2.6 Data protection & record keeping

Policy

We take families' privacy seriously, and in accordance with the General Data Protection Regulation (GDPR), we will process any personal data according to the seven principles below:

- We must have a lawful reason for collecting personal data, and must do it in a fair and transparent way. We will be clear about what data we are collecting, and why.
- We must only use the data for the reason it is initially obtained. This means that we may not use a person's data to market a product or service to them that is unconnected to the reasons for which they shared the data with us in the first place.
- We must not collect any more data than is necessary. We will only collect the data we need to hold in order to do the job for which we have collected the data.
- We will ensure that the data is accurate, and ask parents to check annually and confirm that the data held is still accurate.
- We will not keep data any longer than needed. We must only keep the data for as long as is needed to complete the tasks it was collected for.
- We must protect the personal data. We are responsible for ensuring that staff, and anyone else charged with using the data, processes and stores it securely.
- We will be accountable for the data. This means that we will be able to show how we (and anyone working with us) are complying with the law.

We collect and use children's information under section 537A of the Education Act 1996, and section 83 of the Children Act 1989. We also comply with Article 6(1)(c) and Article 9(2)(b) of the General Data Protection Regulation (GDPR, May 2018).

Procedures

Understanding Data Protection

- In order to provide a quality early years and childcare service and comply with legislation, our setting will need to request information from:
  - parents and carers about themselves, their child/ren and their family.
  - staff about them and their family.
- Information we request will be developmental and personal data.
- Our setting has a 'confidential working relationship' with families and our staff. It is our intention to respect the privacy of all children, their parents and carers and our workforce.
- We aim to ensure that all people can share their information in the confidence that it will only be used in the correct manner.
- There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the Data Protection Act and the Human Rights Act.
- Our setting is registered with the Information Commissioner's Office (ICO), the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
- We expect everyone to respect personal and professional boundaries, keeping private and confidential any sensitive information they may accidentally or intentionally learn about, for example:
  - our employees' private lives.
  - other families using our service(s)/ setting(s).
  - the other children and families attending our setting.

  Any concerns regarding child protection issue must be reported as per our child protection policy.
- We ask people for personal data about themselves and their families (child/ren, spouses, next of kin) in order to deliver our services in a professional and safe way. We are required to hold and use this personal data in order to comply with the statutory framework for the early years foundation stage, Ofsted, Department for Education and the local authorities.

Understanding Privacy Notice

It is a requirement of our registration with the Information Commissioners Office (ICO) to provide information about the details we keep about you and/ or your child/ren. This requirement applies to information we collect in relation to online and paper data processing.

Collecting information

Whilst the majority of information a person provides to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform the person whether they are required to provide certain information to us or if they have a choice in this.

We hold data in line with statutory requirements after a person (parent, child, employee) has left the setting/ company. We have set retention periods for data and records.

Who do we share data with?

Parents: We are required to ensure the information collected about a parent and their child/ren is treated confidentially and only shared when there is a need for it to be shared. In order for us to deliver childcare services we will also share their data as required with the following categories of recipients:

- Our local authority (for example: 2, 3 and 4 year old funding)
- The Department for Education (DfE).
- We share information with other settings or agencies involved in your child's care – requirement of EYFS.
- We share a copy of your child's 2 year progress check with your health visitor – requirement of EYFS.
- We share information about income and expenses including, when requested, your invoices and payments with HMRC and Tax Credits.
- Our childcare management software provider.
- We will not share any information with anyone without parents' consent, unless there is a child protection concern.
- Our insurance underwriter.
- Ofsted may require access to our records at any time.
- Company solicitors to enforce or apply the terms and conditions of your contract with us. If it is necessary to protect our/or others rights, property or safety.

Employees: In order for us to recruit employee's we share data as required with the following categories of recipients:

- Our Local Authority, Ofsted, ICO.
- Government Departments (DfE, DfH, Tax Credits, HMRC).
- Our childcare management software provider.
- HR, Health & Safety, Payroll & Pension Services.
- Legal solicitors.

