Berkswich CE Primary School			
Reference Number S3b	Shared with Staff October 2026	Ratified by Governing Board October 2026	Review Date October 2027
Policy Title	Records Management Policy		

Contents:

Statement of intent
1. Legal framework
2. Responsibilities
3. Management of pupil records
4. Retention of pupil records and other pupil-related information
5. Retention of staff records
6. Retention of senior leadership and management records
7. Retention of health and safety records
8. Retention of financial records
9. Retention of other school records
10. Retention of emails
11. Identifying information
12. Storing and protecting information
13. Accessing information
14. Digital continuity statement
15. Information audit
16. Disposal of data
17. School closures and record keeping
18. Monitoring and review

Statement of intent

As a church school, Berkswich CE's vision is rooted in John 10:10: "I have come that they may have life, and have it to the full." We want every member of our community to flourish, and part of that is knowing that their personal information is treated with care, respect and trust. Our school values of faith, love and courage, and our Christian principles shape how we

handle the information entrusted to us. Berkswich CE Primary School is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible to the appropriate individuals. In line with the requirements of the UK GDPR, the school also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The school has created this policy to outline how records are stored, accessed, monitored, retained and disposed of to meet the school's statutory requirements. The retention schedules in this policy set out how long each type of record is kept and what happens to it at the end of that period; the reasons for holding data and the lawful basis for processing it are set out in the school's privacy notices and record of processing activities.

This document complies with the requirements set out in the UK GDPR and the Data Protection Act 2018, and reflects the DfE's guidance 'Data protection in schools'.

1. Legal framework

1.1. This policy has due regard to legislation including, but not limited to, the following:

- UK General Data Protection Regulation (UK GDPR)
- Education (Pupil Information) (England) Regulations 2005
- Freedom of Information Act 2000
- Limitation Act 1980
- School Attendance (Pupil Registration) (England) Regulations 2024
- Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025)

1.2. This policy also has due regard to the following guidance:

- Information and Records Management Society (IRMS) 'Information Management Toolkit for Schools' (current version)
- DfE (2026) 'Data protection in schools', including 'Record keeping and management'
- DfE (2026) 'Keeping children safe in education'
- HM Government (2026) 'Working together to safeguard children'

1.3. This policy will be implemented in accordance with the following school policies and procedures:

- Data Protection Policy
- Data Retention Settings in Arbor (Management of Information System used by the school)
- Freedom of Information Policy
- Data and E-Security Breach Prevention and Management Plan
- Information Asset Register
- Archived Files Log

2. Responsibilities

2.1. The whole school has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

2.2. The headteacher holds the overall responsibility for this policy and for ensuring it is implemented correctly.

2.3. The governing board is responsible for the school's compliance with the Data Protection Act 2018 and will receive the outcomes of the annual information audit.

2.4. The DPO is responsible for the management of records at the school.

2.5. The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the headteacher.

2.6. The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of safely and correctly.

2.7. All staff members are responsible for ensuring that any records they are responsible for (including emails) are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3. Management of pupil records

3.1. Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievements.

3.2. The following information is stored on the front of a pupil record, and will be easily accessible:

- Forename, surname, and date of birth

3.3. The following information is stored inside the pupils folder, which is kept in their classroom and will be easily accessible:

- Any preferred names
- Emergency contact details and the name of the pupil's doctor
- Any allergies or other medical conditions that are important to be aware of

- Historic medical appointment letters
- Summer and autumn report
- Names of people with parental responsibility, including their home address(es) and telephone number(s)
- Any other agency involvement, e.g. speech and language therapist
- Reference to any other linked files

3.4. The following information is stored in a pupil record within the MIS system (SIMS), and will be easily accessible:

- Admissions form
- Details of any SEND
- If the pupil has attended an early years setting, the record of transfer
- Data collection or data checking form
- Annual written reports to parents
- National curriculum and agreed syllabus record sheets
- Notes relating to major incidents and accidents involving the pupil
- Any information about an EHC plan and support offered in relation to the EHC plan
- Medical information relevant to the pupil's on-going education and behaviour
- Any notes indicating child protection disclosures and reports
- Any information relating to exclusions
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health
- Notes indicating that records of complaints made by parents or the pupil
- Examination results – pupil copy
- SATs results

3.5. The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in either the pupil's classroom, school office or medical room:

- Attendance registers and information
- Absence notes and correspondence

- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
- Accident forms – forms about major accidents will be recorded on the pupil record
- Consent to administer medication and administration records
- Copies of pupil birth certificates, passports etc.
- Correspondence with parents about minor issues, e.g. behaviour
- Pupil work
- Previous data collection forms that have been superseded

3.6. Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet in the SENDCo office. When dealt with, all information is stored digitally on a secure shared drive. Child protection files are kept separately from the main pupil record and, when a pupil moves school, the DSL will ensure the file is transferred securely and separately from the main pupil file, in line with KCSIE.

