Data Protection Policy

POLICY STATEMENT

Vishenka Nursery is committed to the protection of all personal and special category data for which it holds responsibility as the Data Controller, and to handling that data in line with the data protection principles and the Data Protection Act 2018.

This policy applies to all personal data the nursery processes, whether relating to children, parents/carers, staff, volunteers, contractors or applicants. The requirements of this policy are mandatory for all staff employed by the nursery and for any third party contracted to provide services within the nursery.

LEGAL AND STATUTORY FRAMEWORK

This policy is written and implemented in line with:

The **Data Protection Act 2018**.
The **UK General Data Protection Regulation** , as retained and amended in UK law.
The **Data Act 2025**, which amends UK GDPR and the Data Protection Act 2018 and introduces, among other things, a requirement for data subjects to be able to complain directly to a controller and to receive a response within 30 days.
ICO guidance on data protection principles, transparency, security and children's information.
The **Statutory Framework for the Early Years Foundation Stage** , in force from **1 September 2026**, and the record-keeping requirements it places on early years providers.
The setting's **Safeguarding and Child Protection Policy**,**Admission Policy**, **Effective Transition Policy**, **Behaviour Management Policy**, **Equality and Inclusion Policy** and**Screen Use Policy**, which should be read alongside this policy.

Changes to data protection legislation shall be monitored and implemented in order to remain compliant with all requirements. This policy is reviewed on any change to data protection legislation, or every two years, whichever is sooner.

OUR COMMITMENT

The members of staff responsible for data protection are:

Name	Role
Tatiana Henderson Stewart	Director — overall responsibility and data protection contact
Anastasia Trunova	Nursery Administrator — day-to-day records and requests
Luchia Vanyatynska	Nursery Manager — operational compliance

All staff must treat all child and family information in a confidential manner and follow the guidelines set out in this document.

The nursery is committed to ensuring that its staff are aware of data protection policies and legal requirements, and adequate training is provided through annual training sessions to ensure compliance. All staff receive updated training on digital data security, including the safe use of nursery systems, online platforms, and password management protocols.

Data protection contact: enquiries, requests and complaints about data protection should be addressed to Tatiana Henderson Stewart, Vishenka Nursery, 137A St Mark's Road, W10 6BZ London, or by email to clubs@lpebl.com.

LAWFUL BASES FOR PROCESSING

We process personal data only where we have a lawful basis to do so. The lawful bases we rely on are:

Basis	How it applies at Vishenka
Consent	Where a parent/carer or member of staff has given clear consent for the nursery to process their personal data for a specific purpose, for example photographs and video, or sharing information with an external agency.
Contract	Where processing is necessary for a member of staff's employment contract or a child's placement contract.
Legal obligation	Where processing is necessary for the nursery to comply with the law, for example safeguarding, health and safety, and EYFS record-keeping requirements.
Vital interests	Where processing is necessary to protect someone's life, for example in a medical emergency.
Public task	Where processing is necessary for the performance of a task in the public interest, including our duties as an Ofsted-registered early years provider.
Legitimate interests	Where processing is necessary for our legitimate interests or those of a third party, and these are not overridden by the rights of the individual.

Where we rely on consent, it may be withdrawn at any time. Withdrawing consent does not affect the lawfulness of processing carried out before withdrawal.

NOTIFICATION AND REGISTRATION

Our data processing activities are registered with the**Information Commissioner's Office** as a recognised Data Controller. Details are available from the ICO register of data controllers.

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

PERSONAL AND SPECIAL CATEGORY DATA

All data within the nursery's control shall be identified as personal, special category, or both, to ensure that it is handled in compliance with legal requirements and that access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and special category data are as stated in Chapter 1, Article 4 of the **Data Protection Act 2018** and the **UK GDPR**.

Special category data we hold includes information about a child's health, medical conditions, allergies, dietary requirements, additional needs and SEND, ethnicity, and any safeguarding information. This data is processed only where an additional condition under Article 9 UK GDPR is met, most commonly explicit consent, vital interests, or a substantial public interest such as safeguarding.

DATA PROTECTION PRINCIPLES

The principles of the Data Protection Act shall be applied to all data processed:

Ensure that data is fairly and lawfully processed.
Process data only for limited purposes.
Ensure that all data processed is adequate, relevant and not excessive.
Ensure that data processed is accurate.
Not keep data longer than is necessary.
Process the data in accordance with the data subject's rights.
Ensure that data is secure.
Ensure that data is not transferred to other countries without adequate protection, unless specific safeguards or contractual clauses are in place.

FAIR PROCESSING AND PRIVACY NOTICE

We are transparent about the intended processing of data and communicate these intentions by notification to staff, parents/carers and children before processing an individual's data.

Notifications are in accordance with **ICO guidance on transparency** and, where relevant, are written in a form understandable by those defined as "children" under the legislation. Where we operate services likely to be accessed by children, we have regard to the **ICO's Children's Code**and apply age-appropriate design to those services.

There may be circumstances where the nursery is required, either by law or in the best interests of our children or staff, to pass information to external authorities, for example local authorities, Ofsted, or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data they receive or collect.

The intention to share data relating to individuals with an organisation outside our nursery shall be clearly defined within notifications, and details of the basis for sharing given. Data will be shared with external parties where it is a legal requirement to provide such information.

We will ensure that parents/carers and staff are informed of any updates to data-sharing agreements, particularly where data is shared with third-party digital platforms or software used in the nursery. A list of the third-party processors we use is available from the nursery office on request, and we hold a written data processing agreement with each processor.

