

Privacy and Privacy Notices

Updated: 13th August 2025

Contents

Intention	3
Legislative context	3
Legal guidelines and frameworks	3
Legal duties.....	3
Definition of terms used in this policy	3
Retention schedule	3
Guiding principles.....	3
Roles and responsibilities	4
Updates to this policy.....	4
Where to find our privacy notice	4
Categories of individuals we hold information about.....	4
Guidelines for staff for sharing information responsibly	5
How we work with sub-processors.....	5
List of sub-processors we currently work with	6
Sharing data with parties who are not currently authorised sub-processors.....	7
Confidentiality agreements with third parties with access to personal data	7
Sharing data without obtaining additional consent	7
Sharing data with additional consent	7
How the nursery obtains consent to collect personal data	7
How the nursery stores and protects personal data	9
Protecting personal data when it is shared with external parties.....	9
How the nursery responds to data breaches.....	9
How the nursery uses automated data processing	9
Restricted access to sensitive records	10
How to make a complaint about the nursery's use of personal data	10
Privacy notice for families.....	10
What do you use my personal data for?	10
Retention schedule and retention purpose	11
Why do you hold my personal data for this length of time?.....	12
Privacy notice for job applicants	12
What do you use my personal data for?	12
Retention schedule and retention purpose	13

Why do you hold my personal data for this length of time?.....	13
Privacy notice for staff members.....	13
What do you use my personal data for?	13
Retention schedule and retention purpose	14
Why do you hold my personal data for this length of time?.....	14
Privacy notice for other parties	15
What do you use my personal data for?	15
Retention schedule and retention purpose	15
Why do you hold my personal data for this length of time?.....	15
Training requirements.....	15
Monitoring and review	16
Supplementary procedures, risk assessments and other documentation.....	16

Intention

The primary goal of the Privacy Policy is to inform and educate individuals about how their personal data is collected, used, processed and shared. It ensures transparency, builds trust, and demonstrates the nursery's commitment to data protection and privacy. Additionally, it helps the nursery comply with legal requirements, delineates individuals' rights regarding their data, and provides clarity on the recourse available to them.

Legislative context

Legal guidelines and frameworks

- Data Protection Act, 2018
- UK General Data Protection Regulation (UK GDPR).
- The Limitation Act, 1980
- Early Years Foundation Stage Statutory Framework, 2024 (EYFS).
- Working Together to Safeguard Children, 2025

Legal duties

Early years providers, including nurseries, childminders, and reception classes, are subject to the same legal data protection requirements as any other sector under UK GDPR and the Data Protection Act 2018. These laws set out clear duties to handle personal data lawfully, fairly, and transparently; to collect it only for specified, legitimate purposes; to limit the data collected to what is necessary; to ensure accuracy and keep it up to date; to store it only for as long as needed; to protect it with appropriate security measures; and to demonstrate accountability in all aspects of data handling.

Definition of terms used in this policy

Retention schedule

A retention schedule sets out how long different types of records or personal data are kept. For the purposes of this policy:

- For children and families: the retention periods begin from the date a child leaves the nursery. Once the specified retention time has passed, the record will be deleted in January of the following year.
- For successful job applicants and staff members: the retention period begins on the date employment ends, and records are deleted in the following January once the retention period has expired.
- For unsuccessful job applicants: the retention period begins on the date the job applicant was informed they were unsuccessful, and records are deleted in the following January once the retention period has expired.
- For other parties: the retention period begins on the date the personal data was, and records are deleted in the following January once the retention period has expired.

Guiding principles

This policy is guided by the principle that safeguarding children's welfare is the highest priority, with all data handling practices designed to support this aim while ensuring the efficient and lawful running of the nursery. Information is collected and processed strictly on a "need-to-know" basis in line with data minimisation principles, meaning only the data necessary for

specific, legitimate purposes is gathered. This enables the nursery to meet statutory safeguarding duties, fulfil operational needs such as communication and record-keeping, and comply with legal obligations under the UK GDPR and Data Protection Act 2018.