3.7. Hard copies of complaints made by parents or pupils are stored in a file in the headteacher's office.

3.8. Actual copies of accident and incident information are stored separately on the school's management information system and held in line with the retention periods outlined in this policy. An additional copy may be placed in the pupil's file in the event of a major accident or incident.

3.9. The school will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend.

3.10. The only exception to the above is if any records placed on the pupil's file have a shorter retention period and may need to be removed. In such cases, the DPO will remove these records. Data held on the MIS will be retained for two terms after the pupil leaves and then securely deleted.

3.11. Electronic records relating to a pupil's record will also be transferred to the pupils' next school. Section 12 of this policy outlines how electronic records will be transferred.

3.12. The school will not keep any copies of information stored within a pupil's record, unless there is ongoing legal action at the time during which the pupil leaves the school. The responsibility for these records will then transfer to the next school that the pupil attends.

3.13. The school will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The school it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the school.

4. Retention of pupil records and other pupil-related information

4.1. The table below outlines the school's retention periods for individual pupil records and the action that will be taken after the retention period, in line with any requirements.

4.2. Electronic copies of any information and files will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Personal identifiers, contacts and personal characteristics		
Images used for identification purposes	For the duration of the event/activity, or whilst the pupil remains at school, whichever is less, plus one month	Securely disposed of
Images used in displays	Whilst the pupil is at school	Securely disposed of
Images used for marketing purposes	In line with the consent period	Securely disposed of
Biometric data	For the duration of the event/activity, or whilst the pupil remains at school, whichever is less, plus one month	Securely disposed of
Postcodes, names and characteristics	Whilst the pupil is at school, plus five years	Securely disposed of
House number and road	For the duration of the event/activity, plus one month	Securely disposed of
Admissions		

Register of admissions	Every entry in the admissions register will be preserved for a period of six years after the date on which the entry was made	Information is reviewed and the register may be kept permanently
Admissions (where the admission is successful)	Date of admission, plus one year	Securely disposed of
Admissions appeals (where the appeal is unsuccessful)	Resolution of the case, plus one year	Securely disposed of
Proof of address (supplied as part of the admissions process)	Current academic year, plus one year	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Information added to the pupil file	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was not successful)	Retained until the appeals process is complete	Securely disposed of
All records relating to the creation and implementation of the Admissions Policy	Life of the policy, plus three years and then review	Securely disposed of
Pupils' educational records		
Pupils' educational records	Whilst the pupil remains at the school; data on the MIS is retained for two terms after the pupil leaves	Transferred to the next school – if the pupil moves to an independent school, home education or outside of the UK, the file will be kept by the LA and retained for the statutory period
Public test results	Added to the pupil's record and transferred to next school	All uncollected certificates returned to the examination board
Internal test results	Added to the pupil's record and transferred to next school	Reviewed and securely disposed of if no longer needed

Behaviour records	Added to the pupil's record and transferred to the next school Copies are held whilst the pupil is at school, plus one year	Securely disposed of
Exclusion records	Added to the pupil's record and transferred to the next school Copies are held whilst the pupil is at school, plus one year	Securely disposed of
Child protection information held on a pupil's record	Stored as a separate file or in a sealed envelope within the pupil's record, and retained as below	Transferred to the next school separately from the main pupil file
Child protection records held in a separate file	Until the pupil's 25th birthday; where the records relate to child sexual abuse, until the pupil's 75th birthday	Transferred to the next school separately from the main pupil file, or securely disposed of – shredded
Curriculum returns	Current academic year, plus three years	Review and allocate a further retention period or securely dispose of
Schemes of work	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
Timetable	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
Class record books	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
Mark books	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
Record of homework set	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of

