

## **13. Data Protection and Confidentiality Policy**

At La Petite Academy we recognise that we hold sensitive and confidential information about children and their families and the staff we employ. This information is used to meet children's needs, for registers, invoices and emergency contacts. We store all records in a locked cabinet or on the office computer with files that are password protected in line with data protection principles. Any information shared with the staff team is done on a 'need to know' basis and treated in confidence. This policy includes a GDPR privacy notice to ensure compliance under General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR) and Data Protection Act 2018.

### **Legal requirements**

- We follow the legal requirements set out in the Statutory Framework for the Early Years Foundation Stage (EYFS) and accompanying regulations about the information we must hold about registered children and their families and the staff working at the nursery.
- We follow the requirements of the General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR), Data Protection Act 2018 and the Freedom of Information Act 2000 with regard to the storage of data and access to it.

### **Procedures**

It is our intention to respect the privacy of children and their families, and we do so by:

- Storing confidential records in a locked filing cabinet/locked office or on the office computer with files that are password protected;
- Ensuring staff, student and volunteer inductions include an awareness of the importance of the need to protect the privacy of the children in their care as well as the legal requirements that exist to ensure that information relating to the child is handled in a way that ensures confidentiality. This includes ensuring that information about the child and family is not shared outside of the nursery other than with relevant professionals who need to know that information. It is not shared with friends and family, or part of any social discussions outside of the setting. If staff breach any confidentiality provisions, this may result in disciplinary action and, in serious cases, dismissal. Students on placement in the nursery are advised of our policy and required to respect it;

- Ensuring that all staff, volunteers and students are aware that information about children and families is confidential and only for use within the nursery and to support the child's best interests with parental permission;
- Ensuring that parents have access to files and records of their own children but not to those of any other child, other than where relevant professionals such as the police or local authority children's social care team decide this is not in the child's best interest;
- Ensuring all staff are aware that this information is confidential and only for use within the nursery setting. If any of this information is requested for whatever reason, the parent's permission will always be sought other than in the safeguarding circumstances above;
- Ensuring staff do not discuss personal information given by parents with other members of staff, except where it affects planning for the child's needs;
- Students/volunteers should not be informed of personal or safeguarding issues regarding staff or children or families where this is not directly relevant to them. Staff should check relevance with a manager prior to discussing issues with students/volunteers;
- Ensuring staff, students and volunteers are aware of and follow our Social Networking procedures in relation to confidentiality;
- Ensuring issues concerning the employment of staff remain confidential to the people directly involved with making personnel decisions;
- Where staff 'overhear' discussions of a personal nature, especially when working in the office, all information is to be treated as confidential and is not to be repeated to others;
- Ensuring that CCTV recordings are kept confidential and CCTV is viewed only within the context of the CCTV policy;
- Ensuring any concerns or evidence relating to a child's personal safety are kept in a secure, confidential file and are shared with as few people as possible on a 'need-to-know' basis. If, however, a child is considered at risk, our Safeguarding Children and Child Protection policy will override confidentiality.

All the undertakings above are subject to the paramount commitment of the nursery, which is to the safety and well-being of the child.

## **Cyber Security**

At La Petite Academy we recognise that the key to keeping our nursery cyber secure is through effective staff training so that everyone is aware of the actions they should take to protect our systems from threat.

We are actively working towards cyber essentials basic certification and have insurance to mitigate the financial, operational and reputational consequences of a cyber incident.

Good cyber security means protecting the personal or sensitive information we hold on children and their families in line with the Data Protection Act. We are aware that cyber criminals will target any type of business including childcare and ensure all staff are aware of the value of the information we hold in terms of criminal activity, e.g. scam emails. All staff are reminded to follow our procedures including backing up sensitive data, using strong passwords and protecting devices to ensure we are cyber secure.

To prevent any attempts of a data breach (i.e. when our information is stolen or accessed without authorisation) that could cause temporary shutdown of our setting and reputational damage with the families we engage with, we inform staff not to open any suspicious messages such as official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.

Staff are asked to report these to the manager as soon as possible and these will be reported through the National Cyber Security Centre (NCSC) Suspicious email reporting service at [report@phishing.gov.uk](mailto:report@phishing.gov.uk) .

