

Privacy Notice

Children, parents and carers, staff, applicants, volunteers, visitors and other members of our nursery community

Tadpoles Nursery Group Ltd
Company number 13369282
Registered office: 34 Holland Road, London NW10 5AU

Our settings

Setting	Address	Ofsted URN
Chelsea	Park Walk Play Centre, Park Walk, London SW10 0AY	2705358
Kensington	The Studio, 8 Hornton Place, London W8 4LZ	2697963

Data Protection Officer

Francesca Short is our formally appointed Data Protection Officer (DPO). Contact her through the nursery office at francescashort@tadpolesnursery.com, by telephone on 020 7352 9757, or by post at the registered office above.

This notice replaces the previous 2018 wording. It is written to reflect the UK GDPR and the Data Protection Act 2018, as amended including by the Data (Use and Access) Act 2025, together with PECR where relevant.

Version 2.0 | Effective and last reviewed: 28 August 2026 | Next review: August 2027, or sooner if our processing changes

1. About this notice

Tadpoles Nursery Group Ltd is the data controller for the personal data described in this notice. This means we decide why and how it is used. This notice explains what we collect, why we use it, who we share it with, how long we keep it, and the rights available to individuals.

It applies to current, former and prospective children; their parents, carers and guardians; staff, workers, applicants and volunteers; visitors; suppliers; and other people whose personal data we process. Where a child is able to understand and exercise their rights, those rights belong to the child. A parent or guardian may help or act for a child where appropriate.

We provide this information when data is collected and make it available through the nursery office and website. More specific notices may also apply, for example a CCTV sign, recruitment notice, staff notice, biometric notice or cookie notice. If there is a conflict, the more specific notice applies to that processing.

2. Personal data we collect

- Identity and contact details, including names, addresses, dates of birth, telephone numbers, email addresses, emergency contacts and family relationships.
- Admissions, waiting-list, enrolment, attendance, collection permissions and contractual records.
- Learning and development observations, assessments, progress records, photographs and learning-journal entries.
- Health, allergy, medication, disability, special educational needs and/or disabilities (SEND), dietary and welfare information.
- Safeguarding, child-protection, incident, accident, complaint and behaviour records.
- Images and audio/video where used, including CCTV footage.
- Staff biometric identifiers or templates used for access and/or attendance.
- Staff, applicant and volunteer records, including qualifications, references, right-to-work, DBS-related information, absence, performance, payroll, pension and next-of-kin details.
- Fees, invoices, amounts, dates, payer names or references and reconciliation records. Parents pay by BACS. We do not retain parents' bank-account details.
- Website and technical data, including IP address, device/browser data, form submissions and cookie preferences.
- Correspondence, enquiries, complaints, consent choices and records of how rights requests are handled.

Special-category and criminal-offence data

Some information is more sensitive, including health, racial or ethnic origin, religious or philosophical beliefs, trade-union membership, sex life or sexual orientation, and biometric data used for unique identification. Criminal-offence data includes information connected with alleged or proven offences and DBS checks. We process these categories only when both an Article 6 lawful basis and an Article 9 condition (or the relevant DPA 2018 condition for criminal-offence data) apply. Where required, we maintain an Appropriate Policy Document.

3. Why we use personal data and our lawful bases

The lawful basis depends on the purpose and circumstances. We do not use consent where another basis is more appropriate, and withdrawing consent does not affect processing already carried out lawfully.

Activity	Purposes	Lawful basis / special-category condition
Admissions and childcare	Assess enquiries and applications; offer and administer places; provide early-years education and care; manage attendance and collection arrangements.	Steps before entering a contract; contract; legal obligation; legitimate interests in operating the nursery.
Learning and development	Plan, record and share learning, development and progress, including through ARC Pathway.	Contract; legal obligation under applicable early-years requirements; legitimate interests in providing and improving education.
Safeguarding, health and welfare	Protect children and others; manage allergies, medication, SEND, accidents, incidents, emergencies and referrals.	Legal obligation; vital interests; legitimate interests. Article 9: substantial public interest/social protection, vital interests, health or social care, legal claims, or explicit consent where appropriate.
Communications	Communicate with families, staff and others about attendance, activities, administration, emergencies, changes and services.	Contract; legal obligation; legitimate interests in effective nursery administration.
Staff and volunteers	Recruit, employ, schedule, train, safeguard, pay and manage staff, workers and volunteers.	Steps before contract; contract; legal obligation; legitimate interests. Article 9 employment/social-protection conditions and other applicable conditions.
Fees and accounting	Issue invoices, receive BACS payments, reconcile fees, maintain accounts, prevent fraud and meet tax requirements.	Contract; legal obligation; legitimate interests in financial administration and fraud prevention.
Security and claims	Secure premises and systems, prevent or investigate incidents, respond to complaints and establish, exercise or defend legal claims.	Legitimate interests; legal obligation; vital interests where necessary.
Regulation	Meet obligations to Ofsted, HMRC, DfE, local authorities, law enforcement and other competent bodies.	Legal obligation; legitimate interests; substantial public interest where relevant.
Website	Operate our Wix website, answer enquiries, maintain security and measure/use non-essential features where chosen.	Legitimate interests for essential operation/security; consent for non-essential cookies or similar technology under PECR.

