

Riverstone Academy

Records Management Policy

Date of Review: September 2026

Date of Next Review: September 2027

Signed: K Bowe

Contents:

[Statement of intent](#)

1. [Legal framework](#)
 2. [Roles and responsibilities](#)
 3. [Management of pupil records](#)
 4. [Retention of pupil records and other pupil-related information](#)
 5. [Retention of staff records](#)
 6. [Retention of governance records](#)
 7. [Retention of senior leadership and management records](#)
 8. [Retention of health and safety records](#)
 9. [Retention of financial records](#)
 10. [Retention of other school records](#)
 11. [Retention of emails](#)
 12. [Identifying information](#)
 13. [Storing and protecting information](#)
 14. [Accessing information](#)
 15. [Record of processing activities](#)
 16. [Digital continuity statement](#)
 17. [Information audit](#)
 18. [Disposal of data](#)
 19. [School closures and record keeping](#)
 20. [Monitoring and review](#)
-

Statement of intent

Riverstone Academy 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.

This document complies with the requirements set out in the UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025.

1. Legal Framework

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

- UK General Data Protection Regulation (GDPR)
- Data (Use and Access) Act 2025
- Limitation Act 1980
- Data Protection Act 2018

This policy also has due regard to the following guidance:

- DfE (2026) 'Data protection in schools'
- DfE (2026) 'Data protection in schools: record keeping and management'
- Information and Records Management Society (IRMS) 'Information Management Toolkit for Schools' (current edition, where relevant)
- ICO guidance on documentation and records of processing activities
- ICO accountability and governance guidance

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

- Data Protection Policy

2. Roles and Responsibilities

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

The headteacher will hold the overall responsibility for this policy and for ensuring it is implemented correctly.

The Data Protection Lead/DPO (where a statutory DPO is appointed) will be responsible for:

- The management of records at the school.
- Promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the headteacher.
- Ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy and are disposed of safely and correctly.

All staff members will be 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.

Staff will be responsible for ensuring that when pupils use personal data for projects or coursework, they do so appropriately. This includes being compliant when storing personal data.

3. Management of pupil records

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 include all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievements.

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

- Forename, surname, and date of birth
- Unique pupil number
- Note of the date when the file was opened

The following information is stored inside the front cover of a pupil record, 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
- 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
- The following information is stored in a pupil record, 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
- Curriculum and assessment records
- 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
- Assessment and examination results, where applicable
- Statutory or standardised assessment results, where applicable

The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in the school office:

- 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

Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet in the school office – a note indicating this is marked on the pupil's file.

Hard copies of complaints made by parents or pupils are stored in a file in the headteacher's office – a note indicating this is marked on the pupil's file.

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 – a note indicating this is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.

The school will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend. The only exception 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 Data Protection Lead/DPO will remove these records.

Electronic records relating to a pupil's record will also be transferred to the pupils' next school.

Safeguarding records will be retained in accordance with current statutory safeguarding guidance and the school's retention schedule. Child protection files will normally be retained until the pupil's 25th birthday. Records relating to child sexual abuse will be retained until the pupil's 75th birthday, unless a longer period is required by law, litigation hold or specific guidance.

Core pupil records will be retained and transferred in accordance with the school's retention schedule, current DfE guidance and any applicable safeguarding or legal requirements.

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 tracked and secure delivery, 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

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.