## **Procedures**

### **Passwords**

We will:

- Create strong and memorable passwords for important accounts, such as by combining three random words. We will avoid using predictable passwords, such as dates, family and pet names. Passwords will not be reused. All staff must use a separate password for work and personal accounts
- Store passwords using password managers with end-to-end encryption
- Use multi-factor authorisation (MFA) to log in where appropriate, e.g. banking websites

## **Security**

We will:

- Train staff to recognise the techniques that phishers use in emails, as well as recognising spam and other harmful content
- Ensure staff know that they must report suspicious messages or links to management
- Carry out regular software updates and regularly check our back-ups
- Always lock devices when not in use
- Use PIN/password/fingerprint IDs on portable devices as appropriate
- Not install any software that has not been cleared for use by the manager onto our computers, tablets or systems
- Use unknown USBs or external devices on our systems.

## **Reporting**

- Staff are encouraged to ask for further guidance or support from the manager when something feels suspicious or unusual
- Staff are encouraged to flag concerns and must report attacks as soon as possible.

## **System access**

- Visitors are not given access to the wifi unless they are from the Local Authority or Ofsted and therefore required to adhere to their organisation's rules on safe internet use
- We regularly review system access and accounts are removed immediately when a staff member has left employment
- We limit access to the wifi for temporary workers
- Staff follow sign-in/out protocols
- No staff member has access to nursery devices outside working hours other than the manager or where a staff member has been authorised to 'sign out' a tablet where they agree to follow protocols. Tablets are checked when they are signed back in.

## **Actions in the event of a cyber attack**

- The manager will be informed immediately of any actual or suspected security breach
- We will contain the breach, isolate affected devices and disable compromised accounts
- We will avoid deleting anything that could serve as evidence

- We will keep a log of actions taken and notify the Information Commissioner's Office (ICO) if personal data is at risk (<https://ico.org.uk/for-organisations/report-a-breach/>)
- We will seek advice and guidance from the National Cyber Security Centre (NCSC) (<https://report.ncsc.gov.uk/>)
- We will communicate clearly with staff and stakeholders to explain what's happened, what we're doing and how it affects families and staff
- Following an actual or suspected attack, we will review our systems to identify what occurred, what was compromised and what changes are needed.

### **General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR) compliance**

In order to meet our requirements under GDPR we will also undertake the following:

- We will ensure our terms and conditions; privacy and consent notices are easily accessed and made available in accurate and easy to understand language;
- We will use personal data to ensure the safe, operational and regulatory requirements of running our nursery, these include maintaining your child's registration and creating invoices for you. We will only make contact in relation to the safe, operational and regulatory requirements of running our nursery, these include contacting you when your child is absent without notice and for the fulfilment of Government Funding obligations. We will not share or use personal data for other purposes;
- Everyone in our nursery understands that people have the right to access their records or have their records amended or deleted (subject to other laws and regulations);
- We will ensure staff have due regard to the relevant data protection principles, which allow them to share (and withhold) personal information, as provided for in the Data Protection Act 2018 and the GDPR. This includes:
  - Being confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'
  - Understanding that 'safeguarding of children and individuals at risk' is a processing condition that allows practitioners to share special category personal data. This includes allowing practitioners to share information without consent where there is good reason to

do so, and that the sharing of information will enhance the safeguarding of a child in a timely manner, but it is not possible to gain consent, it cannot be reasonably expected that a practitioner gains consent, or if to gain consent would place a child at risk.

### **Staff and volunteer information**

- All information and records relating to staff and volunteers will be kept confidentially in a locked cabinet in the office.
- Individual staff may request to see their own personal file at any time.

### **Access and Storage of Information**

We have an open access policy in relation to accessing information about the nursery and parents' own children. Parents are welcome to view the policies and procedures of the nursery, which govern the way in which the nursery operates. These may be viewed at any time when the nursery is open, simply by asking the nursery manager or by accessing the file in the porch or on the nursery website. The nursery manager or any other relevant staff member will also explain any policies and procedures to parents or use any other methods to make sure that parents understand these.

Parents are also welcome to see and contribute to all the records that are kept on their child. However, we must adhere to data protection laws and, where relevant, any guidance from the relevant agencies for child protection.

As we hold personal information about staff and families, we are registered under data protection law with the Information Commissioner's Office. A copy of the certificate can be viewed on the Health and Safety Noticeboard. All parent, child and staff information is stored securely according to the requirements of data protection registration, including details, permissions, certificates and photographic images. We will ensure that staff understand the need to protect the privacy of the children in their care as well as the legal requirements that exist to ensure that information relating to the child is handled in a way that ensures confidentiality.

We are required under legislation to keep certain records about children, parents and staff members. Due to this legislation, we are required to keep this information for a set amount of time, as per our record retention schedule below.

If parents have a specific deletion or retention request regarding any data that we hold, please raise a query in writing to the manager and we will respond formally to your request.

