Records Management Policy

Document Details	
Category:	Data Protection Policies
Approved By:	Audit and Risk Committee
Version:	3
Status:	Approved
Issue Date:	April 2021
Next Review Date:	Summer Term 2022
Signed:	

Ownership and Control

History

Version	Author	Dated	Status	Details
1	JEl/KHo	Mar 2018	Approved	Original SchoolBus Policy
2	JEl/KHo	May 2019	Approved	Annual review
3	JEL	Apr 2021	Approved	Annual review

Contents:

Statement of intent

The Sigma Trust is committed to maintaining the confidentiality of its information and ensuring that all records within the Trust are only accessible by the appropriate individuals. In line with the requirements of the Data Protection Act 1998, the Trust 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 Sigma Trust has created this policy to outline how records are stored, accessed, monitored and disposed of, and how long data is retained for, in order to meet the Trust's statutory requirements.

NB. For the purpose of this document the term Headteacher refers to Headteacher, Head of School and Executive Headteacher.

1. Legal framework

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

- General Data Protection Regulation (GDPR)
- Data Protection Act 1998
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended)

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

- Information Records Management Society (IRMS) (2019) 'Information Management Toolkit for Schools'
- DfE (2018) 'Data protection: a toolkit for schools'
- DfE (2018) 'Careers guidance and access for education and training providers'

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

- Data Protection Policy
- Freedom of Information Policy
- E-security Policy
- CCTV
- Disaster Recovery Plan

2. Responsibilities

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

2.2. The Sigma Trust, in conjunction with the headteacher, holds overall responsibility for this policy and for ensuring it is implemented correctly.

2.3. The school data lead, in conjunction with The Sigma Trust and the headteacher, are responsible for the management of records within their school.

2.4. The school data lead, in conjunction with The Sigma Trust and the headteacher, are responsible for promoting compliance with this policy, and reviewing the policy on an annual basis.

2.5. The school data lead, in conjunction with The Sigma Trust and the headteacher, are responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of correctly.

2.6. All staff members are responsible for ensuring that any records for which they are responsible 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 documents that are passed to each school that a pupil attends and include all personal information relating to them, as well as their progress.

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

- Forename, surname, gender and date of birth,
- Unique pupil number
- Note of the date when the file was opened (intake year)
- Note of the date when the file was closed, if appropriate

3.3. The following information is stored inside the front cover of a pupil record, and will be easily accessible:

- Ethnic origin, religion and first language (if not English)
- Any preferred names
- Position in their family, e.g. eldest sibling
- 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 parents and/or carers, including home addresses and telephone numbers
- Name of the school, admission number, the date of admission and the date of leaving
- Any other agency involvement, e.g. speech and language therapist

3.4. The following information is stored on a pupil record, and will be easily accessible:

- Admissions form
- Details of any special educational needs and disabilities (SEND)
- If the pupil has attended an early years setting, the record of transfer
- Fair processing notice – only the most recent notice will be included
- 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 SEN statement, and support offered in relation to the statement
- Any notes indicating child protection disclosures and reports are held
- 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 are held

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 the appropriate school office:

- Absence notes
- Parental consent forms for educational visits and trips, photographs and videos, etc.
- Correspondence with parents about minor issues, e.g. behaviour

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

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

3.8. Details of accident and incident information are stored on the school's management information system and actual copies are held in line with the statutory retention periods outlined in this policy – a note indicating this is marked on the pupil's file. An additional copy may be placed on the pupil's file in the event of a major accident or incident.

3.9. The school headteacher 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 any records placed on the pupil's file that have a shorter retention period and may need to be removed. In such cases, the data records clerk responsible for disposing of records will remove these records.

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

3.12. [Primary schools only] The Trust 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 Trust. The responsibility for these records will then transfer to the next Trust that the pupil attends.

3.13. If any pupil attends a Trust school until statutory school leaving age, the school will keep the pupil's records until the pupil reaches the age of 25 years, in accordance with the Limitation Act 1980 (as amended).

3.14. 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 will be 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 Trust'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 also 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 in schools	Whilst the pupil is at school	Securely disposed of
Images used for marketing purposes, or other	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
In-year secondary school admissions	Whilst the pupil remains at the school, 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		
Primary school Pupils' educational records	Whilst the pupil remains at the school	Transferred to the 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
Secondary school Pupils' educational records	25 years after the pupil's date of birth	Reviewed and securely disposed of if no longer needed
Public examination results	Added to the pupil's record and transferred to next school	All uncollected certificates returned to the examination board
Internal examination results	Added to the pupil's record and transferred to next school	Transferred to the next school
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	Stored in a sealed envelope for the same length of time as the pupil's record Records also subject to any instruction given by the Independent Inquiry into Child Sex Abuse (IICSA)	Securely disposed of – shredded
Child protection records held in a separate file	25 years after the pupil's date of birth Records also subject to any instruction given by the IICSA	Securely disposed of – shredded
Curriculum returns	Current academic year, plus three years	Securely disposed 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	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose 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	The pupil's date of birth, plus 31 years	Securely disposed of
An EHC plan maintained under section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Information and advice provided to parents regarding SEND	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold

