Data Retention and Disposal Policy

Aims

Alamiyah Montessori is committed to maintaining the confidentiality of its information and ensuring that all records within the setting are only accessible by the appropriate individuals. In line with the requirements of the GDPR, the setting 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. This policy outlines how records are stored, accessed, monitored, retained and disposed of, in order to meet the setting's statutory requirements.

This document complies with the requirements set out in the GDPR, which is effective as of 25 May 2018.

This policy will be implemented in conjunction with the following other policies of the organisation:

- Data Protection Policy
- E- Safety Policy

1. Responsibilities

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

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

The data protection officer (DPO) is responsible for the management of records at Alamiyah Montessori. The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the manager. 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.

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.

2. 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 setting or school that a pupil attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement.

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

- Forename, surname, gender and date of birth
- Note of the date when the file was opened
- Note of the date when the file was closed, if appropriate

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 setting or school, admission number, date of admission and date of leaving, if applicable
- Any other agency involvement, e.g. speech and language therapist

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, health and care (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

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

- 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

Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet in the administration 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 manager'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 setting'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 setting will ensure that no pupil records are altered or amended before transferring them to the next institution that the pupil will attend.

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.

Electronic records relating to a pupil's record will also be transferred to the pupils' next setting or school. Section 11 of this policy outlines how electronic records will be transferred.

The setting 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 setting. The responsibility for these records will then transfer to the next institution that the pupil attends.

The setting 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 institution 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 setting.

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

The table below outlines the setting'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
Children's Record		
Images used for identification purposes	Whilst the pupil is at setting, plus three years after leaving	Securely disposed of

Images used in displays in setting, marketing purposes or other	Whilst the pupil is at setting, plus three years after leaving	Securely disposed of
House number, road, postcodes, names and characteristics	Whilst the pupil is at the setting, plus three years after leaving	Securely disposed of
Birth Certificate & Parent/Carer ID	Whilst the pupil is at the setting, plus three years after leaving	Securely disposed of
Register of admissions	Whilst the pupil is at the setting, plus three years after leaving	Information is reviewed and the register may be kept permanently
Proof of address (supplied as part of the admissions process)	Whilst the pupil is at the setting, plus three years after leaving	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Whilst the pupil is at the setting, plus three years after leaving	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was not successful)	Whilst the pupil is at the setting, plus three years after leaving	Securely disposed of
Pupils' educational records	Whilst the pupil is at the setting plus three years after leaving	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

Behaviour and Exclusion records	Added to the pupil's record and transferred to the next school/setting Copies are held whilst the pupil is at the setting, plus three years after leaving	Securely disposed of
Attendance registers	Whilst the pupil is at the setting, plus three years after leaving	Securely disposed of
Letters authorising absence	Whilst the pupil is at the setting, plus three years after leaving	Securely disposed of
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 file may be kept for longer than necessary if it is required for the setting to defend themselves in a 'failure to provide sufficient education' case
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

Safeguarding		
Child protection records held on a pupil's record	25 years after the pupil's date of birth	Securely disposed of – shredded
Child protection records held in a separate file	25 years after the pupil's date of birth	Securely disposed of - shredded
Medical information and administration		
Permission slips	For the duration of the period that medication is given, plus one month	Securely disposed of
Accident & pre existing injuries forms		
Medical incidents that have a behavioural or safeguarding influence	Added to the pupil's record and transferred to the next school or setting Copies held whilst the pupil is at setting, plus 25 years	Securely disposed of
Observation, planning and assessment records of children		
Pupils' work	Returned to pupils at the end of the academic year, or retained for the current academic year	Securely disposed of
Trip records		
Parental consent forms for trips offsite where a major incident occurred	Three years from the date of the register	Securely disposed of

	being taken. For inspection purposes	
Personnel records		

Staff members' personal file	Termination of employment, plus seven years	Securely disposed of
Timesheets	Current academic year, plus seven years	Securely disposed of
Half Termly Supervisions and Annual appraisal records	Current academic year, plus seven years	Securely disposed of
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of
DBS certificates	Up to eleven months	Securely disposed of
Proof of identity as part of the enhanced DBS check	After 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 disposed of

