



**GDPR COMPLIANT RECORDS
MANAGEMENT POLICY
(Retention Schedule)**

The Central Team and DPO will review this policy on 2 yearly cycle

Policy Version:	V3
Colleagues affected by this Policy:	All stakeholders
Person responsible for the Policy:	Chief Operating Officer
Approved by/ date:	CEO/ Sept 2021
Next review:	Sept 2023
*Reviewed/ *Next review: (*delete)	

Contents:

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

Statement of intent

The Sea View 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 UK General Data Protection Regulation (UK GDPR), 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 Trust has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the Trust's statutory requirements.

This document complies with the requirements set out in the UK GDPR and the Data Protection Act 2018 (DPA), which came into effect in May 2018.

The retention periods outlined in this policy are good practice guidelines only, and Trusts should ensure that they consider requirements specific to their Trust when implementing these timeframes. The tables for retention periods are based on information provided by the Information Records Management Society (IRMS) and are not an exhaustive list of records that may be kept by Trusts. Where the IRMS has not provided guidance for disposal methods or retention periods, good practice recommendations have been provided in **yellow and bold**.

1. Legal framework

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

- UK General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)

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

- Information Records Management Society 'Information Management Toolkit for Trusts' 2016

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 Policy

2. Responsibilities

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

2.2. The Executive Leader holds overall responsibility for this policy and for ensuring it is implemented correctly.

2.3. The Data Protection Officer is responsible for the management of records at the Trust.

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

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

2.6. All staff members are responsible for ensuring that any records for which they are responsible for are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3. Management of pupil records

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

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
- 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, including their home address(es) and telephone number(s)
 - Name of the Trust, admission number, the date of admission and the date of leaving, where appropriate
 - Any other agency involvement, e.g. speech and language therapist
- 3.4. 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
- 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 education and healthcare (EHC) plan and support offered in relation to the EHC plan
- 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 Trust office:

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

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

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

3.8. Actual copies of accident and incident information are stored separately on the Trust'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.

- 3.9. The Trust will ensure that no pupil records are altered or amended before transferring them to the next Trust that the pupil will attend.
- 3.10. The only exception to the above is if any records placed on the pupil’s file have a shorter retention period and may need to be removed. In such cases, the DPO responsible for disposing records, will remove these records.
- 3.11. Electronic records relating to a pupil’s record will also be transferred to the pupils’ next Trust. Section 10 of this policy outlines how electronic records will be transferred.
- 3.12. If any pupil attends the Trust until statutory Trust leaving age, the Trust will keep the pupil’s records until the pupil reaches the age of 25 years.
- 3.13. The Trust 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 Trust 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 Trust.

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 be destroyed in line with the retention periods below.

Type of File	Retention Period	Action to take
Admissions		
Register of admissions	Three years after the date the entry was made	Information is reviewed and the register may be kept permanently
Secondary Trust admissions	The current academic year, plus one year	Securely dispose of
Proof of address (supplied as part of the admissions process)	The current academic year, plus one year	Securely dispose of
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Added to the pupil’s record	Securely dispose of
Supplementary information submitted, including religious	Until the Appeals’ process has been completed	Securely dispose of

and medical information etc. (where the admission was not successful)		
Pupils' Educational Records		
Primary Pupils' educational records	Whilst the pupil remains at the Trust	Transferred to the next destination – if this is an independent Trust, home-schooling or outside of the UK, the file will be kept by the LA and retained for the statutory period.
Secondary Pupils' educational records	25 years after the pupil's date of birth	Securely dispose of
Public examination results	Added to the pupil's record	Returned to the examination board
Internal examination results	Added to the pupil's record	Securely dispose 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	Shred and securely dispose of
Child protection records held in a separate file	25 years after the pupil's date of birth	Shred and securely dispose of
Attendance registers	Last date of entry on to the register, plus three years	Securely dispose of
Letters authorising absence	Current academic year, plus two years	Securely dispose of
SEND		
SEND files, reviews and individual education plans	25 years after the pupil's date of birth (as stated on the pupil's record)	Information is reviewed and the Trust may keep beyond the retention period in order to defend itself in a 'failure to

		provide sufficient education' case.
Statement of SEN maintained under section 324 of the Education Act 1996 or 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 dispose of unless 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 dispose of unless subject to a legal hold
Accessibility strategy	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely dispose of unless 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 dispose of
Examination papers	Until the appeals/validation process has been completed	Securely dispose of
Published Admission Number (PAN) reports	Current academic year, plus six years	Securely dispose of
Valued added and contextual data	Current academic year, plus six years	Securely dispose of
Self-evaluation forms	Current academic year, plus six years	Securely dispose of
Pupils' work	Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year	Securely dispose of