Accessibility strategy	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Curriculum management		
SATs results	25 years after the pupil's date of birth (as stated on the pupil's record)	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
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 Where a minor incident occurs, field files are added to the core system as appropriate	Securely disposed of
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	Up to 22 years after the pupil's date of birth

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
Walking bus registers	Three years from the date of the register being taken	Securely disposed of
Educational visitors in school – sharing of personal information	Until the conclusion of the visit, plus one month	Securely disposed of
Family liaison officers and home-school liaison assistants		
Day books	Current academic year, plus two years	Reviewed, and 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 destroyed if no longer active
Contact database entries	Current academic year	Reviewed, and 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

5. Retention of staff records

5.1. The table below outlines the Trust's retention periods 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 member of staff is part of any case which falls under the terms of reference of the IICSA. If this is the case, the file will be retained until the IICSA enquiries are complete	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)	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

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
Disciplinary and grievance procedures		
Child protection allegations, including where the allegation is unproven	Added to staff personnel file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer If allegations are malicious, they are removed from personal files If allegations are found, they are kept on the personnel file and a copy is provided to the person concerned unless the member of staff is part of any case which falls under the terms of reference of the IICSA. If this is the case, the file is retained until IICSA enquiries are complete	Reviewed and securely disposed of – shredded
Oral warnings	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 1	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 2	Date of warning, plus 12 months	Securely disposed of – if placed on staff personal file, removed from file
Final warning	Date of warning, plus 18 months	Securely disposed of – if placed on staff personal file, removed from file
Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related and is disposed of as above	Securely disposed of

6. Retention of senior leadership and management records

6.1. The table below outlines the Trust'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
Board of Trustees, associated committees and Local Governance Committees *referred to below as trustee and LGC meetings*		
Agendas for trustee and LGC meetings	One copy alongside the original set of minutes – all others disposed of without retention	Securely disposed of
Original, signed copies of the minutes of governance meetings	Permanent – all other copies disposed of without retention	
Reports presented to the board that are referred to in the minutes of governance meetings	Permanent – all others disposed of without retention	Shredded if they contain any sensitive, personal information
Meeting papers relating to the AGM	Date of meeting, plus a minimum of six years	Securely disposed of or, if they refer to individual reports, retained with the signed, original copy of minutes
Instruments of government, including articles of association	Permanent	If unable to store, these will be provided to the county archives service
Trusts and endowments managed by the trustees	Permanent	Retained in the Trust whilst it remains open, then provided to the county archives service when the school closes
Action plans created and administered by the trustees	Until superseded or whilst relevant	Securely disposed of
Policy documents created and administered by the trustees and LGCs	Until superseded or whilst relevant	Securely disposed of
Records relating to complaints dealt with by the trustees and LGCs	Current academic year, plus six years	Reviewed for further retention in case of

	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	contentious disputes, then securely disposed of
Annual reports created under the requirements of The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	Date of report, plus 10 years	Securely disposed of
Proposals concerning changing the status of the Trust	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 trustees and LGCs 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 trustee and LGC meetings	Date of last meeting in the book, plus six years	Securely disposed of
Records relating to LGC monitoring visits	Date of the visit, plus three years	Securely disposed of
Academies or maintained schools converting to academy status only - All records relating to the conversion of the school to academy status	Permanent	Local archives are consulted before disposal
Correspondence sent and received by the trustees, LGCs and headteacher	Current academic year, plus three years	Securely disposed of
Records relating to the appointment of the clerk to the trust and LGC meetings	Date on which the clerk's appointment ends, plus six years	Securely disposed of
Records relating to the terms of office of serving trustees and	Date on which the trustee/LGC member's appointment ends, plus six years	Securely disposed of

LGC members, including evidence of appointment		
Records relating to trustee and LGC declaration against disqualification criteria	Date on which the trustee/LGC member's appointment ends, plus six years	Securely disposed of
Register of business interests	Date the trustee/LGC member's appointment ends, plus six years	Securely disposed of
Trustee and LGC code of conduct	Dynamic document – kept permanently	Securely disposed of
Records relating to the training required and received by trustees and LGC members	Date the trustee/LGC member steps down, plus six years	Securely disposed of
Records relating to the induction programme for new trustees and LGC members	Date on which the trustee and LGC member's appointment ends, plus six years	Securely disposed of
Records relating to DBS checks carried out on the clerk and members of the board and local governance committees	Date of the DBS check, plus six months	Securely disposed of
Trustee and LGC member personnel files	Date on which the trustee/LGC member's appointment ends, plus six years	Securely disposed of
Headteachers and senior leadership team (SLT)		
Log books of activity in the academy maintained by the headteacher	Date of last entry, plus a minimum of six years	Reviewed and offered to the county archives service 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, 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	Securely disposed of

	the duration of the plan, plus six years	
Academy development plan	Duration of the plan, plus three years	Securely disposed of

7. Retention of health and safety records

7.1. The table below outlines the Trust'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
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 last entry in the accident reporting book	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
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 Trust'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 pensions		
Maternity pay records	Current academic year, plus three years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995 (as amended)	Current academic year, plus six years	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