Children's records: We are advised by the local authority that they do not stipulate a timescale for retention of children's records, however these could be required to be used in conjunction with Child Protection records, therefore a retention period of up to the child becoming 25 years of age is maintained. The majority of these records will be passed onto the child's next setting/school (where known) as part of usual transition procedures. We follow the local authority protocol for transition and sharing of sensitive information.

Accidents and pre-existing (home) injuries: If relevant to child protection we will keep these until the child reaches 25 years old.

Safeguarding records and cause for concern forms: We will pass these on to the child's new educational establishment, e.g. school. In the event that we are not informed of the child's new placement, we will keep the records until the child has reached 25 years old.

Records of any reportable death, injury, disease or dangerous occurrence including fractures, broken limbs, serious head injuries or hospitalisation (for children): As these incidents could result in potential negligence claims, or evolve into a more serious health condition, we keep records until the child reaches the age of 21 years and 3 months.

Records of any reportable death, injury, disease or dangerous occurrence (for staff): 3 years.

Tapestry observations and assessment records of children: Tapestry accounts are deleted 90 days after a child has left the setting. Where they transfer to another setting also using Tapestry we will, with written parental permission, transfer their account electronically.

Personnel files and training records (including disciplinary records and working time records): 7 years.

Visitor signing in book: Up to 24 years as part of the child protection trail.

Complaints: There is an expectation that we will make our records of complaints available to Ofsted if requested. Therefore, all complaints will be kept up to at least the next Ofsted inspection (up to 6 years). In addition, where a complaint is linked to an accident/injury described above, they will be held for the same length of time as detailed in that section.

Nursery records and documentation that are not required to be kept are deleted or destroyed in line with the current data protection laws and our GDPR privacy notice below.

All records are archived at the end of each year or following an Ofsted inspection as appropriate.

### **GDPR Privacy Notice**

La Petite Academy (“we”) is committed to protecting the privacy and security of your personal information. This privacy notice describes how the nursery collects and uses personal information about employees of the nursery (“employees”), children attending the nursery (“child” or “children”) and the parents of the children (“parents”) (known collectively as “you” or “your”), in accordance with the General Data Protection Regulation (GDPR).

We are a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to employees, children and parents. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that employees, children and parents read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

All employees and parents will be required to sign a copy of this notice so that we can process their information.

## **Data protection principles**

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- Relevant to the purposes we have told you about and limited only to those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the purposes we have told you about;
- Kept securely.

## **The kind of information we hold about you**

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are “special categories” of more sensitive personal data which require a higher level of protection, such as information about a person’s health or sexual orientation.

## **Employees**

We will collect, store, and use the following categories of personal information about employees:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses;
- Date of birth;
- Gender;
- Marital status and dependants;
- Next of kin and emergency contact information;
- National Insurance number;
- Bank account details, payroll records and tax status information;
- Salary, annual leave, pension and benefits information;
- Start date and, if different, the date of an employee’s continuous employment;
- Location of employment or workplace;
- Copy of driving licence (where applicable);
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process);
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships)

- Personnel files and training records including performance information, disciplinary and grievance information, and working time records;
- Information about your use of our information and communications systems;
- Records of any reportable death, injury, disease or dangerous occurrence.

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about an employee’s race or ethnicity;
- Information about an employee’s health, including any medical condition, accident, health and sickness records, including:
  - Where an employee leaves employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;
  - Details of any absences (other than holidays) from work including time on statutory parental leave and sick leave, and;
  - Where an employee leaves employment and the reason for leaving is related to their health, information about that condition needed for pensions and permanent health insurance purposes.

## **Children**

We will collect, store, and use the following categories of personal information about children:

- Name
- Date of birth
- Home address
- Dietary requirements
- Attendance information
- Photographs and video clips of the child to signpost children to where their belongings are stored at the nursery that they attend, and also for general display purposes
- Emergency contact should parents be unavailable and the emergency contact’s contact details
- Online Learning Journey (Tapestry) for each child containing observations about the child’s development whilst at the nursery from employees of the nursery, specific examples of the child’s progress, photographs/videos demonstrating the child’s development whilst at the nursery, and personal details of the child (e.g. their date of birth)

- Records relating to individual children, e.g. care plans, common assessment frameworks, speech and language referral forms, progress reports
- Accidents and pre-existing injuries forms
- Records of any reportable death, injury, disease or dangerous occurrence
- Observation, planning and assessment records of children.

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about a child’s race or ethnicity, spoken language and nationality
- Information about a child’s health, including any medical condition, health and sickness records
- Information about a child’s accident or incident reports including reports of pre-existing injuries
- Information about a child’s incident forms, child protection referral forms and child protection case details and/or reports.