Extra-Curricular Activities		
Parental consent forms for Trust trips where no major incident occurred	Until the conclusion of the trip	Securely dispose of
Parental consent forms for Trust 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 dispose of
Walking bus registers	Three years from the date of the register being taken	Securely dispose of
Family liaison officers & home-school liaison assistants		
Day books	Current academic year, plus two years	Review and securely destroy if no longer required
Reports for outside agencies	Duration of the pupils' time at the Trust	Securely dispose of
Referral forms	Whilst the referral is current	Securely dispose of
Contact data sheets	Current academic year	Review and securely destroy if no longer active
Contact database entries	Current academic year	Review and securely destroy if no longer active
Group registers	Current academic year, plus 2 years	Securely dispose of

5. Retention of staff records

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

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

Type of File	Retention Period	Action to take
Operational		
Staff members personal file	Termination of employment, plus six years	Securely dispose of
Timesheets	The current academic year, plus 6 years	Securely dispose of
Annual appraisal and assessment records	The current academic year, plus 5 years	Securely dispose of
Recruitment		
Records relating to the appointment of a new Executive Leader	Date of appointment, plus 6 years	Securely dispose of
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely dispose of
Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the member of staff's personal file and other information retained for six months	Securely dispose of
DBS certificates	Up to 6 months	Securely dispose of
Proof of identify as part of the enhanced DBS check	Until identity has been proven	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, securely dispose of
Evidence of right to work in the UK	Added to staff personal file or, if kept separately, termination	Securely dispose of

	of employment, plus no longer than two years	
Disciplinary & Grievance Information		
Child protection allegations, including where the allegation is unproven	Added to staff personal 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	Review, shred and securely dispose of
Oral warnings	Date of warning, plus six months	Securely dispose of – if placed on staff personal file, removed from file
Written warning – Level 1	Date of warning, plus six months	Securely dispose of – if placed on staff personal file, removed from file
Written warning – Level 2	Date of warning, plus 12 months	Securely dispose of – if placed on staff personal file, removed from file
Final warning	Date of warning, plus 18 months	Securely dispose 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 <u>above</u>	Securely dispose 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.

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

Type of File	Retention Period	Action to take
Governing Board		
Agendas for governing board meetings	One copy alongside the original set of minutes – all others disposed of without retention	Securely dispose of
Original, signed copies of the minutes of governing board meetings	Permanent	If unable to store, these will be provided to the local authority archive service
Inspection copies of the minutes of governing board meetings	Date of meeting, plus three years	Securely dispose of
Reports presented to the governing board	Minimum of six years, unless they refer to individual reports – these are kept permanently	Securely dispose of or, if they refer to individual reports, retained with the signed, original copy of minutes
Meeting papers relating to the annual parents' meeting	Date of meeting, plus a minimum of six years	Securely dispose of
Instruments of government, including articles of association	Permanent	If unable to store, these will be provided to the local authority archive service
Trusts and endowments managed by the governing board	Permanent	Retained in the Trust whilst it remains open, then provided to the local authority archive service when the Trust closes
Action plans created and administered by the governing board	Duration of the action plan, plus three years	Securely dispose of

Policy documents created and administered by the governing board	Duration of the policy, plus three years	Securely dispose of
Records relating to complaints dealt with by the governing board	Date of the resolution of the complaint, plus a minimum of six years	Reviewed for further retention in case of contentious disputes, then securely dispose of
Annual reports created under the requirements of The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	Date of report, plus 10 years	Securely dispose of
Proposals concerning changing the status of the Trust	Date proposal accepted or declined, plus three years	Securely dispose of
Executive Leader & SLT		
Log books of activity in the Trust maintained by the Executive Leader	Date of last entry, plus a minimum of six years	Reviewed and offered to the local authority archives service if appropriate
Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Review and securely dispose of
Reports created by the Executive Leader or SLT	Date of the report, plus a minimum of three years	Review and securely dispose of
Records created by the Executive Leader, deputy Executive Leader, heads of year and other members of staff with administrative responsibilities	Current academic year, plus six years	Review and securely dispose of
Correspondence created by the Executive Leader, deputy Executive Leader, heads of year and other members of	Date of correspondence, plus three years	Review and securely dispose of

staff with administrative responsibilities		
Professional development plan	Duration of the plan, plus six years	Securely dispose of
Trust development plan	Duration of the plan, plus three years	Securely dispose 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 to take
Health and Safety		
Health and safety policy statements	Duration of policy, plus three years	Securely dispose of
Health and safety risk assessments	Duration of risk assessment, plus three years	Securely dispose of
Records relating to accidents and injuries at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of 15 years is applied	Securely dispose of
Accident reporting – adults	Date of the incident, plus six years	Securely dispose of
Accident reporting - pupils	25 years after the pupil's date of birth, on the pupil's record	Securely dispose of
Control of substances hazardous to health	Current academic year, plus 40 years	Securely dispose 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 dispose of
Information relating to areas where employees and persons are likely to come into contact with radiation	Date of last action, plus 50 years	Securely dispose of
Fire precaution log books	Current academic year, plus six years	Securely dispose of