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 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
Members allowance register	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
Pay packet receipt by employee	Current academic year, plus two 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 and or Trust, 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 Trust	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 and requisitions, 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	Current academic year, plus two years	Securely disposed of
School or Trust fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Life of the contract, plus six or 12 years	Securely disposed of
School meals		
Free school meals registers	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

9. Retention of other Trust records

9.1. The table below outlines the Trust's retention periods for any other records held by the Trust, 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		
Title deeds of properties belonging to the Trust	Permanent	Transferred to new owners if the building is leased or sold
Plans of property belonging to the Trust	For as long as the building belongs to the Trust	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the Trust	Expiry of lease, plus six years	Securely disposed of
Records relating to the letting of Trust premises	Current financial year, plus six years	Securely disposed of
Maintenance		

All records relating to the maintenance of the Trust carried out by contractors	For as long as the Trust 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 Trust	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 or Trust 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
Walking bus registers	Date of register, plus six years	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, e.g. SLT@school.co.uk, 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 and emails.

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 hard copies 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 should be reviewed and 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 subject access request (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 in order 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 fee will be charged. All fees will be 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 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.

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

11.3. 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.

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 Sigma Trust, in conjunction with the Headteacher, will undertake a risk analysis to identify which records are vital to Trust management, and these records will be stored in the most secure manner.

12.2. The Sigma Trust, in conjunction with the Headteacher, will conduct a backup of information on a daily 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. 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.

12.8. Memory sticks are not to be used.

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

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

12.11. All members of staff are provided with their own secure login and follow The Sigma Trust password policy

Be at least 8 characters in length.
Contain at least 1 lowercase and 1 uppercase letter.
Contain at least 1 special character (!@#$%^&*)
Contain at least 1 number (0–9)

12.12. The Sigma Trust password policy for renewals is;

System access and log on every 90 days

Management Information System every 12 months

Finance, Personnel and Payroll Systems every 90 days

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

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

12.15. When sending confidential information by fax, staff always check that the recipient is correct before sending.

12.16. Where personal information that could be considered private or confidential is taken off the premises, 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.

12.17. If documents that have been taken off the school premises will be left unattended, the staff member will leave the documents in the locked boot of a car or keep them on their person.

12.18. 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 digitally remotely accessed.

12.19. Before sharing data, all staff always ensure that:

- They are allowed to share it.
- Adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

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

12.21. 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.

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

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

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

12.25. The Trust takes its duties under the DPA 1998 seriously and any unauthorised disclosure may result in disciplinary action.

12.26. The Sigma Trust, in conjunction with the headteacher, are responsible for continuity, and recovery measures in place to ensure the security of protected data.

12.27. Any damage to or theft of data will be managed in accordance with the Trust's Disaster Recovery Plan.

12.28. 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 Annually by the Sigma Trust, in conjunction with the headteachers.

12.29. The Sigma Trust, in conjunction with the headteachers decides what restrictions are necessary to prevent information or records being downloaded, transferred or printed while the user is not on the school site.

13. Accessing information

13.1. All members of staff, parents of registered pupils and other users 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 keep it up-to-date.
- Understand what the Trust is doing to comply with its obligations under the GDPR.

13.2. All members of staff, parents of registered pupils and other users have the right, under the DPA 1998, to access certain personal data being held about them or their child.

13.3. 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.

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

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

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

14. Digital continuity statement (information stored in a format that is usable long term)

14.1. Digital data that is retained for longer than six years will be named as part of a digital continuity statement.

14.2. The Sigma Trust, in conjunction with the headteacher, will identify any digital data that will need be named as part of a digital continuity statement.

14.3. 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 10 of this policy.

14.4. Memory sticks will never be used to store digital data.

14.5. On an annual basis, The Sigma Trust will review the storage methods used to ensure that new technology and storage methods are assessed and, where appropriate, added to the digital continuity statement.

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

- A statement of purpose and 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 is to be managed in accordance with the DPA 1998

15. Information audit

15.1. The Trust conducts information audits on an annual basis against all information held by the Trust: to evaluate the information the Trust is holding, receiving and using, and to ensure that this is correctly managed in accordance with the 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

15.2. The information audit may be completed in a number of ways:

- 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 Trust's needs
- The information needed to meet those needs
- The format in which it is stored
- How long it needs to be kept for
- Vital records status and any protective marking
- Who is responsible for maintaining the original document?

15.4. The Trust Data Manager 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 Data Manager will record all details on the Trust's Information Asset Register.

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 information displayed on the Information Asset Register will be shared with the headteacher and CEO to gain their approval.

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, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut, archived or digitalised The school Data Manager will keep a record of all files that have been destroyed.

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

16.4. 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.

16.5. Where information has been kept for administrative purposes, the school Data manager will review the information again after three years, and conduct the same process. If it should 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 subsequent three years.

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

16.7. Records and information that might be of relevant to the Independent Inquiry into Child Sexual Abuse (IICSA) will not be disposed of or destroyed.

17. Monitoring and review

17.1. This policy will be reviewed on an annual basis by the Trust Data Protection Officer.

17.2. Any changes made to this policy will be communicated to all members of staff.