### **Parents**

We will collect, store, and use the following categories of personal information about parents:

- Name
- Home address
- Telephone numbers, and personal email addresses
- National Insurance number
- Bank account details.

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about a parent’s race or ethnicity, spoken language and nationality
- Conversations with parents where employees of the nursery deem it relevant to the prevention of radicalisation or other aspects of the governments Prevent strategy.

### **How is your personal information collected?**

#### **Employees**

We collect personal information about employees through the application and recruitment process, either directly from candidates or sometimes from an

employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of when an employee works for us.

### **Children and parents**

We collect personal information about children and parents from when the initial enquiry is made by the parents, through the enrolment process and until the children stop using the nursery's services.

### **How we will use information about you**

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract, we have entered with you
- Where we need to comply with a legal obligation
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).

### **Situations in which we will use employee personal information**

We need all the categories of information in the list above (see employee section within the paragraph entitled 'The kind of information we hold about you') primarily to allow us to perform our contracts with employees and to enable us to comply with legal obligations. The situations in which we will process employee personal information are listed below.

- Making a decision about an employee's recruitment or appointment
- Checking an employee is legally entitled to work in the UK. Paying an employee and, if an employee is an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs)
- Providing any employee benefits to employees
- Enrolling you in a pension arrangement in accordance with our statutory

automatic enrolment duties

- Liaising with the trustees or managers of a pension arrangement operated by a group company, your pension provider and any other provider of employee benefits
- Administering the contract we have entered into with an employee
- Conducting performance and/or salary reviews, managing performance and determining performance requirements
- Assessing qualifications for a particular job or task, including decisions about promotions
- Gathering evidence for possible grievance or disciplinary hearings
- Making decisions about an employee's continued employment and engagement
- Making arrangements for the termination of our working relationship
- Education, training and development requirements
- Dealing with legal disputes involving employees, including accidents at work
- Ascertaining an employee's fitness to work
- Managing sickness absence
- Complying with health and safety obligations
- To prevent fraud
- To monitor your use of our information and communication systems to ensure compliance with our Use of Technology and Internet policy
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of an employee's personal information.

### **Situations in which the nursery will use personal information of children**

We need all the categories of information in the list above (see children section within the paragraph entitled 'The kind of information we hold about you') primarily to allow us to perform our obligations (including our legal obligations to children). The situations in which we will process personal information of children are listed below.

- Upon consent from the parents, personal data of children will be shared with schools for progression into the next stage of their education
- Personal information of children will be shared with local authorities

without the consent of parents where there is a situation where child protection is necessary

- The personal information of children will be shared with local authorities without the consent of parents for funding purposes
- Ofsted will be allowed access to the nursery's systems to review child protection records
- To ensure we meet the needs of the children
- To enable the appropriate funding to be received
- Report on a child's progress whilst with the nursery
- To check safeguarding records
- To check complaint records
- To check attendance patterns are recorded
- When a child's progress report is given to his/her parent in order for that parent to pass the same progress report to a school for application or enrolment purposes.

### **Situations in which the nursery will use personal information of parents**

We need all the categories of information in the list above (see parents' section within the paragraph entitled 'The kind of information we hold about you') primarily to allow us to perform our contracts with parents and to enable us to comply with legal obligations. The situations in which we will process personal information of parents are listed below.

- The personal information of parents will be shared with local authorities without the consent of parents for funding purposes
- To report on a child's attendance
- To be able to contact a parent or a child's emergency contact about their child
- To ensure nursery fees are paid and to enable collection of any such outstanding fees.

### **If employees and parents fail to provide personal information**

If employees and parents fail to provide certain information when requested, we may not be able to perform the respective contracts we have entered into with employees and parents, or we may be prevented from complying with our respective legal obligations to employees, children and parents. Withholding certain information may mean that we must terminate our contract with you.

### **Change of purpose**

We will only use your personal information for the purposes for which we

collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify the employee, child or parent, as is appropriate in the circumstances, and we will explain the legal basis which allows us to do so.

Please note that we may process an employee's, a child's or a parent's personal information without their respective knowledge or consent, as relevant to the circumstances, in compliance with the above rules, where this is required or permitted by law.

### **How we use particularly sensitive personal information**

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with employee or parent explicit written consent
- Where we need to carry out our legal obligations or exercise rights in connection with employee employment
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect an employee, a child or a parents' interests (or someone else's interests) and the employee, child or parent as is appropriate is not capable of giving consent, or where the employee or parent has already made the information public.