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,	Securely disposed of

	whichever is less, plus one month	
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 three 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	Transferred to the next destination – if this is an independent school, home-schooling or outside of the UK, the file will be kept by the LA and retained for the statutory period The IRMS advises that information can be retained for a short period to allow for any queries or reports to be completed or where linked records in the school information management system have not yet reached the end of their retention period and deleting would cause problems
Pupils' educational records	Retained in accordance with the school's retention schedule and transferred securely to the next setting where appropriate; safeguarding records are retained separately as set out below	Reviewed and securely disposed of if no longer needed
Assessment and examination results (where applicable)	Added to the pupil's record and transferred to next school	All uncollected certificates returned to the examination board
Internal assessment 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	Securely disposed of

	Copies are held whilst the pupil is at school, plus one year	
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	Retained in line with the separate child protection file and current safeguarding guidance; normally until the pupil's 25th birthday, or 75th birthday where records relate to child sexual abuse	Securely disposed of – shredded
Child protection records held in a separate file	Normally until the pupil's 25th birthday; records relating to child sexual abuse retained until the pupil's 75th birthday, unless a longer period is required	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	Review at the end of each year and allocate a further retention period or securely dispose of

	If this is not possible, hold for the current academic year, plus one year	
Careers advice and subsequent agreed decisions	Whilst the pupil is at the school, plus three years	Securely disposed of
Transition and destination information (where applicable)	Retained only for as long as required for the pupil's transition, statutory reporting or other lawful purpose	Securely disposed of
Attendance		
Attendance registers	Every entry is retained for a period of three 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	Retained in accordance with the pupil record, safeguarding, limitation and other applicable legal/business requirements; no separate blanket SEND retention period is applied	Securely disposed of
Curriculum management		
Statutory or standardised assessment results (where applicable)	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
Admissions and capacity planning records	Current academic year, plus six years where required for business or regulatory purposes	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
Walking bus registers	Date of the register being taken plus six years	Securely disposed of If held electronically, all copies should be destroyed at the same time
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

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.

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, subject to any longer safeguarding, litigation or legal hold requirement	Securely disposed of
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)	Retained for the period required by the relevant safeguarding, regulatory, insurance or employment purpose and reviewed periodically rather than applying a blanket 40-year rule	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 Directors (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
DBS certificates	Up to six months	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	Until the individual reaches normal retirement age or for 10 years from the date of the allegation, whichever is longer, unless a longer period is required by safeguarding guidance, litigation hold or other legal requirement. Malicious or demonstrably false allegations will be handled in accordance with KCSIE 2026.	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 directors' records

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

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
--------------	------------------	--

Governance		
Agendas for Directors' meetings	One copy alongside the original set of minutes – all others disposed of without retention	secure disposal
Original, signed copies of the minutes of Directors meetings	Permanent – or at least for 10 years from the date of the meeting	Shredded if they contain any sensitive or personal information, but the local archives will be consulted first
Reports presented to the directors that are referred to in the minutes	Permanent – all others disposed of without retention	securely disposed of
Meeting papers relating to the annual parents' meeting	Date of meeting, plus a minimum of six years	Securely disposed of
Constitutional, ownership and governance documents	Permanent while legally relevant, with historic copies retained where necessary	securely disposed of
Trusts and endowments managed by the directors	Permanent	securely disposed of
Action plans created and administered by the directors	Until superseded or whilst relevant	Securely disposed of
Policy documents created and administered by the directors	Until superseded or whilst relevant	Securely disposed of
Records relating to complaints dealt with by the directors or headteacher	Date of resolution of complaint, plus six years If negligence is involved, records are retained for the current academic year, plus 15 years If child protection or safeguarding issues are involved, the records are retained for the current academic year, plus 40 years	Reviewed for further retention in case of contentious disputes, then securely disposed of

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 directors	Date of election, plus six months	Securely disposed of
Records relating to the election of the chair of the directors 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 securely retained or disposed of as appropriate
Meeting schedule	Current academic year	Standard disposal
Register of attendance at full director meetings	Date of last meeting in the book, plus six years	Securely disposed of
Records relating to director monitoring visits	Date of the visit, plus three years	Securely disposed of
Correspondence sent and received by the directors or headteacher	Current academic year, plus three years	Securely disposed of
Records relating to the appointment of the clerk to the directors	Date on which the clerk's appointment ends, plus six years	Securely disposed of
Records relating to the terms of office of serving Directors, including evidence of appointment	Date on which the Director's appointment ends, plus six years	Securely disposed of
Records relating to director declaration against disqualification criteria	Date on which the Director's appointment ends, plus six years	Securely disposed of
Register of business interests	Date the Director'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 directors	Date the Director steps down, plus six years	Securely disposed of

Records relating to the induction programme for new directors	Date on which the Director's appointment ends, plus six years	Securely disposed of
Records relating to DBS checks carried out on the clerk and members of the directors	Date of the DBS check, plus six months	Securely disposed of
Director personnel files	Date on which the Director's appointment ends, plus six years	Securely disposed of

7. Retention of senior leadership and management records

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.