Our legitimate interests include providing safe and effective early-years education, administering the organisation, maintaining security and business continuity, communicating appropriately, improving services, preventing misuse and defending legal rights. We balance these interests against individuals' rights, with particular care for children.

4. CCTV

We use CCTV at our premises for site security, safety and safeguarding, and to help prevent, detect and investigate incidents or suspected crime. Our usual lawful basis is our legitimate interests in keeping children, staff, visitors and property safe. Legal obligations or vital interests may also apply in particular cases.

- Clear signs identify monitored areas. Cameras must not be used in places where people reasonably expect a high level of privacy.
- Access is limited to authorised people with a need to know. Footage may be disclosed to police, safeguarding bodies, insurers, legal advisers or affected individuals when lawful and proportionate.
- Routine footage is retained for 30 days and then overwritten or securely deleted. A relevant extract may be kept longer where needed for an incident, investigation, safeguarding concern, complaint or legal claim.
- A person may request footage containing their personal data. We may need identification, timing and location details, and may redact or withhold third-party images where the law requires.

5. Staff biometrics

We use biometric recognition for staff access and/or attendance. When a biometric template is used to uniquely identify a person, it is special-category personal data. We must identify both an Article 6 lawful basis and a separate Article 9 condition before using it.

Biometric use must be necessary and proportionate, supported by a Data Protection Impact Assessment (DPIA), and kept under review.

Staff have a genuine non-biometric alternative: they may enter using keys and the intercom system. Where we rely on explicit consent, staff may withdraw it without disadvantage.

- We use the minimum biometric information needed and restrict access to authorised personnel and contracted system providers.
- Biometric access is not the only way to enter the premises; authorised staff may use keys and the intercom system instead.
- Biometric templates are retained only while the staff member is authorised and the access/attendance purpose continues, then deleted promptly, subject to secure backup-overwrite cycles.
- Raw biometric images should not be retained where the system can operate using a protected template. Attendance records generated by the system may be kept separately under the workforce retention schedule.
- The DPO can provide information about the technology used, the lawful basis and Article 9 condition, the DPIA, alternatives and retention controls.

6. Where personal data comes from

We obtain personal data directly from the individual and, for children, from parents or carers. We may also receive it from previous or future education settings, local authorities, Ofsted, health and safeguarding professionals, emergency services, referees, employers, DBS-related channels, our systems and service providers, CCTV, website interactions, or public sources where lawful.

Some information is required by law or under a contract, or is necessary before a contract can be made. If required information is not provided, we may be unable to offer or safely provide a place, meet safeguarding duties, administer employment or payment, or provide a requested service. We explain when providing information is optional.

7. Who we share personal data with

We share only what is necessary, using role-based access and confidentiality controls. Depending on their role and legal obligations, a recipient may act as our processor, a separate controller, or both. We do not sell personal data.

Recipient/category	Reason for sharing
ARC Pathway	Digital learning journal used to record and share children's learning and development observations, assessments and progress records.
Apple iCloud	Cloud storage, synchronisation and backup used for authorised nursery information and devices.
Xero	Accounting, invoices, payment reconciliation and financial records.
Owadally & King (O&K)	External accountants providing payroll and related accounting services.
Wix	Website hosting and systems, website forms, security, analytics and cookies in line with our cookie settings and notice.
Banks and BACS services	Receiving and reconciling fee payments. We do not retain parents' bank-account details, although transaction references and payer names may appear in payment records.
Public and safeguarding bodies	Ofsted, HMRC, DfE where applicable, local authorities, LADO, police, social care, health professionals, emergency services and courts where required or permitted by law.
Professional and operational providers	Insurers, lawyers, auditors, pension providers, occupational health, IT/security support, hosting, communications and other suppliers where necessary.
Other education settings	Transfer of relevant education or safeguarding information when a child moves, where required or appropriate.

