



The Wilnecote School

Title: Data Retention Policy

Member of leadership team with lead responsibility for oversight and update of policy	Mr. M Stevenson
Approved at SLT	July 2026
Policy approval at Governing Body	July 2026
Policy review cycle	Bi-annually
Policy review date	July 2028

Data Retention Policy

The Wilnecote School

1. Policy Statement

The Wilnecote School is committed to managing personal data responsibly and lawfully. This policy sets out how long the school retains personal data, the rationale for those periods, and how data is securely disposed of once it is no longer required.

The school recognises its responsibility to ensure that personal data is:

- kept only for as long as is necessary,
- processed in line with its lawful purpose,
- disposed of securely when no longer required.

This policy is based on the principles of data minimisation and storage limitation under UK GDPR and reflects DfE expectations for schools.

2. Scope

This policy applies to all personal data held by The Wilnecote School in whatever format, including:

- pupil data,
- staff and governor data,
- safeguarding and SEND records,
- financial and administrative records,
- electronic and paper records,
- data held by third-party processors acting on behalf of the school.

It applies to all employees, governors, volunteers, and contractors.

3. Legal Framework

This policy complies with the requirements of:

- UK General Data Protection Regulation (UK GDPR),
- Data Use Act 2025,
- Data Protection Act 2018,

- Freedom of Information Act 2000,
- Education (Pupil Information) (England) Regulations 2005,
- Limitation Act 1980.

DfE guidance makes clear that schools must be able to evidence that data is not kept longer than necessary, supported by a retention schedule and annual review.

4. Retention Principles

The Wilnecote School adheres to the following principles:

- Personal data is retained only where there is a legal, statutory, or operational need.
- Retention periods are informed by DfE guidance and IRMS retention schedules.
- Where possible, data that is no longer needed for operational use will be deleted, anonymised, or depersonalised.
- Data subject to ongoing complaints, safeguarding concerns, audits, or legal claims will be retained until those matters are fully resolved.

DfE guidance confirms that retention decisions should be documented and reviewed annually.

5. Retention Schedule

The school maintains a Data Retention Schedule which sets out retention periods for different categories of records. This schedule is based on:

- DfE record-keeping guidance,
- IRMS Information Management Toolkit for Schools,
- statutory requirements where applicable.

Key Retention Periods (Summary)

- Pupil educational records (secondary): Retain until end of the academic year following the pupil's 25th birthday.
- Child protection files: Retain until the pupil's 25th birthday; records relating to child sexual abuse are retained until the end of the academic year following the pupils 75th birthday.
- SEND records / EHCPs: Normally, the end of the academic year following the pupils 31st birthday, unless legal hold applies.

- Staff personnel files: the end of the academic year following the 6 years after employment ends.
- Allegations against staff: Retained in line with statutory guidance (generally until normal retirement age or 10 years from conclusion).
- Governing body minutes (signed master copy): Permanent retention.

These periods reflect DfE and IRMS recommendations for schools.

6. Secure Storage and Access

All personal data is stored securely:

- electronic data is protected by access controls, encryption where appropriate, and secure systems,
- paper records are stored in locked cabinets with restricted access.

Access to data is limited to those who need it to carry out their role, in line with DfE expectations for school data management.

7. Disposal of Data

When data reaches the end of its retention period, it is disposed of securely:

- paper records are cross-cut shredded or disposed of via a secure confidential waste service,
- electronic records are permanently deleted from live systems and backups where feasible.

DfE guidance emphasises that confidential data remains confidential even when no longer required, and must be destroyed securely.

A record of destruction is maintained, including:

- type of record,
- date of destruction,
- method of disposal,
- authorising officer.

Please see a template of this document in the appendix, the record will be maintained by the Data Manager.

8. Roles and Responsibilities

- **Governing Body:** Overall responsibility for compliance with data protection law.
- **Headteacher:** Ensures this policy is implemented across the school.
- **Data Protection Officer (DPO):** Advises on compliance, reviews retention schedules, and supports audits.
- **All staff:** Responsible for managing records in line with this policy and the retention schedule.

DfE guidance makes clear that leadership and governance arrangements are central to compliance.

9. Review and Monitoring

The Wilnecote School will:

- carry out an annual audit of the personal data it holds,
- review retention periods regularly,
- update this policy where legislation or DfE guidance changes.

These will be completed by The School Business Manager and The Data Manager.

The policy will be reviewed at least every two years, or sooner if required. Annual review is recommended by the DfE as good practice.

