Snowflake School

‘Improving the quality of family life’

Records Management Policy

Contents

1. Statement of Intent

Snowflake School is committed to maintaining accurate, secure, and lawful records that support the safety, wellbeing, education, and life opportunities of its pupils. As an independent special school for pupils with autism, we recognise that records management is not solely a compliance activity, but a key part of safeguarding, effective SEND provision, and high-quality leadership.

This policy sets out how records are created, stored, accessed, retained, reviewed, and disposed of in a way that:

- Complies with all relevant legislation and statutory guidance
- Protects personal and sensitive data
- Reflects autism-aware and trauma-informed practice
- Supports inspection requirements (OFSTED and ISI)
- Enables staff to work confidently and consistently

2. Legal and Regulatory Framework

The school processes personal data under the lawful basis of legal obligation, public task, vital interests, and explicit consent where required, including special category data under Article 9.

This policy has due regard to, and is implemented in accordance with, the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended)
- Data (Use and Access) Act 2025
- Education (Independent School Standards) Regulations

Guidance includes (but is not limited to):

- DfE: *Data Protection in Schools*
- DfE: *Data Protection Toolkit for Schools*
- DfE: *Record Keeping and Retention Information for Academies and Trusts*
- Information Records Management Society (IRMS): *Information Management Toolkit for Schools*
- Information Commissioner’s Office (ICO) guidance

This policy operates alongside:

- GDPR Data Protection Whole School Policy
- Safeguarding and Child Protection Policy
- SEND Policy
- Behaviour and Positive Support Policy
- Freedom of Information Policy
- Cyber Security Policy

3. Roles and Responsibilities

3.1 The Board of Trustees

The Trustees hold overall responsibility for records management and ensure this policy is implemented consistently by the school.

3.2 Head (including Executive Head / Head of School/SLG)

The Head is responsible for:

- Day-to-day implementation of this policy
- Ensuring staff understand their responsibilities
- Secure management of safeguarding and sensitive records
- Ensuring inspection readiness

3.3 Data Protection Officer (DPO)

The Trustees appoint a Data Protection Officer (DPO), Faryaneh Akhavan who is responsible for:

- Oversight of records management and compliance
- Annual review of this policy
- Advising on retention, disposal, and lawful processing
- Managing Subject Access Requests (SARs) and FOI requests
- Conducting information audits

3.4 Staff

All staff are responsible for:

- Creating accurate, factual, and respectful records
- Storing records securely

- Following retention and disposal requirements
- Seeking advice when unsure

Failure to comply may result in disciplinary action.

4. Autism-Aware and SEND-Specific Principles

4.1 Accessibility and Respect

Records relating to pupils with autism are managed in a way that respects dignity, individuality, and communication needs. Where appropriate:

- Information may be shared with pupils in accessible formats
- Language used in records is factual, respectful, and non-judgemental
- Records reflect underlying needs, triggers, and support strategies

4.2 Capacity and Best Interests

Where pupils are not able to make decisions about access to their personal data, decisions will be made in accordance with:

- The Mental Capacity Act 2005
- The pupil's best interests
- Advice from parents/carers and professionals

Capacity is recognised as decision-specific and may change over time.

5. Management of Pupil Records

5.1 Content of Pupil Records

Pupil records include personal details, educational progress, SEND information, safeguarding records, and relevant correspondence. Safeguarding records are stored separately in line with statutory guidance.

5.2 Safeguarding Records

- Stored separately from the main pupil file
- Access restricted to the Head, DSL, or authorised senior leaders
- Retained for statutory periods (up to 75 years where required)

5.3 Behaviour and Incident Records

Records relating to behaviour, distress, or incidents:

- Are written in a trauma-informed manner

- Are used to inform positive behaviour support and risk reduction
- Support safeguarding oversight and staff training

6. Retention of Records

The School follows retention periods aligned with IRMS and DfE guidance. Detailed retention schedules for:

- Pupil records (including SEND and safeguarding)
- Staff records and safer recruitment
- Governance records
- Health and safety records
- Financial and operational records

are set out within this policy and applied consistently.

Records subject to litigation, safeguarding investigations, or the Independent Inquiry into Child Sexual Abuse (IICSA) are never destroyed until lawfully permitted.

7. Storage and Security

Any actual or suspected data breach will be reported immediately to the Head and DPO and managed in line with ICO guidance, including notification to the ICO within 72 hours where required.

7.1 Paper Records

- Stored in locked cabinets or secure rooms
- Access restricted to authorised staff
- Never left unattended or in public view

7.2 Digital Records

- Stored on secure, encrypted systems
- Password-protected user accounts
- Regular backups and disaster recovery arrangements
- Digital access permissions are role-based and managed centrally.