  This is an non-exhaustive list.

Ensuring data is accurate
We are required to keep data about our staff, parents and their child/ren up-to-date and to ensure it is accurate; We will do this regularly. Everyone has the right to access personal data about themselves and their child/ren and we will share this information with them on request following our procedures outlined herein.

Why we share children's information
We do not share information about our children with anyone without consent unless the law and our policies allow us to do so. We share children's data with the Department for Education (DfE) on a statutory basis. The DfE may also share child level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998 and the General data Protection Regulations 2018.Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to child level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit: https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

Your data protection rights
Under data protection law, you have rights including:
- Your right of access - You have the right to ask us for copies of your personal information.
- Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances. have inaccurate personal data rectified, blocked, erased or destroyed.
- Your right to restriction of processing.
- You have the right to ask us to restrict the processing of your personal information in certain circumstances.
- Your right to object to processing - You have the the right to object to the processing of your personal information in certain circumstances.
- Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.
- You are not required to pay any charge for exercising your rights.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or if you had or continue to have concerns about the way your data is handled and remain dissatisfied after raising your concern you can contact the Information Commissioner's Office (ICO).

Helpline number: 0303 123 1113
ICO website: https://www.ico.org.uk

We keep this notice under regular review. You will be notified of any changes where appropriate.

Requesting access to your personal data
Under data protection legislation, parents and staff have the right to request access to information about them that we hold. To make a request to the manager of the setting for your personal information, or be given access to your child's educational record, contact:

Designated people

Our Data Protection Officer (the Manager) who leads is:

Our Data Protection Manager (the Area Manager) who oversees is:

The role of the Data Protection Officer (The Manager) involves:
- DPOs assist our setting to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO).
- The DPO must have the relevant experience in the given field, in data protection, be adequately resourced, and report to the highest management level (area manager or director).
- The DPO, in a timely manner, accesses support from the DPM in all issues relating to the protection of personal data.
- A DPO can be an existing employee or externally appointed.
- DPOs helps our settings demonstrate compliance and the enhanced focus on accountability.
- Our DPO is sufficiently well resourced to be able to perform their tasks.
- We do not penalise the DPO for performing their duties.
- When performing their tasks, our DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

The role of the Data Protection Manager (area manager) involves:
- Our DPM is tasked with monitoring compliance with the UK data protection laws, our data protection policies, awareness-raising, training, and audits.
- We will take account of our DPO's advice and the information they provide on our data protection obligations.
- The DPM may carry out a Data Protection Impact Assessment (DPIA), we seek the advice of our DPO who also monitors the process. A DPIA is a process to help the setting identify and minimise the data protection risks of a project.
- Our DPM acts as a contact point for the ICO. They co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter.
- When performing their tasks, our DPM has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Further guidance on the role of a Data Protection Officer can be found on the ICO website:

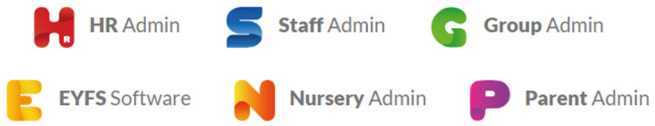
ico.
Information Commissioner's Office

Children's Records
We keep the following records on children attending our setting:

Developmental records
These may include:
- Observations of children in the setting, photographs, video clips and samples of their work and summary developmental reports.
- Any form of observation and/or assessments are usually kept on Nursery in a Box (NIAB) our secure early years management software system. Platforms we use include:
  - Group Admin
  - Nursery Admin
  - Parent Admin
- Records can also be stored in the classroom on wall displays, and can be accessed, contributed to, by staff, the child and the child's parents.

