for Education (DfE) Retention Schedule (2025). The Trust will maintain records that are accurate, necessary, secure, and retained only for as long as required.

2. Legal Framework

- Data Protection Act 2018 and UK GDPR
- Department for Education: Data protection in schools – Record keeping and management (updated Oct 2025)
- Department for Education: Retention Schedule (Dec 2025)
- Keeping Children Safe in Education (2025)– transfer and handling of safeguarding records
- Care Planning, Placement and Case Review (England) Regulations 2010 – retention of Looked After Children records
- NSPCC guidance on child protection records retention and storage

3. Principles

The Respect Collaboration Trust ensures that all student records are handled lawfully, fairly and transparently in accordance with the Data Protection Act 2018, UK GDPR and national safeguarding guidance. Information is collected only for clear educational, pastoral, safeguarding or statutory purposes, and staff are responsible for ensuring that records are accurate, relevant and kept to the minimum necessary.

All records are stored securely, with access restricted to those who need the information to fulfil their role. Safeguarding files are managed separately with enhanced security, and the welfare of the child remains the priority in all decisions about record-keeping and information sharing.

The Trust follows statutory retention requirements, including those relating to Child Protection, Children in Need, Looked After Children and records concerning sexual abuse. Where a child has ever been subject to one of these safeguarding categories, the highest relevant retention period will apply.

Records are transferred securely when a pupil moves setting, with safeguarding files sent directly between DSLs and receipt confirmed. Subject Access Requests and external agency requests are managed in line with the Data Protection Act 2018, and original files are never released.

Records are securely destroyed at the end of their retention period unless a legal hold or ongoing investigation requires continued preservation. The Trust maintains

accountability through clear processes for creating, storing, transferring and disposing of all student information.

4. Record Creation

On admission, a pupil file—both paper and electronic—is created as part of the induction process. Any safeguarding documentation received at this stage is immediately passed to the Designated Safeguarding Lead (DSL) for secure storage. Once an electronic file has been established, no further additions are made to the legacy paper file; instead, all new documents are scanned and uploaded to the electronic record to ensure consistency, security and effective information management.

5. Storing Information

Paper files are stored securely in locked, non-portable, fire-resistant cabinets to ensure their protection and confidentiality. Electronic records are maintained within secure systems that use role-based access controls and robust backup procedures to safeguard information. Access to all records is strictly limited to staff who require the information to fulfil their professional responsibilities, ensuring that pupil data is handled safely and appropriately at all times.

No additions will be made to the paper file once a student is admitted to School. All information received will be scanned and uploaded to the electronic file. No separate data, information, or documentation shall be retained by any site.

6. Transfer of files

When a pupil moves to another setting, their pupil record is transferred securely and without delay to ensure continuity of support and information. The safeguarding file is always sent separately directly to the Designated Safeguarding Lead (DSL) at the new setting and obtains confirmation that it has been received. Where a pupil leaves at 16+ to attend a college or sixth-form provider, the main pupil record is retained by the Trust and may be passed to the local authority archive where this is required or appropriate.

7. Retention Schedule

There are clear file retention dates that must be adhered to throughout this process they are Department for Education, Record Retention Schedule, December 2025

Record Type	Retention Period	Action After Retention
General pupil record	Until age 25 (best practice)	Review/Destroy
Child Protection (non-sexual abuse)	Until age 25 or 10 years after case received (whichever is longer)	Review
Child Sexual Abuse (CSA) records	Minimum 75 years from DOB (subject to review)	Retain; do not destroy without legal review

Children in Need (CIN)	Until age 25 or 10 years after case received (whichever is longer)	Review
Looked After Children (LAC)	Until 75th anniversary of DOB; if death before 18 → 15 years from date of death	Destroy
SEND/EHCP	Follow pupil record (until age 25)	Review/Destroy
Attendance data/registers	3 years after end of academic year	Destroy
Admissions records	1 year after academic year of admission	Destroy
Asylum seekers (non-LAC)	6 years from end of involvement	Destroy
Serious Incident Notifications	2 years from date created	Review

8. Electronic Archiving and back ups

Electronic files are archived at leaving and retained for the duration of applicable retention periods. Systems are backed up; immutable backups may extend data presence beyond deletion for cyber/disaster recovery.

It is not uncommon for the school to receive a request for a copy file or chronology after a child has left school, it is therefore essential that a process is followed that allows access to this information and access to files by authorised bodies

9. External Storage:

At the end of year 11/12. The paper school file for each student will be moved to external secure storage for long term archiving.

10. Monitoring and Review

This policy will be reviewed annually, and files will be destroyed as per legal expectations.

11. GDPR

Data will be processed to be in line with our requirements and protections set out in the UK General Data Protection Regulation, Data Protection Act as amended by the Data (Use and Access) Act 2025.