Pupils' work	Returned to pupil at the end of current academic year If this is not possible, hold for the current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
Education, training or employment destinations data	Whilst the pupil is at the school, plus at least three years or from the end of KS4, whichever is earliest	Securely disposed of
Attendance		
Attendance registers	Every entry is retained for a period of six years after the date on which the entry was made	Securely disposed of
Correspondence relating to any absence (authorised or unauthorised)	Current academic year, plus two years	Securely disposed of
Medical information and administration		
Permission slips	For the duration of the period that medication is given, plus one month	Securely disposed of
Medical conditions – ongoing management	Added to the pupil's record and transferred to the next school Copies held whilst the pupil is at school, plus one year	Securely disposed of
Medical incidents that have a behavioural or safeguarding influence	Added to the pupil's record and transferred to the next school Copies held whilst the pupil is at school, plus 25 years	Securely disposed of
SEND		

SEND files, reviews and EHC plans, including advice and information provided to parents regarding educational needs and accessibility strategy	The pupil's date of birth, plus 31 years	Securely disposed of
Curriculum management		
SATs results	25 years after the pupil's date of birth (as stated on the pupil's record) A composite of the whole year's results may be held for the current year plus six years, for comparative purposes	Securely disposed of
Examination papers	Until the appeals/validation process has been completed	Securely disposed of
Published Admission Number (PAN) reports	Current academic year, plus six years	Securely disposed of
Valued added and contextual data	Current academic year, plus six years	Securely disposed of
Self-evaluation forms (internal moderation)	Current academic year, plus one year	Securely disposed of
Self-evaluation forms (external moderation)	Retained until superseded	Securely disposed of
Pupils' work	Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year	Securely disposed of
Extra-curricular activities		
Field file – information taken on school trips	Until the conclusion of the trip, plus one month	Securely disposed of

	Where a minor incident occurs, field files are added to the core system as appropriate	
Trip packs – information taken on school trips	Until the end of the visit Where a minor incident occurs, files are added to the core system as appropriate	Shredded upon return to school
Financial information relating to school trips	Whilst the pupil remains at school, plus one year	Securely disposed of
Parental consent forms for school trips where no major incident occurred	Until the conclusion of the trip, unless a school risk assessment decides the forms are likely to be required for any reason, in which case they should be retained for 22 years after the pupil's date of birth	Securely disposed of – shredded
Parental consent forms for school trips where a major incident occurred	25 years after the pupil's date of birth on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)	Securely disposed of – shredded
Educational visitors in school – sharing of personal information	Until the conclusion of the visit, plus one month	Securely disposed of
Records of educational visits (planning, risk assessments and approvals)	Date of the visit, plus 10 years – incident records and permission slips relating to an incident are added to the pupil's record	Securely disposed of
Family liaison officers and home-school liaison assistants		
Day books	Current academic year, plus two years	Reviewed and securely destroyed if no longer required
Reports for outside agencies	Duration of the pupil's time at school	Securely disposed of

Referral forms	Whilst the referral is current	Securely disposed of
Contact data sheets	Current academic year	Reviewed and securely destroyed if no longer active
Contact database entries	Current academic year	Reviewed and securely destroyed if no longer required
Group registers	Current academic year, plus two years	Securely disposed of
Catering and free school meal management		
Meal administration	Whilst the pupil is at school, plus one year	Securely disposed of
Meal eligibility	Whilst the pupil is at school, plus five years	Securely disposed of
School meal registers	Current year plus three years	Securely disposed of
Free school meal registers (where used as a basis for funding)	Current year plus six years	Securely disposed of
School meals summary sheets	Current year plus three years	Securely disposed of

5. Retention of staff records

5.1. The table below outlines the school's retention period for staff records and the action that will be taken after the retention period, in line with any requirements.

5.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Operational		
Staff members' personnel file	Termination of employment, plus six years, unless the file is relevant to an ongoing or anticipated legal case or investigation, in which case	Securely disposed of