Roles and responsibilities

Role	Responsibility
All staff	Follow the guidelines in this policy about confidentiality and information sharing
Manager	- Ensuring that all staff follow confidentiality requirements - Ensuring Data Protection Agreements are in place - Ensuring data is held in line with retention schedules
Data Protection Officer	- Responding to questions or concerns about this policy - Responding to subject access requests - Ensuring this policy is in line with statutory requirements

Updates to this policy

This policy may be unilaterally updated at any time with immediate effect to ensure clarity, reflect the nursery's current operational practices, and maintain compliance with the latest government legislation and guidance. Please refer to the 'More Information' section on the website for the latest copy of this policy.

Where to find our privacy notice

This document includes both our Privacy Policy and our Privacy Notices. By combining these into one document, we aim to give a clear, transparent explanation of how we collect, use, store, share, and protect personal information, as well as the rights individuals have in relation to their data.

Categories of individuals we hold information about

This policy explains how the nursery collects, uses, and protects the personal information of the groups listed below. For details on what data we keep, why we keep it, and how long for, see the relevant Privacy Notice in this policy.

Category	Privacy Notice	Description
Children	Families	Those currently attending, previously enrolled, or registered for future attendance
Parents/carers		Individuals with parental responsibility or legal guardianship
Job applicants	Job applicants	Those applying for job roles or voluntary positions, whether successful or unsuccessful.

Staff members	Staff members	Current and former employees, volunteers, apprentices, and agency workers
Service providers and external partners	Other parties	Individuals who support nursery operations or provide professional services such as speech therapists, SEND specialists, safeguarding consultants, trainers, assessors and Early Years consultants
Visitors		All other parties who may visit the nursery, such as prospective parents and contractors.

Guidelines for staff for sharing information responsibly

Every staff member is required to maintain strict confidentiality about information relating to the nursery, its children, families, and suppliers. This responsibility continues even when not at work or after employment ends.

Guidance on sharing information	
Acceptable	Not acceptable
• Sharing information with other staff members is permissible when necessary to fulfil your job responsibilities and provide appropriate care for the children. • Sharing information about a child's day, development, or well-being with their parent/carer. • In situations where disclosure is required by law, such as reporting suspected abuse or neglect to child protection agencies or complying with a court order. • If a child's safety or well-being is at immediate risk, sharing information with emergency services or other appropriate authorities is necessary.	• Never post photos or videos of children at the nursery or discuss children or families on social media platforms. • Never share information about children or families with individuals who are not authorised to receive it, including friends, family members, or other parents/carers. • Never gossip or spread rumours about children, families, or staff members. • Avoid sharing confidential information in casual settings, unless strictly necessary and in the best interests of a child's welfare.

How we work with sub-processors

Each sub-processor is bound by a Data Processing Agreement, which clearly sets out their responsibilities and obligations for handling personal data securely and lawfully. This agreement may be our own internal version or, in the case of larger organisations, the sub-processor's standard data processing terms. For large multinational companies, it is often not practical or feasible to require them to sign our own version, as they operate under global standard agreements that already meet or exceed UK GDPR requirements.

List of sub-processors we currently work with

The following sub-processors are authorised to process, host, or have access to personal data on behalf of the nursery. This list is not exhaustive and may be updated from time to time.

Authorised sub-processors			
<i>Sub-processor</i>	<i>Location</i>	<i>Description of services</i>	<i>Data processed</i>
Family Ltd	UK	Nursery management software	• Children's records • Safeguarding records • Employee records
Minoa Holdco KBL Ltd	UK	Support services	• Children's records • Safeguarding records • Employee records • Job applications records
Minoa LGH Ltd	UK	Support services	• Children's records • Safeguarding records • Employee records • Job applications records
Microsoft Corporation, Inc	EU	Cloud storage, email services and operating system	• Children's records • Safeguarding records • Employee records • Job applications records
Jotform, Inc	EU and US	Online form creation and submission platform	• Children's records • Safeguarding records • Employee records • Job applications records
Stripe Payments Europe Ltd	US	Payment processing	• Bill payer information
Early Years Fundamentals Ltd	UK	Educational consultant	• Children's records • Safeguarding records • Employee records • Job applications records
The Local Authority Early Years Team	UK	Educational consultant	• Children's records • Safeguarding records • Employee records • Job applications records