We require processors to use personal data only on documented instructions, keep it secure, help us meet data-protection obligations and delete or return it at the end of the service, subject to lawful retention. We carry out proportionate supplier due diligence and put data-processing terms in place.

8. International transfers

Some technology suppliers, including Apple, Xero and Wix and their approved service providers, may process or support personal data outside the UK. Where a transfer is restricted by UK data-protection law, we use a lawful transfer mechanism, such as UK adequacy regulations, the UK International Data Transfer Agreement or the UK Addendum to approved standard contractual clauses, together with a transfer risk assessment and additional safeguards where required. Contact the DPO for information about the safeguards relevant to a particular supplier.

9. Retention and secure disposal

We keep personal data only for as long as necessary for the purpose for which it was collected, to meet legal or regulatory duties and to establish, exercise or defend legal claims. Retention is determined by record type, not simply by the system in which it is stored.

Record	Retention
Relevant Ofsted and regulatory records	Seven years under Tadpoles' adopted retention arrangements, unless a longer period is required for an active matter or by law.
Safeguarding and child-protection records	Until the child's 25th birthday. A file relating to child sexual abuse is retained until the child's 75th birthday. Records may be transferred securely to a new setting where required.
CCTV	30 days for routine footage; longer only for an identified incident, investigation, safeguarding matter, complaint or legal claim.
Staff biometric templates	Only while the staff member is authorised and the access/attendance purpose continues; delete promptly when no longer required, subject to secure backup-overwrite cycles.
Learning-journal, cloud and website data	According to the underlying record type and purpose. Use of ARC Pathway, iCloud or Wix does not extend the applicable retention period.
Accounting, payment and payroll records	For the period required by tax, accounting, employment and legal-claims requirements under the detailed retention schedule. Xero or O&K use does not extend that period.
Recruitment and workforce records	According to the workforce retention schedule, taking account of recruitment, employment, safeguarding, tax, pension and legal-claims requirements.
Complaints, rights and consent records	For as long as needed to deal with the matter, demonstrate compliance and meet applicable limitation periods.

At the end of the relevant period, records are securely deleted, destroyed or irreversibly anonymised. A legal hold or active safeguarding, regulatory, complaint or litigation matter may require longer retention. Retention decisions and exceptions are documented.

10. Security

We use proportionate technical and organisational measures to protect personal data. These include access controls, staff confidentiality and training, secure devices and accounts, appropriate authentication, encrypted transmission/storage where supported, backups, incident procedures, supplier contracts and periodic review. No system is completely risk-free; suspected personal-data breaches must be reported promptly to the DPO for assessment and, where required, notification to the ICO and affected individuals.

11. Your data-protection rights

Depending on the circumstances, an individual may have the right to:

- Be informed about how personal data is used.
- Request access to personal data and receive a copy.
- Have inaccurate or incomplete data corrected.
- Request erasure where the law permits.
- Request restriction of processing.
- Object to processing based on legitimate interests or to direct marketing.
- Receive certain data in a portable format where the right applies.
- Withdraw consent at any time where consent is relied on, without affecting earlier lawful processing.
- Seek human review and safeguards for a solely automated decision with a legal or similarly significant effect, if such processing is used.

These rights are not absolute. For example, safeguarding, legal obligations, third-party rights or legal claims may limit what we can erase or disclose. We normally respond within one calendar month after receiving the information needed to verify identity and understand the request. We do not usually charge a fee.

For a child, we consider the child's age, maturity and ability to understand the request, the person with parental responsibility, the child's best interests and any safeguarding concerns. Information provided to children will be made age-appropriate where practical.

12. Questions, rights requests and complaints

Contact Francesca Short, DPO, at francescashort@tadpolesnursery.com, telephone 020 7352 9757, or by post at 34 Holland Road, London NW10 5AU. Please state that the matter is a data-protection request or complaint.

We provide a clear way to complain, acknowledge a data-protection complaint within 30 days, take appropriate steps to investigate without undue delay, keep the complainant informed and communicate the outcome.

You may also complain to the Information Commissioner's Office (ICO), the UK supervisory authority. Visit ico.org.uk/make-a-complaint or call 0303 123 1113. We ask that you contact us first where possible so we can try to resolve the concern, but this does not remove the right to approach the ICO.

13. Changes to this notice

We review this notice at least annually and when our services, suppliers, systems or legal obligations change. Material changes will be brought to the attention of affected people in an appropriate way. The current version will be available from the nursery office and website.

Controller: Tadpoles Nursery Group Ltd (company number 13369282)

DPO: Francesca Short | francescashort@tadpolesnursery.com | 020 7352 9757

Last reviewed: 28 August 2026 | Next scheduled review: August 2027