	it will be retained until that has concluded	
Annual appraisal and assessment records	Current academic year, plus six years	Securely disposed of
Sickness absence monitoring (where sickness pay is not paid)	Current academic year, plus three years	Securely disposed of
Sickness absence monitoring (where sickness pay is paid)	Current academic year, plus six years	Securely disposed of
Staff training (where training leads to CPD)	Length of time required by the CPD professional body	Securely disposed of
Staff training (except where the training relates to dealing with pupils, e.g. first aid or health and safety)	Retained in the personnel file	Securely disposed of
Staff training (where the training relates to pupils, e.g. safeguarding or other pupil-related training)	Date of the training, plus 40 years	Securely disposed of
Recruitment		
Records relating to the appointment of a new headteacher (unsuccessful attempts)	Date of appointment, plus six months.	Securely disposed of
Records relating to the appointment of a new headteacher (successful appointments)	Added to personnel file and retained until the end of appointment, plus six years, except in cases of negligence or claims of child abuse, then records are retained for at least 15 years	Securely disposed of
Records relating to the appointment of new members of staff or governors (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of
Pre-employment vetting information (successful candidates)	For the duration of the employee's employment, plus six years	Securely disposed of
Copies of DBS certificates	Up to six months from recruitment	Securely disposed of

Proof of identify as part of the enhanced DBS check	If it is necessary to keep a copy, it will be placed in the staff member's personnel file	Securely disposed of
Evidence of right to work in the UK	Added to staff personnel file or, if kept separately, termination of employment, plus no longer than two years	Securely disposed of
Disciplinary and grievance procedures		
Child protection allegations, including where the allegation is unproven	Added to staff personnel file and retained until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer. Malicious allegations are removed from personnel files. Substantiated allegations are kept on the personnel file and a copy is provided to the person concerned.	Reviewed and securely disposed of – shredded
Oral warnings	Date of warning, plus six months	Securely disposed of – if placed on staff personnel file, removed from file
Written warning – level 1	Date of warning, plus six months	Securely disposed of – if placed on staff personnel file, removed from file
Written warning – level 2	Date of warning, plus 12 months	Securely disposed of – if placed on staff personnel file, removed from file
Final warning	Date of warning, plus 18 months	Securely disposed of – if placed on staff personnel file, removed from file
Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related, then it is disposed of as above.	Securely disposed of

6. Retention of senior leadership and management records

6.1. The table below outlines the school's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements.

6.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Governing board		
Agendas for governing board meetings	One copy alongside the original set of minutes – all others disposed of without retention	Local archives consulted before secure disposal
Original, signed copies of the minutes of governing board meetings	Permanent – all other copies disposed of without retention	Shredded if they contain any sensitive or personal information, but the local archives will be consulted first
Reports presented to the governing board that are referred to in the minutes	Permanent – all others disposed of without retention	Local archives consulted and then securely disposed of
Meeting papers relating to the annual parents' meeting	Date of meeting, plus a minimum of six years	Securely disposed of
Instruments of government	Permanent	Local archives consulted and then securely disposed of
Action plans created and administered by the governing board	Until superseded or whilst relevant	Securely disposed of
Policy documents created and administered by the governing board	Until superseded or whilst relevant	Securely disposed of
Records relating to complaints dealt with by the governing board or headteacher	Current academic year, plus six years If negligence is involved, records are retained for the current academic year, plus 15 years	Reviewed for further retention in case of contentious disputes, then securely disposed of

	If child protection or safeguarding issues are involved, the records are retained for the current academic year, plus 40 years	
Annual reports required by the DfE	Date of report, plus 10 years	Securely disposed of
Proposals concerning changing the status of the school	Date proposal accepted or declined, plus three years	Securely disposed of
Records relating to the appointment of co-opted governors	Date of election, plus six months	Securely disposed of
Records relating to the election of the chair of the governing board and the vice chair	Destroyed after the decision has been recorded in the minutes	Securely disposed of
Scheme of delegation and terms of reference for committees	Until superseded or whilst relevant	Reviewed and offered to the local archives if appropriate
Meeting schedule	Current academic year	Standard disposal
Register of attendance at full governing board meetings	Date of last meeting in the book, plus six years	Securely disposed of
Records relating to governor monitoring visits	Date of the visit, plus three years	Securely disposed of
Correspondence sent and received by the governing board or headteacher	Current academic year, plus three years	Securely disposed of
Records relating to the appointment of the clerk to the governing board	Date on which the clerk's appointment ends, plus six years	Securely disposed of
Records relating to the terms of office of serving governors, including evidence of appointment	Date on which the governor's appointment ends, plus six years	Securely disposed of
Records relating to governor declaration against disqualification criteria	Date on which the governor's appointment ends, plus six years	Securely disposed of
Register of business interests	Date the governor's appointment ends, plus six years	Securely disposed of