The Local Authority Funding Team	UK	Processes government early years funding claims and payments	• Children's records
----------------------------------	----	--	--

Sharing data with parties who are not currently authorised sub-processors

If the nursery needs to share personal data with a third party who is not on our authorised sub-processor list, we will take the following steps before any data is shared:

- We will obtain consent from the individual(s) whose data will be shared, explaining the purpose and scope of the sharing.
- We will put in place a Data Protection Agreement or ensure there is an equivalent contractual agreement in place with that third party that safeguards personal information in line with legal requirements.

Confidentiality agreements with third parties with access to personal data

Some third parties do not actively process or use personal data on our behalf but may have incidental or temporary access to it while carrying out their duties. Examples include IT support providers and cleaning staff who may see or come into contact with documents, systems, or records containing personal information.

Where such access is possible, we will ensure appropriate contractual safeguards are in place before they begin work. This may take the form of a Data Processing Agreement (if the access is significant or involves any element of processing) or a confidentiality agreement (if the access is incidental and no processing takes place).

Sharing data without obtaining additional consent

We may share personal data with other organisations in the following situations without obtaining additional consent:

- When the law requires us to share information, or when we believe it is necessary to meet legal or regulatory obligations.
- When we need to share information with our legal or professional advisers to establish, exercise, or defend our rights.
- If our company or assets are sold or transferred, personal data may be shared with the new owner as part of the transfer.

In these cases, we do not need to ask for your additional consent, as the sharing is permitted under data protection law.

Sharing data with additional consent

There may be occasions where sharing personal data with third parties could benefit the individual it relates to. For example, opportunities may arise to share relevant information with specialists such as Speech and Language Therapists, Occupational Therapists, or Local Authority advisors to support a child's needs. If this type of sharing is not covered by the original reason the data was collected, explicit consent will always be sought before doing so.

How the nursery obtains consent to collect personal data

The nursery obtains consent to collect personal data either by asking the individual (or their parent/carer, where appropriate) to tick a consent box on a form or by requesting it in writing. Before giving consent, individuals are provided a copy of or directed to our Privacy Policy, which explains how personal data is collected, used, and protected. The Privacy Policy can be found in the More Information section of our website.

What happens if we use personal data for a different reason than it was collected for

Personal data will only be used for the purposes for which it was collected. If it needs to be used for another reason, this will only happen if the new purpose is compatible with the original one. This means the new use must be closely related to why the data was collected, must not cause harm to the individual, and must be in line with what they could reasonably expect. If the data ever needs to be used for a purpose that is not compatible with the original reason, the individual will be informed, the legal basis for the new use will be explained, and their consent will be obtained before proceeding.

Individuals' rights over their personal data held by the nursery

Under data protection law, individuals have specific rights over the personal information held about them.

Any of these rights can be exercised by sending an email to the nursery's Data Protection Officer at the email address below.

dataprotection@minoaeducation.com

Once a request has been submitted, the nursery may contact the individual to authenticate their identity or to gather any information needed to respond. Except in rare cases, a response will be provided within one month of receiving the required information. If any right is not available to the individual, they will be informed along with the reason for the decision. The table below explains each right, what it means, and when it applies.

