Data Retention Policy
Richard Cloudesley School

March 2026

1. Introduction

Richard Cloudesley School is committed to ensuring that all records containing personal data are managed, stored, retained, and disposed of in accordance with the UK GDPR, the Data Protection Act 2018, and relevant statutory guidance.

This policy outlines the required retention periods for key categories of school records and specifies how these records must be securely disposed of when no longer required.

2. Purpose

The purpose of this policy is to:

- Ensure compliance with legal and statutory requirements.
- Promote effective information governance.
- Protect the rights and privacy of pupils, staff, governors, and visitors.
- Reduce risks associated with the keeping of unnecessary data.

3. Scope

This policy applies to:

- All members of staff, including leadership, teaching, support staff, and governors.
- All records kept in paper or digital form.
- All school systems including email, MIS, safeguarding software, and visitor systems.

4. Responsibilities

- **Headteacher**: overall accountability for data retention and compliance.
- **Data Protection Officer (DPO)**: advisory role, oversight of compliance.
- **All Staff**: responsible for following this policy when handling school records.
- **Governors**: responsible for ensuring proper oversight.

5. Deletion of Information Without a Clear and Defensible Purpose

The school must only retain personal data where there is a **clear, specific, and lawful purpose** for holding it. In accordance with the principles of data minimisation and storage limitation under the UK GDPR, any information that no longer has a **defined, necessary, and defensible purpose** must be **securely deleted**.

Staff must ensure that:

- Personal data is **not kept "just in case"** or stored beyond the retention periods set out in this policy.
- Any documents, emails, digital files, notes, or duplicate records that do not serve an ongoing operational, legal, safeguarding, or educational purpose are **promptly removed**.
- Regular reviews of storage locations—including email folders, shared drives, MIS attachments, cloud storage, and portable media—are conducted to identify information that should be deleted.
- Disposal methods match the sensitivity of the information and comply with the secure disposal requirements in this policy.

Failure to delete unnecessary data increases risks around privacy, data breaches, and non-compliance; therefore, all staff share responsibility for ensuring records are retained **only for as long as they are needed**.

6. Use of Email and Electronic Messaging Systems

Email, instant messaging and other electronic communication tools (including Microsoft Teams, SMS, and similar platforms) are provided **solely for the transmission of information**, not for the long-term storage or archiving of records.

To support good information governance and compliance with UK GDPR:

- Email inboxes, sent folders, Teams chats, and other messaging platforms **must not be used as filing systems**.
- Staff must ensure that any information which needs to be kept for operational, safeguarding, or legal reasons is **saved into the appropriate secure system** (e.g., MIS, safeguarding software, shared drive, or approved cloud workspace).
- Once key information has been saved to its correct location, the original email or message **should be deleted** in line with the school's retention policy.
- Staff must avoid keeping long-term email threads, duplicate attachments, or personal data within messaging apps beyond the necessary communication purpose.
- Messaging platforms, such as MS Teams messages, should only contain **short-term, task-based exchanges**, and not any material that forms part of a formal record.

This approach ensures that staff follow the principles of data minimisation and storage limitation, helps reduce the risk of data breaches, and ensures that official records are stored in their correct, secure, and retrievable locations.

7. Record Retention Schedule

The school retains records according to statutory requirements and best practice guidance. Key categories are summarised below.

Data Type / Record Category	Retention Period	Disposal Method	Statutory/Best Practice Reference
Contracts (under seal)	Last payment/end of contract + 12 years	Secure Disposal	Limitation Act 1980
Contracts (under signature)	Last payment/end of contract + 6 years	Secure Disposal	Limitation Act 1980
Maintenance records (contractors)	Current year + 6 years (major works: while owned)	Secure Disposal	Best Practice
Title deeds	While property owned	Transfer to new owner	Best Practice
Admission records	Current year + 6 years	Secure Disposal	Best Practice
Pupil educational record (Primary)	While pupil at school	Transfer to next school/LA	Education (Pupil Information) Regulations 2005
Pupil educational record (Secondary)	Date of birth + 25 years	Secure Disposal	Limitation Act 1980
Attendance registers	6 years after entry	Secure Disposal	School Attendance Regulations
Policy documents (e.g. Complaints, SEN)	Life of policy or superseded + 3 years	Secure Disposal	Best Practice

Equality Information	Life of statement or superseded + 3 years	Secure Disposal	Best Practice
SATs papers	Until appeals/validation complete	Secure Disposal	Best Practice
SATs results	Pupil file until age 25	Secure Disposal	Best Practice
Exam results (school copy)	Current year + 6 years	Secure Disposal	Best Practice
Invoices, receipts, order books	Current financial year + 6 years	Secure Disposal	Best Practice
Payroll records	Current year + 6 years	Secure Disposal	Taxes Management Act 1970
School fund records	Current financial year + 6 years	Secure Disposal	Best Practice
Board minutes (Governing Body)	Date of meeting + 10 years	Offer to archives/Secure Disposal	Companies Act 2006
Governor personnel files	Appointment ceases + 6 years (25 if child allegations)	Secure Disposal	Best Practice
Register of Directors/Members	Resignation + 10 years	Secure Disposal	Companies Act 2006
Accident books (adults)	Last entry + 3 years (15 if negligence)	Secure Disposal	Social Security Regulations
Accident books (children)	Last entry + 3 years	Secure Disposal	Social Security Regulations
Fire risk assessments	Life of assessment + 3 years	Secure Disposal	Fire Service Order 2005
Asbestos monitoring	Last action + 40 years	Secure Disposal	Control of Asbestos Regulations
SEN files/IEPs	Date of birth + 25 years	Secure Disposal	Limitation Act 1980
Child protection records	Date of birth + 25 years	Secure Disposal	Keeping Children Safe in Education
Staff personal file	Termination + 6 years	Secure Disposal	Limitation Act 1980
Disciplinary warnings	Oral/Written: Date of warning + 6-12 months; Final: +18 months	Secure Disposal	ACAS Code
DBS checks	Date of check + 6 months	Secure Disposal	DBS Code of Practice
School brochures/prospectus	Current year + 3 years	Standard Disposal	Best Practice
Newsletters	Current year + 1 year	Secure Disposal	Best Practice
Visitor management systems	Academic year + 1 year	Secure Disposal	Best Practice
Emails	Retain according to subject/content (routine: current year + 1 year; safeguarding: DOB + 25 years)	Secure Disposal	IRMS Toolkit / DfE Data Protection Toolkit

Digital Communications (including MS Teams messages, text messages)	Retain for 3 months	Permanent Delete	Best Practice

8. Disposal Methods

All records must be disposed of securely in accordance with the retention schedule. Methods include:

- Shredding of paper files.
- Secure digital deletion, ensuring removal from backups where feasible.
- Transfer of records where required (e.g. pupil records to next school).

Disposal methods listed in the source schedule are followed — including **secure disposal**, **standard disposal**, or **transfer to new owner** where appropriate.

9. Data Breaches

Any accidental loss or unauthorised disclosure of personal data must be reported immediately to the headteacher and DPO. Serious breaches may need to be reported to the ICO within 72 hours.

10. Policy Review

This policy will be reviewed **annually** or sooner if legislation changes. The headteacher is responsible for ensuring the policy remains up to date.