Personal records
These may include:
- Personal details – including the child's registration form and any consent forms.
- Contractual matters – including a copy of the signed parent contract, the child's days and times of attendance, a record of the child's fees, any fee reminders or records of disputes about fees.
- Child's development, health and well-being – including a summary only of the child's EYFS profile report, a record of discussions about every day matters about the child's development health and well-being with the parent.
- Early Support – including any additional focussed intervention provided by our setting (e.g. support for behaviour, language or development that needs an Individual Educational Health Care Plan) and records of any meetings held.
- Welfare and child protection concerns – including records of all welfare and protection concerns, and our resulting action, meetings and telephone conversations about the child, a Statement of Special Educational Need and any information regarding a Looked After Child.
- Correspondence and Reports – including a copy of the child's 2 Year Old Progress Check (as applicable), all letters and emails to and from other agencies and any confidential reports from other agencies.
- These confidential records are stored securely digitally or in a lockable file or cabinet, which is always locked when not in use and which our manager keeps secure in an office or other suitably safe place.
- We read any correspondence in relation to a child, note any actions and file it immediately.
- We ensure that access to children's files is restricted to those authorised to see them and make entries in them, this being our manager, deputy or designated person for child protection, the child's key person, or other staff as authorised by our manager and other staff.
- We may be required to hand children's personal files to Ofsted as part of an inspection or investigation process; or to local authority staff conducting audit, as long as authorisation is seen. We ensure that children's personal files are not handed over to anyone else to look at.
- Parents have access to the files and records of their own children, but do not have access to information about any other child.
- Our staff will not discuss personal information given by parents with other members of staff, except where it affects planning for the child's needs.
- We keep a daily record of the names of the children we are caring for, their day/ sessions and hours of attendance and the names of their key person.
- Our staff induction programme includes an awareness of the importance of confidentiality in the role of the key person.
- We retain children's records for three years after they have left the setting; except records that relate to an accident or child protection matter, which are kept until a child reaches the age of 21 years or 24 years respectively. These are kept in a secure place.

Childcare management system
We use Nursery in a Box, our chosen childcare management secure software platform, to store records.



More information about these services can be found here:
https://www.nurseryinabox.com/login/

Transfer of records to school
We recognise that children sometimes move to other early years settings before they go on to school, although many will leave our setting to enter a nursery or reception class. We prepare children for these transitions and involve parents and the receiving setting in this process. We prepare records about a child's development and learning in the EYFS in our setting; in order to enable smooth transitions we share appropriate information with the receiving setting or school at transfer. Confidential records are shared where there have been child protection concerns according to the process required by our Local Safeguarding Children Board. The procedure guides this process and determines what information we can and cannot share with a receiving school or setting.

Transfer of development records for a child moving to another early years setting or school
- Using the EYFS assessment of development and learning we ensure the key person prepares a summary of achievements in the 7 areas of learning and development.
- This record refers to any additional language spoken by the child and their progress in both languages; any additional needs that have been identified or addressed by our setting; any special needs or disability, whether a CAF was raised in respect of special needs or disability, whether there is a Statement of Special Educational Needs, and the name of the lead professional.
- The record contains a summary by the key person and a summary of the parent's view of the child.
- The document may be accompanied by other evidence, such as photos or drawings that the child has made.
- When a child transfers to a school, most local authorities provide an assessment summary format or a transition record, which we will follow as applicable.

Confidentiality
- We always check whether parents regard the information they share with us to be regarded as confidential or not.
- Some parents sometimes share information about themselves with other parents as well as staff; the setting cannot be held responsible if information is shared beyond those parents whom the person has 'confided' in.
- Information shared between parents in a discussion or training group is usually bound by a shared agreement that the information is confidential to the group and not discussed outside of it.
- As a setting we need to record confidential information beyond the general personal information which include:
  - communication via notifications.
  - accidents or incidents.
  - concerns or complaints.
  - changes in relation to the child or the family circumstance.
  - discussions with parents on sensitive matters.
  - records we are obliged to keep regarding action taken in respect of SEND / child protection.
  - contact and correspondence with external agencies in relation to their child.
- We keep all records securely.