Right	What does this mean?	Is it available to you?
The right to be informed	You have the right to know how we collect, use, store, and share your personal data.	Yes
The right to request access to personal data	You can request a copy of the data we hold about you and related information	Yes
The right to request rectification of personal data	You can ask us to correct any inaccurate data about you and to complete any incomplete data that we hold about you	Yes

The right to request deletion of personal data	You can request that we delete the personal data we hold about you	Yes, in certain situations
The right to request a restriction on processing of personal data	You can request that we restrict our use of your data to storage only, that we stop using it for all other purposes or that we retain data that was due for deletion	Yes, in certain situations
The right to object to the processing of personal data	You can object to certain types of processing of your personal data in certain specific circumstances	Yes, in certain situations
The right of data portability	You have the right to receive a copy of your personal data and, where possible, have this sent to another organisation	Yes, where you have given consent for us to process personal data
The right to withdraw consent	You have the right to withdraw any consent that you have given, at any time	Yes, whenever you have given consent

How the nursery stores and protects personal data

The nursery takes measures to keep personal data safe from loss, misuse, unauthorised access, disclosure, alteration, or destruction. These measures include:

- Partnering only with reputable, trusted companies to store and process data.
- Keeping all physical records securely locked away when not in use.
- Restricting access to personal data to authorised staff who need it for their work.
- Training staff on their data protection and confidentiality responsibilities.
- Implementing the IT controls set out in our Technology and e-Safety Policy to prevent unauthorised access or cyber threats.

Protecting personal data when it is shared with external parties

When we share personal data with an external party, we take the following steps to keep it safe:

- Password-protect any attachments containing personal data.
- Send the password in a separate email so that, if one message is intercepted or opened by the wrong person, they cannot access the protected file.
- Use initials where names are not necessary to convey the information being shared.
- Use initials instead of full names in the email body, as its content may be viewed by someone other than the intended recipient (e.g., if their screen is left unlocked or monitored).

How the nursery responds to data breaches

If a personal data breach occurs, the nursery will act quickly to contain and assess it, notify the Information Commissioner's Office (ICO) within 72 hours where required, or consult the ICO if unsure whether notification is needed, and inform affected individuals without undue delay.

How the nursery uses automated data processing

Some personal data is processed using automated systems, for example when a form is submitted through Jotform and an automatic email acknowledgement or follow-up message is sent. These automated actions are used only to support efficient communication and administration. The nursery does not use automated decision-making or profiling that produces legal effects or significantly affects individuals.

Restricted access to sensitive records

Some personal information is highly sensitive and is subject to additional access restrictions. This includes, for example, child protection records, safeguarding reports, and information received from external agencies marked as confidential. Access to such information is strictly limited to designated staff who require it to fulfil their safeguarding responsibilities. These records will only be shared to protect the welfare of a child or to respond to any legal requirements.

In certain circumstances, these records may not be made available in response to a subject access request if doing so would risk harm to an individual, interfere with an ongoing investigation, or breach the confidentiality of another person.

How to make a complaint about the nursery's use of personal data

If there is a concern about how personal data has been handled, there are three ways to raise a complaint:

- Raise it internally by following the steps in our Complaints and Compliments Policy.
- Escalate the complaint to the Information Commissioner's Office (ICO) if the issue is not resolved internally. The ICO will usually expect the complaint to have been raised with us first and for us to have been given adequate time to respond.

ICO contact details

Website	https://ico.org.uk/
Telephone	0303 123 1113

Privacy notice for families

What do you use my personal data for?

Retention purpose	Code	Description
Enrolment	EN	To set up a record for each child, gather key onboarding and contact information, identify any reasonable adjustments needed, and record safeguarding details.
Safeguarding	SG	To record essential information that protects a child's health, safety, and well-being, and to meet legal requirements for safeguarding and child protection.

Communication	CM	To keep families informed about their child's progress, wellbeing, and nursery matters, and to maintain accurate records of these interactions.
Compliance and legal	LE	To meet legal and regulatory requirements and to retain evidence to support recruitment decisions if legal issues arise.
Progress tracking	PT	To monitor and support each child's learning in line with the nursery's curriculum.
Funding and billing	FB	To process and manage government funding claims, childcare vouchers, billing, invoicing, and other financial arrangements.
Marketing	MA	To share information about nursery services, events, and activities that may be of interest to prospective families.