Governor code of conduct	Dynamic document – kept permanently	Securely disposed of
Records relating to the training required and received by governors	Date the governor steps down, plus six years	Securely disposed of
Records relating to the induction programme for new governors	Date on which the governor's appointment ends, plus six years	Securely disposed of
Records relating to DBS checks carried out on the clerk and members of the governing board	Date of the DBS check, plus six months	Securely disposed of
Governor personnel Information - GIAS	Date on which the governor's appointment ends, plus six years	Securely disposed of
Headteacher and SLT		
Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Reviewed annually and securely disposed of if not needed
Reports created by the headteacher or SLT	Date of the report, plus a minimum of three years	Reviewed annually and securely disposed of if not needed
Records created by the headteacher, deputy headteacher, heads of year and other members of staff with administrative responsibilities	Current academic year, plus six years	Reviewed annually and securely disposed of if not needed
Correspondence created by the headteacher, deputy headteacher, heads of year and other members of staff with administrative responsibilities	Date of correspondence, plus three years	Securely disposed of
Professional development plan	Held on the individual's personnel record. If not, then it is retained for the duration of the plan, plus six years	Securely disposed of
SDP	Duration of the plan, plus three years	Securely disposed of

7. Retention of health and safety records

7.1. The table below outlines the school's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements.

7.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Health and safety		
Health and safety policy statements	Duration of policy, plus three years	Securely disposed of
Health and safety risk assessments	Duration of risk assessment, plus three years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred	Securely disposed of
Accessibility plans	Life of the plan, plus six years	Securely disposed of
Records relating to any reportable death, injury, disease or dangerous occurrence under RIDDOR	Date of incident, plus three years provided that all records relating to the incident are held on the personnel file	Securely disposed of
Accident reporting – adults	Three years after the last entry in the accident reporting book	Securely disposed of
Accident reporting – pupils	Three years after the date of the accident – a copy is also added to the pupil's record	Securely disposed of
Records kept under the Control of Substances Hazardous to Health Regulations	Date of incident, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Securely disposed of
Health surveillance records for staff	40 years	Securely disposed of

Fire precautions log books	Current academic year, plus six years	Securely disposed of
Fire risk assessments	Life of the risk assessment, plus six years	Securely disposed of
Health and safety file to show current state of buildings, including all alterations (wiring, plumbing, building works etc.) to be passed on in the case of change of ownership	Permanent	Passed to new owner on sale or transfer of building

8. Retention of financial records

8.1. The table below outlines the school's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.

8.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Payroll and pensions		
Maternity pay records	Three years after the end of the tax year in which the maternity pay period ends	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	A minimum of six years from the end of the year in which the accounts were signed	Securely disposed of
Timesheets, clock cards and flexitime records	Current academic year, plus three years	Securely disposed of
Absence record	Current academic year, plus three years	Securely disposed of
Car mileage outputs	Current academic year, plus six years	Securely disposed of

Elements	Current academic year, plus two years	Securely disposed of
Income tax form P60	Current academic year, plus six years	Securely disposed of
Insurance	Current academic year, plus six years	Securely disposed of
National insurance – schedule of payments	Current academic year, plus six years	Securely disposed of
Overtime	Current academic year, plus three years	Securely disposed of
Part-time fee claims	Current academic year, plus six years	Securely disposed of
Payroll awards	Current academic year, plus six years	Securely disposed of
Payroll (gross/net weekly or monthly)	Current academic year, plus six years	Securely disposed of
Payroll reports	Current academic year, plus six years	Securely disposed of
Pension payroll	Current academic year, plus six years	Securely disposed of

Personal bank details	Until superseded, plus three years	Securely disposed of
Sickness records	Current academic year, plus three years	Securely disposed of
Staff returns	Current academic year, plus three years	Securely disposed of
Superannuation adjustments	Current academic year, plus six years	Securely disposed of
Superannuation reports	Current academic year, plus six years	Securely disposed of
Tax forms	Current academic year, plus six years	Securely disposed of
Risk management and insurance		
Employer's liability insurance certificate	Closure of the school, plus 40 years	Securely disposed of Passed to the LA if the school closes
Asset management		
Inventories of furniture and equipment	Current academic year, plus six years	Securely disposed of
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely disposed of
Accounts and statements including budget management		
Annual accounts	Current academic year, plus six years	Disposed of against common standards
Loans and grants managed by the school	Date of last payment, plus 12 years	Information is reviewed then securely disposed of
All records relating to the creation and management of budgets	Duration of the budget, plus three years	Securely disposed of

Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Securely disposed of
Records relating to the collection and banking of monies	Current financial year, plus six years	Securely disposed of
Records relating to the identification and collection of debt	Final payment, plus six years	Securely disposed of
Contract management		
All records relating to the management of contracts under signature	Last payment on the contract, plus six years	Securely disposed of
All records relating to the monitoring of contracts	Life of the contract, plus six or 12 years	Securely disposed of
School fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Securely disposed of
School meals		
FSM registers (where the register is used as a basis for funding)	Current academic year, plus six years	Securely disposed of
School meals registers	Current academic year, plus three years	Securely disposed of
School meals summary sheets	Current academic year, plus three years	Securely disposed of
Pupil finance		
Pupil premium fund records	Date the pupil leaves the school, plus six years	Securely disposed of

9. Retention of other school records

9.1. The table below outlines the school's retention periods for any other records held by the school, and the action that will be taken after the retention period, in line with any requirements.

9.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Property management		

Leases of property leased by or to the school	Expiry of lease, plus six years	Securely disposed of
Records relating to the letting of school premises	Current financial year, plus six years	Securely disposed of
Maintenance		
All records relating to the maintenance of the school carried out by contractors	For as long as the school owns the building and then passed onto any new owners if the building is leased or sold	Securely disposed of
All records relating to the maintenance of the school carried out by school employees	For as long as the school owns the building and then passed onto any new owners if the building is leased or sold	Securely disposed of
Operational administration		
General file series	Current academic year, plus five years	Reviewed and securely disposed of
Records relating to the creation and publication of the school brochure and/or prospectus	Current academic year, plus three years	If a copy is not preserved by the school, standard disposal
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current academic year, plus one year	Disposed of against common standards
Newsletters and other items with short operational use	Current academic year, plus one year	One copy archived, other copies standard disposal
Records relating to the creation and management of parent-teacher associations and/or old pupil associations	Current academic year, plus six years	Reviewed then securely disposed of
School privacy notice which is sent to parents	Until superseded, plus six years	Standard disposal
Consents relating to school activities	While pupil attends the school	Secure disposal

10. Retention of emails

10.1. Group email addresses will have an assigned member of staff who takes responsibility for managing the account and ensuring the correct disposal of all sent and received emails.

10.2. All staff members with an email account will be responsible for managing their inbox.

10.3. Emails can act as evidence of the school's activities, i.e. in business and fulfilling statutory duties, so all relevant emails (e.g. invoices) will be retained for at least 12 months.

10.4. Invoices received and sent in emails will be printed off and retained in accordance with section 8 of this policy.

10.5. The school's expectations of staff members in relation to their overall conduct when sending and receiving emails is addressed in the school's E-Safety Policy.

10.6. All emails will be automatically deleted after 12 months, unless stated otherwise.

10.7. Correspondence created by the SLT and other members of staff with administrative responsibilities will be retained for three years before being reviewed and, if necessary, securely disposed of.

10.8. Personal emails, i.e. emails that do not relate to work matters or are from family members, will be deleted as soon as they are no longer needed.

10.9. Staff members will review and delete any emails they no longer require at the end of every term.

10.10. Staff members will not, under any circumstances, create their own email archives, e.g. saving emails on to personal hard drives.

10.11. Staff members will be aware that the emails they send could be required to fulfil a SAR or freedom of information (FOI) request. Emails will be drafted carefully, and staff members will review the content before sending.

10.12. Individuals, including children, have the right to submit an SAR to gain access to their personal data to verify the lawfulness of the processing – this includes accessing emails.

10.13. All SARs will be handled in accordance with the school's Data Protection Policy.

10.14. FOI requests will be handled in accordance with the school's Freedom of Information Policy.

10.15. When handling a request for information, the DPO will speak to the requestor to clarify the scope of the request and whether emails will be required to fulfil the SAR or FOI request.

10.16. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

10.17. All requests will be responded to without delay and at the latest, within one month of receipt.

10.18. If a request is manifestly unfounded, excessive or repetitive, a reasonable fee may be charged, based on the administrative cost of providing the information.

10.19. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

10.20. Staff members will discuss any queries regarding email retention with the DPO.

11. Identifying information

11.1. Under the UK GDPR, the school applies the principles of data minimisation and data protection by design and default, and, as the data controller, ensures appropriate measures are in place to uphold them.