### **The nursery's obligations as an employer**

We will use particularly sensitive personal information of employees in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws
- We will use information about the physical or mental health of an employee, or their disability status, to ensure employee health and safety in the workplace and to assess the fitness of employees to work, to

provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance

- We will use information about an employee's race or national or ethnic origin, religious, philosophical or moral beliefs, or an employee's sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

### **Do we need employee consent?**

We do not need the consent of employees if we use special categories of personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law.

In limited circumstances, we may approach employees for their written consent to allow us to process certain particularly sensitive data. If we do so, we will provide employees with full details of the information that we would like and the reason we need it, so that employees can carefully consider whether they wish to consent. Employees should be aware that it is not a condition of their contract with the nursery that they agree to any request for consent from us.

### **Information about criminal convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our Data Protection and Confidentiality policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect the interests of you (or someone else's interests) and you are not capable of giving your consent, or where an employee or a parent, as is relevant to the circumstances, has already made the information public.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so, which includes but is not limited to Disclosure and Barring Service ("DBS") checks. Where appropriate, we will collect information about criminal convictions as part of the recruitment process, or we may be notified of such information

directly by you in the course of you working for us.

We will use information about criminal convictions and offences in the following ways:

- To conduct a DBS, check on each employee, to record the date of the DBS check, the number of the DBS check and the name of the body conducting the DBS check.

We are allowed to use your personal information in this way to carry out our obligations.

We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

### **Automated decision-making**

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified employees or parents of the decision and given the employee or the parent as is appropriate 21 days to request a reconsideration
- Where it is necessary to perform the contract with an employee or a parent and appropriate measures are in place to safeguard the employee's, the child's or the parent's rights as is appropriate
- In limited circumstances, with explicit written consent from the employee or the parent, as is appropriate, and where appropriate measures are in place to safeguard employee or parent rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either explicit written consent from an employee or a parent as is appropriate, or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard an employee's or a parent's rights as is relevant in the circumstances.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified the employee, or the parent as is appropriate in the circumstances.

### **Data sharing**

We may have to share employee, child or parent data with third parties,

including third-party service providers and other entities in the group. We require third parties to respect the security of your data and to treat it in accordance with the law.

**Why might the nursery share employee, child or parent personal information with third parties?**

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

**Which third-party service providers process my personal information?**

“Third parties” includes third-party service providers (including contractors and designated agents), local authorities, regulatory bodies, schools and other entities within our group. The following third-party service providers process personal information about you for the following purposes:

- Local Authorities – for funding and monitoring reasons (e.g. equal opportunities and uptake of funded hours)
- Regulatory bodies – for ensuring compliance and the safety and welfare of the children
- Schools – to provide a successful transition by ensuring information about the child’s progress and current level of development and interests are shared.

We will share personal data regarding your participation in any pension arrangement operated by a group company with the trustees or scheme managers of the arrangement in connection with the administration of the arrangements.

**How secure is my information with third-party service providers and other entities in our group?**

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

**When might you share my personal information with other entities in the group?**

We will share your personal information with other entities in our group as part of our provision of Health Care to employees or with our HR company.

### **What about other third parties?**

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, as far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties, if and to the extent required, under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law.

### **Data retention**

#### **How long will you use my information for?**

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available from the manager. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Once you are no longer an employee, or a child benefiting from the nursery's services or a parent, as is appropriate, we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

### **Rights of access, correction, erasure, and restriction**

#### **Your duty to inform us of changes**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

#### **Your rights in connection with personal information**

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected
- **Request erasure** of your personal information. This enables employees or parents to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below)
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes
- **Request the restriction of processing** of your personal information. This enables employees or parents, as is appropriate, to ask us to suspend the processing of personal information about you for example if you want us to establish its accuracy or the reason for processing it
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the manager in writing.

### **No fee usually required**

You will not have to pay a fee to access your personal information (or to exercise any of the other rights).

### **What we may need from you**

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

**Right to withdraw consent**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact Carol Daly (Manager). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

**Changes to this privacy notice**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

**If you have any questions about this privacy notice, please contact Carol Daly (Manager).**

I, \_\_\_\_\_  
(employee/parent),

acknowledge that on \_\_\_\_\_ (date), I received a copy of the nursery’s privacy notice for employees, children and parents and that I have read and understood it.

Signature.....

Name .....

This policy will be reviewed annually and amended according to any change in law and/or legislation. Where legislation changes this will take precedent over the contents of this policy.

<b>This policy was adopted on</b>	<b>Signed on behalf of the nursery</b>	<b>Date for review</b>
02/04/26	<i>Jodie Hursthouse</i>	30/04/2027