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 to take
Payroll pensions		
Maternity pay records	Current academic records, plus three years	Securely dispose of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely dispose of
Risk management & insurance		
Employer's liability insurance certificate	Closure of the Trust, plus 40 years	Securely dispose of
Asset Management		

Inventories of furniture and equipment	Current academic year, plus six years	Securely dispose of
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely dispose of
Accounts, Statements & Budget Management		
Annual accounts	Current academic year, plus six years	Securely dispose of
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 dispose of
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Securely dispose of
Records relating to the collection and banking of monies	Current financial year, plus six years	Securely dispose of
Records relating to the identification and collection of debt	Current financial year, plus six years	Securely dispose of
Contract Management		
All records relating to the management of contracts under seal	Last payment on the contract, plus 12 years	Securely dispose of
All records relating to the management of contracts under signature	Last payment on the contract, plus 6 years	Securely dispose of
All records relating to the monitoring of contracts	Current academic year, plus 2 years	Securely dispose of

Trust Fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus 6 years	Securely dispose of
Trust Meals		
Free Trust meals registers	Current academic year, plus 6 years	Securely dispose of
Trust meals registers	Current academic year, plus 3 years	Securely dispose of
Trust meals summary sheets	Current academic year, plus 3 years	Securely dispose 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 to take
Property Management		
Title deeds of properties belonging to the Trust	Permanent	Transfer to new owner upon sale or lease
Plans of property belonging to the Trust	For as long as the building belongs to the Trust	Transfer to new owner upon sale or lease

Leases of property leased by or to the Trust	Length of the lease, plus six years	Securely dispose of
Records relating to the letting of Trust premises	Current financial year, plus six years	Securely dispose of
Maintenance		
All records relating to the maintenance of the Trust buildings carried out by contractors	Current academic year, plus 6 years	Securely dispose of
All records relating to the maintenance of the Trust buildings carried out by employees	Current academic year, plus 6 years	Securely dispose of
Operational Maintenance		
General file series	Current academic year, plus five years	Review and securely dispose of
Records relating to the creation and publication of the Trust brochure and/or prospectus	Current academic year, plus three years	Disposed of against common standards
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	Disposed of against common standards
Visitors' books and signing-in sheets	Current academic year, 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
---	---------------------------------------	------------------------------------

10. Storing and protecting information

- 10.1. The DPO 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.
- 10.2. The DPO will conduct a back-up of information on a termly basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.
- 10.3. Where possible, backed-up information will be stored off the Trust premises, using a central back-up service operated by the LA.
- 10.4. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.
- 10.5. Confidential paper records are not left unattended or in clear view when held in a location with general access.
- 10.6. 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.
- 10.7. 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.
- 10.8. Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.
- 10.9. All electronic devices are password-protected to protect the information on the device in case of theft.
- 10.10. Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- 10.11. Staff and governors do not use their personal laptops or computers for Trust purposes.
- 10.12. All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- 10.13. Emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.

- 10.14. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 10.15. When sending confidential information by fax, members of staff always check that the recipient is correct before sending.
- 10.16. 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 Trust premises accepts full responsibility for the security of the data.
- 10.17. Before sharing data, staff always ensure that:
- They have consent from data subjects to share it, if consent is required
 - Adequate security is in place to protect it.
 - The data recipient has been outlined in a privacy notice.
- 10.18. 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.
- 10.19. 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.
- 10.20. The physical security of the Trust's buildings and storage systems, and access to them, is reviewed termly by the Site Manager in conjunction with the DPO. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the Executive Leader and extra measures to secure data storage will be put in place.
- 10.21. The Trust takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- 10.22. The DPO is responsible for continuity and recovery measures are in place to ensure the security of protected data.
- 10.23. Any damage to or theft of data will be managed in accordance with the Trust's Data Breach Policy.

11. Policy review

- 11.1. This policy is reviewed every two years by the Data Protection Officer and the Executive Leader.
- 11.2 The next scheduled review date for this policy is September 2023.