11.2. Wherever possible, the school uses pseudonymisation, also known as the 'blurring technique', to reduce the risk of identification.

11.3. Before older data is deleted entirely, and once identifiers are no longer required (e.g. after a pupil leaves), the school will depersonalise it, e.g. by replacing names with random IDs, dates of birth with year of birth, and postcodes with the locality or town.

11.4. Where data is required to be retained over time, e.g. attendance data, the school removes any personal data not required and keeps only the data needed – in this example, the statistics of attendance rather than personal information.

12. Storing and protecting information

12.1. The DPO will undertake a business impact assessment to identify which records are vital to school management and these records will be stored in the most secure manner.

12.2. The DPO will conduct a back-up of information on a termly basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.

12.3. Where possible, backed-up information will be stored off the school premises, using a central back-up cloud service operated by the LA. The DPO will ensure that the location of the cloud storage and the security offered is appropriate for the information and records stored on it.

12.4. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.

12.5. Any room or area where personal or sensitive data is stored will be locked when unattended.

12.6. Confidential paper records are not left unattended or in clear view when held in a location with general access.

12.7. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up off-site.

12.8. Where data is saved on removable storage or a portable device, the device is kept in a locked and fireproof filing cabinet, drawer or safe when not in use.

12.9. Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.

12.10. All electronic devices are password-protected to protect the information on the device in case of theft.

12.11. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

12.12. Staff and governors do not use their personal laptops or computers for school purposes.

12.13. All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

12.14. Emails containing sensitive or confidential information are password-protected or sent via a secure encrypted or data transfer system to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.

12.15. Personal information is never put in the subject line of an email.

12.16. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

12.17. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the UK GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

12.18. If digital documents are taken home, a device is used that is password protected and fully encrypted.

12.19. A record will be kept of any document that is taken off the school premises that logs the location of the document and when it is returned to the school site; this includes records that are remotely accessed digitally.

12.20. Before sharing data, staff always ensure that:

- There is a lawful basis for sharing it, which may be consent from the data subject.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

12.21. The school has data sharing agreements with all data processors and third parties with whom data is shared. These agreements are developed by the DPO and cover information about issues such as access controls and permissions.

12.22. All staff members implement a digital device locking policy and ensure that physical records are stored in a securely locked filing cabinet, drawer or safe with restricted access.

12.23. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

12.24. Staff are required to use their school login details to use photocopiers and printers.

12.25. The physical security of the school's buildings and storage systems, and access to them, is reviewed termly by the site technician in conjunction with the DPO. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the headteacher and extra measures to secure data storage will be put in place.

12.26. The DPO decides what restrictions are necessary to prevent information or records being downloaded, transferred or printed while the user is not on the school site.

12.27. The school takes its duties under the UK GDPR seriously and any unauthorised disclosures may result in disciplinary action.

12.28. The DPO is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

12.29. Any damage to or theft of data will be managed in accordance with the school's Data Protection Policy and Data and E-Security Breach Prevention and Management Plan.

13. Accessing information

13.1. We are transparent with data subjects, the information we hold and how it can be accessed.

13.2. All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, are entitled to:

- Know what information the school holds and processes about them or their child and why.
- Understand how to gain access to it.
- Understand how to provide and withdraw consent to information being held.
- Understand what the school is doing to comply with its obligations under the UK GDPR.

13.3. All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the UK GDPR, to access certain personal data being held about them or their child.

13.4. Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.

13.5. Pupils who are considered by the school to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

13.6. The school will adhere to the provisions outlined in the school's Data Protection Policy when responding to requests seeking access to personal information.

14. Digital continuity statement

14.1. Digital data that is retained for longer than six years will be identified by the DPO and named as part of the Safeguarding policy.

14.2. The data will be archived to dedicated files on the school's server, which are password-protected – this will be backed-up in accordance with section 12 of this policy.

14.3. Memory sticks are never used to store digital data, subject to procedures stated in the online safety and digital technology policy; these memory sticks are encrypted and password protected and signed in and out of school. Data is not kept on these devices for any longer than two years.

14.4. The IT Technician will review new and existing storage methods annually and, where appropriate add them to the online safety and digital technology policy.