Personal devices are not used for school data.

8. Access to Information

Access to records is role-based and limited to staff with a legitimate professional need, including the Head, Designated Safeguarding Lead (DSL), Class Teams, and designated administrative staff.

Access permissions reflect job roles and responsibilities and are reviewed regularly to ensure continued appropriateness.

Individuals have the right to know what data is held about them and how it is used.

- Subject Access Requests are handled within statutory timescales
- Requests are managed sensitively, particularly where safeguarding applies
- Information may be shared directly with pupils where appropriate

9. Staff Training and Awareness

All staff receive regular training on:

- Records management
- Data protection and confidentiality
- Safeguarding record keeping
- Autism-aware and trauma-informed practice

Training is refreshed at least annually.

10. Monitoring, Audit, and Quality Assurance

- Annual information audits are conducted by the DPO
- Leaders sample records to ensure consistency and quality
- Findings inform improvement and training

Records management is recognised as a key indicator of effective leadership and governance.

11. Disposal of Records

Records are disposed of securely once retention periods expire:

- Paper records are shredded
- Digital records are permanently deleted

Records are never destroyed where safeguarding or legal requirements apply.

12. School Closure or Structural Change

In the event of closure, merger, or change of ownership, records will be transferred or disposed of in line with DfE guidance and statutory requirements.

13. Review

This policy is reviewed annually or sooner if required by changes in legislation, guidance, or inspection expectations.

Appendix A – Records Retention Schedules

1. Pupil Records

Record type	Retention period	Legal / statutory basis
Main pupil file (education record)	Until pupil reaches **25 years of age**	IRMS / Limitation Act
SEN records (EHCPs, reviews, reports)	Until **25 years of age**	SEND Code of Practice
Individual education plans / support plans	Until **25 years of age**	IRMS / SEND
Behaviour records (including incident logs)	**25 years** from date of birth	Limitation Act / safeguarding
Risk assessments (pupil-specific)	**25 years** from date of birth	Safeguarding / H&S
Attendance records	**6 years** after end of academic year	Education regulations
Accident and injury records (non-safeguarding)	**25 years** from date of birth	Limitation Act
Safeguarding / child protection records	**75 years** from date of birth or indefinitely if required	KCSIE / IICSA
Looked After Child (LAC) records	**75 years**	Safeguarding
Correspondence with parents/carers (significant)	Until **25 years**	IRMS

2. Staff Records (including Safer Recruitment)

Record type	Retention period	Legal / statutory basis
Staff personnel file	**6 years** after employment ends	Limitation Act
Safer recruitment records	**6 years** after employment ends	Keeping Children Safe in Education
DBS certificate information (not the certificate itself)	**6 months**	DBS Code of Practice
Allegations against staff (substantiated)	Until **normal retirement age** or **10 years**, whichever is longer	KCSIE

Record type	Retention period	Legal / statutory basis
Allegations against staff (unsubstantiated / false)	**10 years**	KCSIE
Staff training records (safeguarding, SEND)	**6 years**	Inspection evidence
Disciplinary records	**6 years** after employment ends	Limitation Act
Staff accident records	**6 years**	RIDDOR

3. Governance and Leadership Records

Record type	Retention period	Legal / statutory basis
Trustee meeting minutes	**Permanent**	Governance best practice
Policies (superseded versions)	**6 years**	Inspection evidence
Complaints (formal, including outcomes)	**6 years**	Education regulations
Inspection reports	**Permanent**	Statutory record
Strategic plans	**6 years**	Governance

4. Health, Safety, and Premises

Record type	Retention period	Legal / statutory basis
Health & safety risk assessments	**6 years** after superseded	H&S legislation
Fire safety records	**6 years**	Fire Safety Order
Premises maintenance records	**6 years**	H&S
COSHH assessments	**5 years** after superseded	COSHH regulations

5. Financial and Operational Records

Record type	Retention period	Legal / statutory basis
Financial accounts	**6 years**	HMRC
Payroll records	**6 years**	HMRC
Contracts and agreements	**6 years** after end	Limitation Act

Record type	**Retention period**	**Legal / statutory basis**
Procurement records	**6 years**	Audit requirements

6. Special Circumstances

Circumstance	**Retention rule**
Ongoing safeguarding concern	**Do not destroy**
Legal proceedings	Retain until case concluded + advised period
IICSA relevance	**Do not destroy without legal advice**
Subject Access Request in progress	Disposal suspended until request completed

Disposal Method

- **Paper records:** cross-cut shredding or certified confidential waste
- **Digital records:** permanent deletion from systems and backups

Revision

Version Update	January 2026
Review due	January 2027
Reviewed By	Sumen Starr
Approved by Board of Trustees on	January 2026