Provider's Records

- We keep records and documentation for the purpose of maintaining our business. These include:
  - Records relating to our registration.
  - Landlord/lease documents and other contractual documentation pertaining to amenities, services and goods.
  - Financial records pertaining to income and expenditure.
  - Risk assessments.
  - Employment records of staff including their name, date of birth, home address, telephone number and email.
  - Name, address and telephone number of anyone else who is regularly in unsupervised contact with the children.

- Our records are regarded as confidential on the basis of sensitivity of information, such as with regard to employment records and these are maintained with regard to the framework of the Data Protection Act and the Human Rights Act.
- All records are the responsibility of the management team who ensure they are kept securely.
- All records are kept in an orderly way in files and filing is kept up-to-date.
- Financial records are kept up-to-date for audit purposes.
- Health and safety records are maintained; these include risk assessments, details of checks or inspections and guidance etc.
- Our Ofsted registration certificate is displayed.
- Our Public Liability insurance certificate is displayed.
- All our employment and staff records are kept securely and confidentially.

- We notify Ofsted of any change:
  - the nominated person
  - in the address of the premises;
  - to the premises which may affect the space available to us;
  - to the name and address of the provider, or, the provider's contact information;
  - to the person managing the provision;
  - any significant event which is likely to affect our suitability to look after children; or
  - any other event(s) as detailed in the Early Years Foundation Stage

Who does data protection cover in the workplace?

Data Protection information that we (the employer) might collect and keep on any individual who might wish to work, current work, or have worked for them. In the code the term 'worker' includes:

- applicants (successful and unsuccessful)
- former applicants (successful and unsuccessful)
- employees (current and former)
- agency staff (current and former)
- casual staff (current and former)
- contract staff (current and former)

Some of this code will also apply to others in the workplace, such as volunteers and those on work experience placements.

Employees Records

These may include:

- A living person (their personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.
- Identifying a person, whether by itself, or together with other information in the organisation's possession or that is likely to come into its possession. This includes personal details – including the completion of our employee registration process and any consent forms and agreements. Which may include but not limited to: name, date-of-birth, address, telephone number, email, employment history, qualifications.
- Contractual matters – including a copy of the signed contract, the days and times of attendance, a record of the qualifications, any training or records of disputes.
- Details of a worker's salary and bank account held on an organisation's computer system.
- An e-mail about an incident involving a named worker.
- A supervisor's notebook (hardcopy or digital) containing information on a worker where there is an intention to put that information in that worker's computerised personnel file.
- an individual worker's personnel file where the documents are filed in date order but there is an index to the documents at the front of the file.
- An individual worker's personnel file where at least some of the documents are filed behind sub dividers with headings such as application details, leave record and performance, supervision reviews, grievance and/or disciplinary information.
- A set of leave/ holiday records where each worker has an individual account/ data.
- A set of completed application forms, filed in alphabetical order within a file of application forms for a particular vacancy.

Sensitive Personal Records

What is sensitive data?

Sensitive data is information concerning an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- physical or mental health or condition
- sexual life
- commission or alleged commission of any offence
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

Sensitive data processed by an employer might typically be about a worker's;

- physical or mental health
  - as a part of sickness records revealed through monitoring e-mails sent by a worker to his or her manager or to an occupational health advisor
  - obtained as part of a pre-employment medical questionnaire or examination.
  - drug or alcohol test results
- criminal convictions
  - to assess suitability for certain types of employment
- disabilities
  - to facilitate adaptations in the workplace
  - to ensure special needs are catered for at interview or selection testing
  - in monitoring equality of opportunity
- racial origin
  - to ensure that recruitment processes do not discriminate against particular racial groups
  - to ensure equality of opportunity
- trade union membership
  - to enable deduction of subscriptions from payroll
  - revealed by internet access logs which show that a worker routinely accesses a particular trade union website.