Retention schedule and retention purpose

Source	Retention schedule	Retention purpose						
		EN	SG	CM	LE	PT	FB	MA
Enquiry form	25 years	✓		✓				✓
Application form	25 years	✓					✓	
Agreement form	25 years	✓			✓		✓	
Enrolment form	25 years	✓	✓		✓			
Observations	25 years					✓		
Assessments	25 years					✓		
Funding form	25 years						✓	
Child health care plan	25 years		✓					
Child risk assessment	25 years		✓					
Safeguarding referrals	25 years		✓		✓			
SEND referrals	25 years		✓					
Accidents form	25 years		✓		✓			
Incident form	25 years		✓		✓			

Head bump monitoring form	25 years		✓		✓			
Child concern form	25 years		✓		✓			
Visitors book	25 years		✓		✓			
Conversation logs	25 years		✓		✓			
Photography for marketing purposes	25 years							✓

Why do you hold my personal data for this length of time?

We retain all personal data related to children and families who attend the nursery for a period of 25 years. Retention periods begin from the date a child leaves the nursery. Once the specified retention time has passed, the record will be deleted in January of the following year.

This satisfies the EYFS requirement to keep children's records for a "reasonable period" and complies with UK GDPR's storage-limitation principle by linking retention to legal necessity. Under the Limitation Act 1980, time limits for claims from childhood incidents run from age 18 and can extend up to six years, so evidence may be needed into a young adult's mid-twenties.

We apply a blanket 25-year retention because any data we hold could potentially become relevant in safeguarding matters, even if the connection is not immediately obvious at the time of collection. For example, a record of a child's authorised collectors might seem routine but could, years later, provide critical evidence in an investigation into historical abuse, child abduction, or custody disputes. Retaining such information ensures that, if a safeguarding concern arises long after the child has left, we have the fullest possible record to support the investigation and protect those involved.

Privacy notice for job applicants

What do you use my personal data for?

Retention purpose	Code	Description
Candidate assessment	CA	To review each applicant's skills, qualifications, work history and suitability to work with children to decide whether to offer a role.
Talent pool for future vacancies	TP	To refer to existing applicant records when a future role becomes available to see if there is a potential match for the role.
Recruitment feedback	RF	To provide applicants with specific and constructive feedback explaining why their job application was successful or unsuccessful.
Compliance and legal	LE	To meet legal and regulatory requirements and to retain evidence to support recruitment decisions if legal issues arise.

Retention schedule and retention purpose

Source	Retention schedule for <u>unsuccessful</u> candidates	Retention schedule for <u>successful</u> candidates	Retention purpose			
			CA	TP	RF	LE
Application form	2 years	7 years	✓	✓	✓	✓
CV	2 years	7 years	✓	✓	✓	✓
Cover letter	2 years	7 years	✓	✓	✓	✓
Interview notes	2 years	7 years	✓	✓	✓	✓
References	2 years	7 years	✓	✓	✓	✓
Online screening	2 years	7 years	✓	✓	✓	✓
Proof of right to work	2 years	7 years	✓	✓	✓	✓

Why do you hold my personal data for this length of time?

These retention periods are set to balance operational needs with legal and regulatory requirements. Unsuccessful candidate records are kept for 2 years to allow for reference in future recruitment cycles and to respond to any short-term queries or challenges to the recruitment process. Successful candidate records are retained for 7 years after employment ends to meet statutory limitation periods for employment-related claims, comply with HMRC payroll and tax record requirements, and provide accurate references or employment verification if requested.

Privacy notice for staff members

What do you use my personal data for?

Retention purpose	Code	Description
Assessment of staff suitability	SS	To review each applicant's skills, qualifications, work history and suitability to work with children to decide whether to offer a role.
Payroll	PA	To refer to existing applicant records when a future role becomes available to see if there is a potential match for the role.
Staff welfare and safeguarding	WE	To understand staff needs and any reasonable adjustments required to support their wellbeing and enable them to carry out their role effectively.