10. Related Policies

This policy should be read alongside:

- Data Protection Policy,
- Privacy Notices (Pupils, Parents, Staff),
- Safeguarding and Child Protection Policy,
- Information Security Policy

Retention Schedule:

1. Pupil Records

Record Type	Description / Examples	Retention Period (all will be at the end of the academic year following)	Retention Trigger	End of Retention Action	Authority
Pupil Educational Record (Secondary)	Core pupil file including reports, attendance, assessments, parental correspondence	Until pupil's 25th birthday	Date of birth	Secure disposal	Education (Pupil Information) (England) Regs 2005; Limitation Act 1980; DfE
Admission Forms – Unsuccessful	Applications, evidence, decision records	1 year from decision	Decision date	Secure disposal / anonymise stats	IRMS; DfE
Attendance Registers	Daily attendance records (electronic or paper)	7 years from last entry	Last date of entry	Secure disposal	IRMS; DfE
Examination Results	Internal and external exam records	Part of pupil educational record	DOB	Secure disposal	IRMS; DfE
Parental Consent Forms	Trips, photos, activities	Life of consent + 1 year	Consent expiry	Secure disposal	IRMS

2. Safeguarding and Child Protection

Record Type	Description	Retention Period (all will be at the end of the academic year following)	Trigger	End Action	Authority
Child Protection File	Safeguarding concerns, referrals, conference reports	Until 25th birthday	Date of birth	Secure disposal or transfer	DfE <i>Keeping Children Safe in Education</i>
Child Protection – Sexual Abuse	Any file relating to child sexual abuse	Until 75th birthday	Date of birth	Secure disposal	IICSA recommendation; DfE
Safeguarding Chronology	Chronological logs	Same as CP file	DOB	Secure disposal	IRMS; DfE
Transfer of CP Records	Transfer to new school	Immediate on transfer	School change	Secure handover	DfE

Child protection records must be kept separate from the main pupil file and transferred securely.

3. SEND Records

Record Type	Description	Retention Period	Trigger	End Action	Authority
SEND Support Records	SEN plans, reviews, correspondence	Until aged 25 plus 6 years	Birthday	Secure disposal	SEND Code of Practice; IRMS
EHCP Records	Education, Health & Care Plans	Until aged 25 plus 6 years	Birthday	Secure disposal	SEND Regulations 2014
Specialist Reports	Educational psychology, external agency reports	Linked to SEND file	Leaving date	Secure disposal	IRMS

4. Staff Records

Record Type	Description	Retention Period (all will be at the end of the academic year following)	Trigger	End Action	Authority
Personnel File	Contracts, appraisals, disciplinary	6 years after employment ends	End date	Secure disposal	IRMS; Limitation Act
Single Central Record (SCR)	Safer recruitment checks	Life of record + 6 years	Leaving date	Secure disposal	KCSIE; DfE
DBS Certificate Data	Certificate numbers only	Not retained once check complete	Verification	Secure disposal	DfE
Training Records	CPD, safeguarding training	Employment + 6 years	Leaving date	Secure disposal	IRMS

5. Allegations Against Staff

Record Type	Description	Retention Period (all will be at the end of the academic year following)	Trigger	End Action	Authority
Allegations (Substantiated)	Allegations meeting harm threshold	Until normal retirement age or 10 years	Conclusion date	Secure disposal	KCSIE
Allegations (Unsubstantiated/False)	Where not substantiated	Until 10 years	Conclusion date	Secure disposal	KCSIE
Low-Level Concerns	Low-level concern logs	Life of employment + 6 years	Leaving date	Secure disposal	KCSIE

6. Governance and Management

Record Type	Description	Retention Period	Trigger	End Action	Authority
Governing Body Minutes (Signed)	Master copy	Permanent	Date of meeting	Archive	IRMS
Committee Papers	Agendas and supporting papers	6 years	Date of meeting	Secure disposal	IRMS
Complaints Files	Formal complaints	6 years after resolution	Resolution date	Secure disposal	IRMS; Limitation Act
School Policies	Approved policies	Life of policy + 3 years	Superseded	Secure disposal	IRMS

7. Financial Records

Record Type	Description	Retention Period	Trigger	End Action	Authority
Accounting Records	Budgets, ledgers, invoices	7 years	Financial year end	Secure disposal	HMRC; IRMS
Payroll Records	Salaries, pensions	6 years	Leaving date	Secure disposal	HMRC
Free School Meal Eligibility	FSM evidence	6 years	Eligibility end	Secure disposal	IRMS

8. ICT and Communications

Record Type	Description	Retention Period	Trigger	End Action	Authority
Emails (Routine)	Day-to-day communications	As required, usually no longer than 2 years	Creation	Delete	DfE
Emails (Corporate/Significant)	Decisions, complaints, safeguarding	Retain under relevant category	Event date	Secure disposal	DfE
System Logs	Network and security logs	1–2 years	Creation	Delete	IRMS

9. Disposal and Audit Requirements

- Disposal must be secure and irreversible (cross-cut shredding or certified deletion).
- A record of destruction must be kept including date, category, and authorisation.
- Annual data audit required to confirm continued need for retained data.

Status

- Owner: SLT
- Applies to: All Wilnecote School staff, students and systems
- Reviewed annually

Data Destruction Record (completed as an example)

[illegible]