Staff Disciplinary and grievance procedures		
Child protection allegations, including where the allegation is unproven	Added to staff personal file, and until the individual's normal retirement age, or 25 years from the date of the allegation – whichever is longer If allegations are malicious, they are removed from personal files	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

5. Retention of senior leadership and management records

The table below outlines the setting'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
Organisation		
Original, signed copies of the minutes of Trustee board meetings, annual report	Date of meeting plus 10 years	If unable to store, these will be provided to the county archives service
Instruments of government, including articles of association	Permanent	If unable to store, these will be provided to the county archives service
Policy documents created and administered by the trustee board	Duration of the policy, plus three years	Securely disposed of
Records relating to complaints dealt with by the Trustee board	Date of the resolution of the complaint, plus a minimum of seven years	Reviewed for further retention in case of contentious disputes, then securely disposed of

6. Retention of health and safety records

The table below outlines the setting'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	Permanently	If unable to store, these will be provided to the county archives service
Health and safety risk assessments	Permanently	If unable to store, these will be provided to the county archives service
Records relating to accidents and injuries at work	Permanently	If unable to store, these will be provided to the county archives service
Accident reporting – adults	Permanently	If unable to store, these will be provided to the county archives service
Accident reporting – pupils	Permanently	If unable to store, these will be provided to the county archives service
Control of substances hazardous to health	Current academic year, plus 40 years of the last entry	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	Date of last action, plus 50 years	Securely disposed of

come into contact with radiation		
Fire precautions log books	Permanently	If unable to store, these will be provided to the county archives service

7. Retention of financial records

The table below outlines the setting'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
Accounting		
Maternity pay records	Current academic year, plus seven years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus seven years	Securely disposed of
Annual accounts	Current academic year, plus seven years	Disposed of against common standards
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus seven years	Securely disposed of
Records relating to the collection and banking of monies	Current financial year, plus seven years	Securely disposed of

Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus seven years	Securely disposed of
Wages pay records	Current financial year, plus seven years	Securely disposed of

8. Retention of other records held by the organisation

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

Insurance		
All records relating to Insurance for the organisation and setting	40 years from date insured	Securely disposed of

9. Identifying information

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

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

Once an individual has left the setting, 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 setting removes any personal data not required and keeps only the data needed – in this example, the statistics of attendance rather than personal information.

10. Storing and protecting information

The DPO will undertake a risk analysis to identify which records are vital to the setting's management and these records will be stored in the most secure manner.

The DPO will test the restoration of information from the backup 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.

Backed-up information is stored off the premises using a 3rd party hosted solution.

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

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

Digital data is password-protected, and stored 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.

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

The setting's iPads have the feature enabled which allows remote blocking in the event of theft.

Staff, trustees and board members do not use their personal laptops or computers for the purposes of the organisation.

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

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.

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

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 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 premises accepts full responsibility for the security of the data.

Before sharing data, staff always ensure that:

- They have consent from data subjects to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

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.

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

The physical security of the organisation'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 manager and extra measures to secure data storage will be put in place.

The organisation takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

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

11. Accessing information

Alamiyah Montessori is 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 setting, e.g. visitors and third-party providers, are entitled to:

- Know what information the setting 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 setting is doing to comply with its obligations under the GDPR.

All members of staff, parents of registered pupils and other users of the setting and its facilities have the right, under the 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 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 setting will adhere to the provisions outlined in the organisation's Data Protection Policy when responding to requests seeking access to personal information.

14. 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.

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. The DPO will keep a record of all files that have been destroyed.

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

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 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.

Review of Policy

This policy will be reviewed every 3 years or sooner or if there is any change in statutory guidance or legislation. See 'Policy Review Schedule'.

Adopted in a meeting at Alamiyah Montessori on 08/09/2025

Last Reviewed: 10/09/2026

Signed: N Bobat (Manager) and S Motara (Nominated Person)

On behalf of Alamiyah Montessori

With reference to -

General Data Protection Regulation 2018

Freedom of Information Act 2000

Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)

Information Records Management Society IRMS (2016)

Information Management Toolkit for Schools

DfE (2018) 'Data protection: a toolkit for schools