Safe storage

- We keep all paper-based records about children and their families and our staff securely locked away. All digital records on our childcare management system, computers, externally or in cloud storage such as Onedrive, including but not limited to digital photos or videos are security encrypted and password protected. This also includes CCTV.
- We store the information securely, for example, in password-protected files, to prevent viewing of the information by others with access to the computer and/or system.
- Our setting uses third parties to store data cloud based, (for example: Employment HR & Payroll, Childcare Management Software). These companies have firewalls and virus protection software in place. We ensure we have carried out due diligence to ensure they are compliant with data protection.

Archiving & keeping records

- When a child or staff leaves our setting, the manager enters the official leave date onto the NIAB account. The persons personal file/ folder or account is assigned as a leaver. Our digital record system saves the data in name order.
- Leaver's data is placed in our archive, stored in a safe place for three years. Hard copies are scanned, and digital copies saved. After three years relevant data is automatically destroyed.
- It is our only intention to keep data for as long as permitted. We are required by law to keep some data for some time after a person has left the setting. We have a review plan in place and ensure that any data is disposed of appropriately and securely.
- We store financial information according to our finance procedures.
- We record all accidents and incidents on a secure password protected system. Paper copies may also be completed and kept securely in a locked place.
- We notify our insurance provider of any accidents or incidents which may result in an insurance claim, e.g. an accident resulting in a doctor or hospital visit. These details will be logged and we seek acknowledgement via receipt of the correspondence and forward the information to the company providing the public liability insurance policy to enable a claim number to be allocated (if applicable).
- We will inform Ofsted, the local child protection agency and/ or the Health and Safety Executive of any significant injuries, accidents or deaths which have happened as soon as possible.
- We record all significant incidents on a 'contact sheet' detailing the series of events (dates/ times/ people/ conversations/ descriptions/ action taken). We will share these with parents so that together we can work to resolve any issues (if applicable).
- We will only share information if it is in a child's best interests to do so. For example, in a medical emergency we will share medical information with a healthcare professional. If we are worried about a child's welfare we have a duty of care to follow the Local Safeguarding Children Board procedures and make a referral. Where possible we will discuss concerns with you before making a referral.

Suspected breach

If we suspect that data has been accessed unlawfully, we will inform the relevant parties immediately and report to the Information Commissioner's Office within 72 hours. This may by reportable to the police. We will keep a record of any data breach.

Access to records procedures

People may request access to any confidential records held on themselves, their child and their family following the procedure below:

- Any request to see a personal file by a person or parent (with parental responsibility) must be made in writing to the setting manager.
- The setting manager informs the area manager and sends a written acknowledgement.
- The setting commits to providing access within 14 days, although this may be extended.
- A mediator may be assigned to the case.
- The manager accumulates data and prepares the file for viewing.
- A legal representative may be assigned to the case.
- All third parties are written to, stating that a request for disclosure has been received and asking for their permission to disclose to the person requesting it. Copies of these letters are retained on file.
- 'Third parties' include all family members who may be referred to in the records. It also includes workers from any other agency, including social services, the health authority, etc. It is usual for agencies to refuse consent to disclose, preferring the individual to go directly to them.
- ICO or Local Authority may be contacted and advice sort.
- When all the consents/refusals to disclose have been received these are attached to the copy of the request letter.
- The area manager is assigned to go through the file and remove any information which a third party has refused consent to disclose. A black marker is used, to score through every reference to the third party and information they have added to the file.
- What remains is the information recorded by the setting, detailing the work initiated and followed by them in relation to confidential matters. This is called the 'clean copy'.

Workers' access to information about themselves

Workers, like any other individuals, have a right to gain access to information that is kept about them. This right is known as subject access. The right applies, for example, to sickness records, disciplinary or training records, appraisal or performance review notes, e-mails, word-processed documents, e-mail logs, audit trails, information held in general personnel files and interview notes, whether held as computerised files, or as structured paper records. A fee of up to £10 can be charged by the employer for giving access.