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
Headteacher and SLT		
Log books of activity in the school maintained by the headteacher	Date of last entry, plus a minimum of six years	Reviewed and offered to the local archives if appropriate
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, other senior leaders 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, other senior leaders 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
-----	--	----------------------

8. Retention of health and safety records

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.

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
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	At least three years from the last entry, and longer where required because of the pupil’s age, a significant incident, safeguarding concern, claim or limitation period	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

Information relating to areas where employees and persons are likely to come into contact with radiation (maintenance records or controls, safety features and PPE)	Two years from the date on which the examination was made	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with radiation (dose assessment and recording)	Until the person to whom the record relates would have reached 75-years-old, but in any event for at least 30 years from when the record was made	Securely disposed of
Fire precautions log books	Current records plus sufficient historic records to demonstrate compliance; normally at least three years, subject to fire risk and insurance requirements	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
Significant use of force / restrictive intervention and seclusion records	Retained in accordance with current statutory guidance, safeguarding requirements, the pupil record and any applicable limitation period	Reviewed and securely disposed of when no longer required

9. Retention of financial records

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.

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	Current academic year, plus three years	Securely disposed of

Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely disposed of
Absence record	Current academic year, plus three years	Securely disposed of
Batches	Current academic year, plus six years	Securely disposed of
Bonus sheets	Current academic year, plus three years	Securely disposed of
Car allowance claims	Current academic year, plus three years	Securely disposed of
Car loans	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
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
Payslips (copies)	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 seal	Last payment on the contract, plus 12 years	Securely disposed of
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		
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		
Student grant applications	Current academic year, plus three years	Securely disposed of

10.Retention of other school records

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.

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		
Title deeds of properties belonging to the school	Permanent	Transferred to new owners if the building is leased or sold
Plans of property belonging to the school	For as long as the building belongs to the school	Transferred to new owners if the building is leased or sold

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
Records relating to routine premises maintenance coordinated by the school	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
Visitors' books and signing-in sheets	Last entry in the logbook, plus six years	Reviewed then securely disposed of
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 notices	Until superseded, plus six years	Standard disposal
Consents relating to school activities	While pupil attends the school	Secure disposal

11.Retention of emails

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

Emails can form part of the school's substantive business records. Emails will be retained according to their content and purpose. Where an email forms part of a safeguarding matter, complaint, contract, personnel matter, financial transaction, pupil record or other substantive record, it will be retained for the same period as the underlying record. Routine or transitory emails will be deleted when no longer required.

The school's expectations of staff members in relation to their overall conduct when sending and receiving emails is addressed in the school's Online Safety Policy. All emails will be automatically deleted after 12 months, unless stated otherwise.

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.

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

Staff members will not, under any circumstances, create their own email archives, e.g. saving emails on to personal hard drives. Staff members will be aware that the emails they send could be required to fulfil a subject access request (SAR) or other lawful information request. Emails will be drafted carefully, and staff members will review the content before sending.

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.

All subject access requests will be handled in accordance with the school's Data Protection Policy.

When handling a request for information, the Data Protection Lead/DPO will speak to the requestor to clarify the scope of the request and whether emails will be required to fulfil the SAR or other lawful request. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format. All requests will be responded to without delay and at the latest, within one month of receipt.