14.5. The following information will be included within the digital continuity statement:

- A statement of the business purposes and statutory requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement
- A description of when the record needs to be captured into the approved file formats
- A description of the appropriate supported file formats for long-term preservation
- A description of the retention of all software specification information and licence information
- A description of how access to the information asset register is to be managed in accordance with the UK GDPR

15. Information audit

15.1. The school conducts information audits on an annual basis against all information held by the school, including pupil and staff data, to check that it is up to date, still needed and correctly managed in accordance with the UK GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases

- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information
- Knowledge
- Apps and portals

15.2. The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
- Questionnaires to key staff members to identify information and information flows, etc.
- A mixture of the above

15.3. The DPO is responsible for completing the information audit. The information audit will include the following:

- The school's data needs
- The information needed to meet those needs
- The format in which data is stored
- How long data needs to be kept for
- Vital records status and any protective marking
- A decision for each item on whether it will be kept, destroyed, depersonalised, converted from paper to electronic format, or retained for research or litigation
- Who is responsible for maintaining the original document

15.4. The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.

15.5. Once it has been confirmed that the information is accurate, the DPO will record all details on the school's Data Asset Register, which forms part of the school's record of processing activities.

15.6. An information asset owner is assigned to each asset or group of assets. They will be responsible for managing the asset appropriately, ensuring it meets the school's requirements, and for monitoring risks and opportunities.

15.7. The outcomes of the information audit will be shared with the headteacher for approval and reported to the governing board.

16. Disposal of data

16.1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.

16.2. Where disposal of information is outlined as secure disposal, paper records will be shredded using a cross-cut shredder, or by an approved external company that shreds records on site in the presence of a member of staff and provides a certificate of destruction. Hard disks and other storage media will be destroyed to particles no larger than 6mm. Records will never be placed in general waste or skips.

16.3. In line with the Freedom of Information Act 2000, all destruction will be approved by the headteacher, and the DPO will keep a record of each disposal, including a brief description of the records, the number of files and who authorised destruction.

16.4. Where the disposal action is indicated as reviewed before it is disposed, the DPO will review the information against its administrative value – if the information should be kept for administrative value, the DPO will keep a record of this.

16.5. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

16.6. Where information has been kept for administrative purposes, the DPO will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.

16.7. Where information must be kept permanently, this information is exempt from the normal review procedures. Records of historical value will be offered to the local record office in line with National Archives guidance.

16.8. Records and information that may be relevant to any ongoing or anticipated legal case, statutory inquiry or investigation will not be disposed of or destroyed until it has concluded.

17. School closures and record keeping

Sale or re-use of the site

17.1. If the school site is being sold or re-allocated to another use, the LA will take responsibility for the records from the date the school closes.

- Transfer to the local record office any records with historical value.

Managing records

17.2. The DPO will identify which records need to be destroyed or transferred to the relevant body – they will allocate personnel as necessary to sort through records.

17.3. The DPO will notify the other organisations as soon as possible so that necessary disposal, storage and transfer arrangements can be made. The school's IT provider will also be notified so that arrangements can be made to ensure the safe transfer or deletion of electronic records, including all back-up copies.

17.4. When sorting records, the DPO and their team will:

- Review all records held within the school as soon as notification of closure is received, including paper and electronic records.
- Use the retention periods outlined in this policy to categorise the records into those to be destroyed and those that need to be transferred
- Contact the relevant body to make arrangements for the safe and secure transfer of records.
- Sort, list and box the records in preparation for the transfer, ensuring records are stored in a safe environment whilst awaiting collection.
- Plan how the disposal of records will be undertaken.
- Sort expired records in readiness for confidential disposal, ensuring they are stored securely whilst awaiting disposal.

17.5. All forms of storage will be completely emptied before the building is vacated or before disposal.

17.6. Records awaiting transfer will be held in a secure area.

17.7. The identity of any third parties collecting or disposing of records will be checked and a collection receipt will be obtained.

17.8. Records will be disposed of in line with section 16 of this policy.

17.9. Electronic records will be either transferred to the new body or deleted.

17.10. All IT equipment will be decommissioned in accordance with the school's Online safety and digital technology policy and the appropriate records/certificates of decommission will be maintained.

17.11. No records will be left behind once the school building is vacated.

Monitoring and review

17.12. This policy and its retention schedules will be reviewed on an annual basis by the DPO in conjunction with the headteacher, and sooner if legislation or DfE guidance changes. Staff will be trained in the secure and timely disposal of records.

17.13. Any changes made to this policy will be communicated to all members of staff and the governing board.