Responding to a subject access request involves:

- Telling the worker if the organisation keeps any personal information about them.
- Giving the worker a description of the type of information the organisation keeps, the purposes it is used for and the types of organisations which it may be passed on to, if any.
- Showing the worker all the information, the organisation keeps about them, explaining any codes or other unintelligible terms used.
- Providing this information in a hard copy or in readily readable, permanent electronic form unless providing it in a way would involve disproportionate effort or the worker agrees to receive it in some other way.
- Providing the worker with any additional information the organisation has as to the source of the information kept about them.

References

- The provision of a reference about a worker from one party, such as a present employer, to another, such as a prospective employer, will generally involve the disclosure of personal data. In considering how the act applies to such disclosure it is important to establish who the reference is being given by or on behalf of.
- We distinguishes between a reference given in a personal capacity and one given in a corporate capacity. A corporate reference is one given on behalf of the employer by one of its staff.
- We have rules about who can give such a reference (area - manager, manager) and what it can include. The employer remains legally responsible for compliance with the Data Protection Act.
- Under a specific exemption in the Data Protection Act, a worker does not have the right to gain access to a confidential job reference from our organisation which has given it. However, once the reference is with the organisation to which it was sent then no such specific exemption from the right of access exists. That organisation is though entitled to take steps to protect the identity of third parties such as the author of the reference.

Information sharing

We recognise that people have a right to know that information they share will be regarded as confidential as well as be informed about the circumstances, and reasons, when we are obliged to share information.

We are obliged to share confidential information without authorisation from the person who provided it, or to whom it relates, if it is in the public interest. That is when:

- It is to prevent a crime from being committed or intervene where one may have been, or to prevent harm to a child or adult.
- not sharing it could be worse than the outcome of having shared It.

The decision should never be made as an individual, but with the back-up of management. The three critical criteria are:

- Where there is evidence that the child is suffering, or is at risk of suffering, significant harm.
- Where there is reasonable cause to believe that a child may be suffering, or at risk of suffering, significant harm.
- To prevent significant harm arising to children and young people or serious harm to adults, including the prevention, detection and prosecution of serious crime.

Our procedure is based on the 7 golden rules for information sharing as set out in Information sharing advice for safeguarding practitioners (July 2018).

1. Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk.
5. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.
6. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Parents' consent

When parents choose our setting for their child, they will share information about themselves and their families. This information is regarded as confidential. Parents have a right to be informed that we will see their consent to share information in most cases, as well as the kinds of circumstances when we may not seek their consent, or may override their refusal to give consent. We inform them as follows:

- Our policies and procedures as well as our terms & conditions, set out our responsibility regarding gaining consent to share information and when it may not be sought or overridden.
- We may cover this verbally when the child starts.
- Parents sign our digital registration form to confirm that they understand this. Our Terms & conditions must be agreed prior to the child starting.
- We ask parents to give written consent to share information about any additional needs their child may have, or to pass on child development summaries to the next provider/school.
- Parents have access to digital copies of the forms they sign via their ParentAdmin app.
- We consider the following questions when we need to share:
  - Is there legitimate purpose to us sharing the information?
  - Does the information enable the person to be identified?
  - Is the information confidential?
  - If the information is confidential, do we have consent to share?
  - Is there a statutory duty or court order requiring us to share the information?
  - If consent is refused, or there are good reasons for us not to seek consent, is there sufficient public interest for us to share information?
  - If the decision is to share, are we sharing the right information in the right way?
  - Have we properly recorded our decision?

- Consent must be informed - that is the person giving consent needs to understand why information will be shared, what will be shared, who will see information, the purpose of sharing it and the implications for them of sharing that information.
- Consent may be explicit, verbally but preferably in writing (via notification), or implicit, implied if the context is such that sharing information is an intrinsic part of our service or it has been explained and agreed at the outset.
- The setting reserves the right to place a childcare place on hold or terminate if consents are not completed.
- We explain about our policies and procedures to parents when they register, and they are assessable via our website.