Where a request is manifestly unfounded or excessive, the school may charge a reasonable fee or refuse to act where permitted by data protection legislation. Any fee will reflect the administrative cost of complying with the request.

Where the school refuses to act on a request, the individual will be informed without undue delay of the reasons and of their right to complain to the Information Commissioner and seek a judicial remedy. The school will conduct reasonable and proportionate searches when responding to subject access requests.

Staff members will discuss any queries regarding email retention with the Data Protection Lead/DPO.

12. Identifying information

Under the UK GDPR, all individuals have the right to data minimisation and data protection by design and default – as the data controller, the school ensures appropriate measures are in place for individuals to exercise this right.

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

Once an individual has left the school, if identifiers such as names and dates of birth are no longer required, these are removed or less specific personal data is used, e.g. the month of birth rather than specific date – the data is blurred slightly.

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.

13. Storing and protecting information

The Data Protection Lead/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. The Data Protection Lead/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.

Backups will be stored securely using approved on-site and/or cloud services. The school will ensure that providers, storage locations, contractual safeguards, access controls and recovery arrangements are appropriate for the sensitivity of the information stored.

Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access. Any room or area where personal or sensitive data is stored will be locked when unattended. Confidential paper records are not left unattended or in clear view when held in a location with general access.

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

All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft. Staff and Directors do not use their personal laptops or computers for school purposes. All members of staff are provided with their own secure login and password, and staff use strong, unique passwords and multi-factor authentication where appropriate; passwords are changed when compromise is suspected or required by risk.

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. Personal information is never put in the subject line of an email. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

Where legacy transmission methods are exceptionally used, staff will verify the recipient and apply appropriate security before sending confidential information.

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.

Confidential records taken off site will not be left unattended unless secured in accordance with an approved risk-assessed arrangement. The school will maintain proportionate records of the removal and return of particularly sensitive physical records where necessary.

Before sharing personal data, staff will ensure that:

- An appropriate lawful basis has been identified; consent will only be relied upon where it is genuinely appropriate.
- Adequate security is in place to protect it.
- The sharing is necessary and proportionate and is consistent with applicable privacy information or another lawful transparency arrangement.

Safeguarding information may be shared without consent where this is necessary and lawful to protect a child or another person. Data protection legislation will not be treated as a barrier to appropriate safeguarding information sharing. The school will maintain appropriate contracts or data-sharing arrangements with processors and third parties where required.

A record is kept of what level of access each staff member has to data. This record details information including:

- What level of access each staff member has.
- Limits on how staff members access data.
- What actions staff members can perform.
- What level of access is changed or retained when a staff member changes role within the school.
- Who is able to authorise requests to change permissions and access.

All staff members implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information is stored in a securely locked filing cabinet, drawer or safe with restricted access.

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.

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

The physical security of the school's buildings and storage systems, and access to them, is reviewed termly. 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.

All systems that allow staff and pupils to remotely access information from the school's network whilst they are not physically at the school have strong security controls in place which are reviewed termly by the Data Protection Lead/DPO.

The Data Protection Lead/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.

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

The Data Protection Lead/DPO is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data. Any damage to or theft of data will be managed in accordance with the school's Data and Cyber-security Breach Prevention and Management Plan.

As a result of the UK's exit of the EU data controllers and processors follow the UK GDPR, and the Data Protection Act 2018, where:

- As UK data controllers, they collect, store or process the personal data of individuals residing in the UK.
- As non-UK data controllers, they offer goods or services to, or monitor the behaviour of, UK residents.

Where the school processes personal data in circumstances that are subject to another jurisdiction, including the EU GDPR, the school will identify and comply with the applicable legal requirements.

- Any such processing will be documented and appropriate safeguards applied.
- The school will seek specialist advice where cross-border processing creates additional legal obligations.

14. Accessing information

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

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.

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.

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. 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.

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

15. Record of processing activities

The school will maintain a record of processing activities, to capture all the important information about data processing activities.