Communication and scheduling	CO	To coordinate work schedules, plan staffing, and ensure staff have access to necessary information, including emergency contact details in case of incidents.
Compliance and legal	LE	To meet legal and regulatory requirements and to retain evidence to support recruitment decisions if legal issues arise.

Retention schedule and retention purpose

Source	Retention schedule	Retention purpose				
		SS	PA	WE	CO	LE
Contract	7 years					✓
Training records	7 years	✓				✓
Disciplinary records	7 years	✓				
Performance management records	7 years	✓		✓		
Return to work interviews	7 years	✓		✓		✓
DBS records	7 years	✓				✓
Health declarations	7 years	✓		✓		✓
Declarations of disqualification	7 years	✓		✓		✓
Staff induction	7 years	✓		✓	✓	✓
Payroll records	7 years	✓	✓			✓
Safeguarding allegations	50 years	✓				✓

Why do you hold my personal data for this length of time?

We retain general staff employment records for 7 years after employment ends. The retention period begins on the date employment ceases, and records are deleted in the following January once the period has expired. This timeframe aligns with statutory limitation periods for employment and contractual claims under the Limitation Act 1980 and meets HMRC requirements for payroll and tax record retention.

Records relating to safeguarding matters (whether substantiated, unsubstantiated, or unfounded) are retained for 50 years from the date of the safeguarding incident. This timeframe ensures we meet Department for Education statutory guidance, maintain information for potential safeguarding inquiries or reference checks, and cover the maximum potential working life from first employment to retirement.

The retention period begins on the date employment ends, and records are deleted in the following January once the retention period has expired.

Privacy notice for other parties

What do you use my personal data for?

Retention purpose	Code	Description
Safeguarding	SG	To review each applicant's skills, qualifications, work history and suitability to work with children to decide whether to offer a role.
Compliance and legal	LE	To meet legal and regulatory requirements in the recruitment process, and to retain evidence to support recruitment decisions if legal issues arise.

Retention schedule and retention purpose

Source	Retention schedule	Retention purpose	
		SG	LE
Accident forms	25 years	✓	✓
Visitor logs	3 years	✓	✓

Why do you hold my personal data for this length of time?

We retain visitor accident and incident records for 25 years to align with our longest safeguarding retention period. This ensures that, if the incident involved a child or vulnerable individual, the record remains available for the full period in which safeguarding inquiries, historical abuse investigations, or related legal claims may be made. The extended 25 year retention provides a consistent and cautious approach across all safeguarding-related records, reduces the risk of premature disposal, and ensures evidence is available if required by insurers, investigators, or regulatory authorities.

We retain visitor sign-in logs for 3 years to meet security and safeguarding needs, while limiting the storage of personal data in line with UK GDPR's storage limitation principle. This period is long enough to investigate or respond to any safeguarding concerns, health and safety issues, or security incidents that may come to light after a visit, while avoiding unnecessary long-term retention of personal details.

Training requirements

Type	Learning	Required for
------	----------	--------------

Explainer	Go through the guidance on acceptable and unacceptable practices on sharing confidential information	L1
Explainer	Explain who our approved sub-processors of personal data are, and when a new Data Protection Agreement or Confidentiality Agreement may be required	L2
Explainer	Explain what you should do if there is a data breach	L2
Knowledge Check	What is the retention period for personal data related to children and families who attend the nursery?	L2
Knowledge Check	What is the retention period for personal data related to unsuccessful job applicants?	L2
Knowledge Check	What is the retention period for personal data related to safeguarding allegations against staff members?	L2
Knowledge Check	What is the retention period for personal data related to visitor logs?	L2
Knowledge Check	What is the retention period for personal data related to visitor accidents?	L2
Knowledge Check	What is the retention period for personal data related to staff members?	L2
Training	Data Protection in Education (Flick)	L2

Monitoring and review

The management team will conduct termly audits of each room to ensure that this policy is being followed.

Supplementary procedures, risk assessments and other documentation

- Ensure DPAs and Confidentiality Agreements are in place