Separated parents' consent

- Consent to share need only be sought from one parent. Where parents are separated, this would normally be the parent with whom the child resides. Where there is a dispute, we will consider this carefully.
- The parents should consult any domestic agreements in writing with the manager which may affect the child's attendance in our care. The setting may consult to ensure all parties have agreed and authorised consent.
- The setting reserves the right to ask for proof of any form of court order or copies of birth certificates.
- The setting may refer any disrupts to the local authority or police to act as a mediator.
- Where the child is looked after, we may also need to consult the Local Authority, as 'corporate parent' before information is shared.
- All the undertakings above are subject to our paramount commitment, which is to the safety and well-being of the child. Please also see our Child Protection policies and procedures.

Retention periods for records

Records	Retention period	Status	Authority
Children's Records			
Developmental & Personal: Including registers, medication record books and accident record books pertaining to the children. Including Safeguarding, child protection, and SEND.	Up to 3 years. A reasonable period of time after children have left the provision (e.g. until after the next Ofsted inspection)	Requirement	Statutory Framework for the Early Years Foundation Stage (given legal force by Childcare Act 2006)
	Until the child reaches the age of 21 - or until the child reaches the age of 24 for child protection records	Recommendation	Data Protection Act 2018 Limitation Act 1980 Normal limitation rules (which mean that an individual can claim for negligence causing personal injury up to 3 years after, or deliberately caused personal injury up to 6 years after the event) are postponed until a child reaches 18 years of age
Records of any reportable death, injury, disease or dangerous occurrence	3 years after the date the record was made	Requirement	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (as amended)
Providers Records			
Records relating to our registration. Ofsted / HMRC / Companies House	Permanently	Requirement	Statutory Framework for the Early Years Foundation Stage (given legal force by Childcare Act 2006) Data Protection Act and the Human Rights Act.
Landlord/lease documents and other contractual documentation pertaining to amenities, services and goods.	Permanently	Requirement	Land Registry / Companies House / ICO
Accident/medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	Requirement	The Control of Substances Hazardous to Health Regulations 2002 (COSHH)
Risk Assessments Assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	Permanently	Recommendation	Chartered Institute of Personnel and Development
Accounting records	3 years from the end of the financial year for private companies, 6 years for public	Requirement	Companies Act 2006
Employers' liability insurance records	20 years For as long as possible	Recommendation	Health and Safety Executive
Director's boardroom minutes/ records / bank & accounting meetings	10 years from the date of the meeting for companies	Requirement	Companies Act 2006

Employees Records			
Employees records Personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases	Recommendation	Chartered Institute of Personnel and Development
DBS check	6 months	Recommendation	DBS Code of Practice The following basic information should be retained after the certificate is destroyed: the date of issue; the name of the subject; the type of disclosure; the position for which the disclosure was requested; the unique reference number; and the details of the recruitment decision taken
Wage/salary records (including overtime, bonuses and expenses)	6 years	Requirement	Taxes Management Act 1970
Statutory Maternity Pay (SMP) records	3 years after the end of the tax year to which they relate	Requirement	The Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay (SSP) records	3 years after the end of the tax year to which they relate	Requirement	The Statutory Sick Pay (General) Regulations 1982
Income tax and National Insurance returns/records	At least 3 years after the end of the tax year to which they relate	Requirement	The Income Tax (Employments) Regulations 1993 (as amended)
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years after employment ends	Recommendation	Chartered Institute of Personnel and Development
Staff accident records (for organisations with 10 or more employees)	3 years after the date the record was made (there are separate rules for the recording of accidents involving hazardous substances)	Requirement	Social Security (Claims and Payments) Regulations 1979