The school will adopt the following procedure when developing and maintaining its record:

- Identify personal data assets, locating all the personal data the school has received
- Compile the personal data assets into a list
- Add extra information about the school's personal data assets in the list, developed to suit the school's individual needs

The school's record of processing activities will contain the following mandatory information as a minimum:

- Name and contact details of the school
- Name and contact details of the school's data protection officer
- Name and contact details of any joint controllers
- Purposes of carrying out personal data processing
- Categories of personal data which the school processes
- Categories of individuals whose personal data the school process
- Categories of organisations with which the school shares personal data
- Schedule for retaining each category of personal data
- General description of the school's technical and organisational security

More details about further information that the record of processing activities will be included via the following prompts:

- Source of personal data
- Category of personal data
- Whether the school is a data controller, data processor, a joint controller, or has a controller-processor contract in place
- Access and use
- Data retention and destruction
- Comments, rights, and subject access requests
- Security and personal data breaches
- Automated decision-making

16. Digital continuity statement

Digital data that is retained for longer than six years will be identified by the Data Protection Lead/DPO and named as part of a Digital Continuity Statement. 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.

Memory sticks are never used to store digital data, subject to a Digital Continuity Statement.

The external IT support provider or designated IT lead will review new and existing storage methods annually and, where appropriate, add them to the digital continuity statement.

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

17.Information audit

The school conducts information audits on an annual basis against all information held by the school to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the UK GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Microfilm or microfiche
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information
- Knowledge
- Apps and portals

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.

The Data Protection Lead/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
- Who is responsible for maintaining the original document

The Data Protection Lead/DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.

Once it has been confirmed that the information is accurate, the Data Protection Lead/DPO will record all details on the school's Data Asset Register.

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.

The information displayed on the Data Asset Register will be shared with the headteacher to gain their approval.

18. Disposal of data

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.

All records containing personal or sensitive information will be made either unreadable or unreconstructable.

Where disposal of information is outlined as secure disposal, this will be shredded or pulped. Electronic information will be scrubbed clean and, where possible, cut, archived or digitalised. The Data Protection Lead/DPO will keep a record of all files that have been destroyed.

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

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.

Where information has been kept for administrative purposes, the Data Protection Lead/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.

Where information must be kept permanently, this information is exempt from the normal review procedures.

Records subject to a legal hold, safeguarding retention requirement, complaint, claim, investigation or other preservation requirement will not be destroyed until the hold or requirement has ended and disposal has been authorised.

19. School closures and record keeping

If Riverstone Academy closes, merges, changes proprietor or transfers its undertaking, records will be reviewed and transferred, retained or securely disposed of in accordance with

current DfE requirements, safeguarding obligations, data protection law, contractual and limitation requirements, and any lawful directions that apply.

Safeguarding, pupil, staff, governance, premises, financial and other records will be mapped to an appropriate successor or retention arrangement. Records will not automatically be transferred to a local authority unless there is a lawful requirement or agreed receiving arrangement.

The Data Protection Lead/DPO will coordinate the closure or transfer plan, including secure inventories, transfer methods, destruction certificates, continuity of access to long-retention records, and arrangements for electronic systems, backups and cloud services.

Where the school merges with another school or is taken over by a successor proprietor, current records required for the continuing education, safeguarding, employment or operation of the school will be transferred securely to the successor where lawful and necessary.

Expired records will be securely destroyed in accordance with this policy. Records subject to safeguarding, legal hold, complaint, claim, investigation or other preservation requirements will not be destroyed until the relevant requirement has ended.

No records will be abandoned or left unsecured when premises are vacated. The school will verify the identity and authority of any third party collecting or receiving records and will retain appropriate evidence of transfer or destruction. [Record keeping and retention information for academies and academy trusts](#)

20. Monitoring and review

This policy and the detailed retention schedule will be reviewed at least annually by the Data Protection Lead/DPO in conjunction with the headteacher and Directors, and sooner where legislation, guidance, systems or the school's operating model changes.