Any proposed change to the processing of an individual's data shall first be notified to them. Under no circumstances will the nursery disclose information or data:

that would cause serious harm to the child's or anyone else's physical or mental health or condition;
indicating that the child is or has been subject to child abuse, or may be at risk of it, where the disclosure would not be in the best interests of the child;
recorded by the child in an examination;
that would allow another person to be identified, or identifies another person as the source, unless that person is an employee of the nursery or a local authority, or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed;
in the form of a reference given to another nursery or any other place of education and training, the child's potential employer, or any national body concerned with child admissions, without the parents' consent.

DATA SECURITY

In order to assure the protection of all data being processed and inform decisions on processing activities, we undertake an assessment of the associated risks of proposed processing and the impact on an individual's privacy in holding data related to them.

Risk and impact assessments are conducted in accordance with guidance given by the ICO: **A guide to the data protection principles** and **Data protection impact assessments**.

Data protection impact assessments will be reviewed annually to ensure ongoing compliance with data protection requirements, and a DPIA will be carried out before any processing likely to result in a high risk to individuals, including any new system involving children's data.

Security of data is achieved through the implementation of proportionate physical and technical measures. Nominated staff are responsible for the effectiveness of the controls implemented and for reporting on their performance.

The security arrangements of any organisation with which data is shared shall also be considered, and where required those organisations shall provide evidence of their competence in the security of shared data.

Staff guidelines

Paper copies of data or personal information should not be taken off the nursery site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy off site, the information should not be on view in public places or left unattended under any circumstances.
Unwanted paper copies of data, sensitive information or children's files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or child by name.
Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
If information is being viewed on a PC, staff must ensure that windows and documents are properly closed before leaving the computer unattended. Sensitive information should not be viewed on public computers.
Where data must be accessed away from the nursery, staff should use the nursery's encrypted, access-controlled cloud storage with multi-factor authentication.
Personal USB sticks and personal email accounts must not be used to store or transfer nursery data.
Any device used for accessing nursery data must have up-to-date antivirus software and encryption protocols in place.
Passwords must be strong and unique to the nursery's systems, and must not be shared between staff.

These guidelines are clearly communicated to all nursery staff, and any person found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

INTERNATIONAL TRANSFERS

We do not transfer personal data outside the UK unless adequate protection is in place. Where a transfer is necessary — for example where we use software hosted outside the UK — we rely on one of the following mechanisms:

UK adequacy regulations, where the destination country or territory is covered by an adequacy finding;
the **International Data Transfer Agreement** or the UK Addendum to the EU Standard Contractual Clauses;
a relevant exemption under UK GDPR.

We record the transfer mechanism for each processor in our record of processing activities.

DATA RETENTION

We keep personal data only for as long as it is needed for the purpose it was collected. Our retention periods are:

Record type	Retention period
Child's general records	Until the child's 21st birthday
Safeguarding and child protection records	Until the child's 21st birthday, or longer where required by the Local Authority
Accident, incident and medication records	3 years after the record is created, or until the child's 21st birthday where linked to safeguarding
Two-year-old progress check and EYFS profile records	Until the child's 21st birthday
Staff employment records	6 years after the end of employment
Recruitment records for unsuccessful applicants	6 months after the decision
Financial and fee records	6 years
Photographs and video, where consent has been given	Until consent is withdrawn, or until the child leaves the setting and consent is not renewed

When a retention period ends, data is securely destroyed in line with the Data Disposal section of this policy.

DATA ACCESS REQUESTS

All individuals whose data is held by us have a legal right to request access to that data, or information about what is held. Requests should be made in writing to Tatiana Henderson Stewart, Vishenka Nursery, 137A St Mark's Road, W10 6BZ London, or by email to clubs@lpebl.com.

We will respond to such requests **within one month** of receipt. Where a request is complex, we may extend this by a further two months and will tell you if we do. No charge will be applied to process a request.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless obliged by law or in the best interests of the child. Data may be disclosed to the following third parties without consent:

Other nurseries

If a child transfers from Vishenka Nursery to another nursery, their records and other data relating to their health and welfare will be forwarded to the new nursery. This supports a smooth transition from one setting to the next and ensures the child is provided for as necessary. It aids continuity and should ensure minimal impact on the child's progress as a result of the move.

Examination authorities

This may be for registration purposes, to allow children at our nursery to sit examinations set by external exam bodies.

Health authorities

As obliged under health legislation, the nursery may pass on information regarding the health of children in the nursery to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts

If a criminal investigation is being carried out, we may have to forward information to the police to aid their investigation. We will pass information to courts as and when ordered.

Social workers and support agencies

In order to protect or maintain the welfare of our children, and in cases of child abuse, it may be necessary to pass personal data to social workers or support agencies.

Educational division

Nurseries may be required to pass data on in order to help the government monitor the national educational system and enforce laws relating to education.

Right to erasure

Where personal data is no longer required for its original purpose, an individual can ask that processing is stopped and that their personal data is erased by the nursery, including any data held by contracted processors. This right is not absolute: we may need to retain data where we have a legal obligation to do so, for example safeguarding records or financial records.

COMPLAINTS

Under the Data Act 2025, individuals have the right to complain directly to the nursery about how we have handled their personal data. Complaints should be sent in writing to the data protection contact named above.

We will acknowledge your complaint promptly and provide a substantive response **within 30 days**.
If you are not satisfied with our response, you may escalate the matter to the Headteacher, and then to the **Information Commissioner's Office**.

We log all complaints, our responses and any remedial action taken, and review them annually.

DATA BREACHES

A personal data breach is a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In the event of a breach, the following steps apply:

Contain and assess. Staff must report any suspected breach immediately to the data protection contact. We contain the breach and assess the risk to the rights and freedoms of the individuals affected.
Notify the ICO within 72 hours of becoming aware of the breach, where it is likely to result in a risk to the rights and freedoms of individuals.
Notify affected individuals without undue delay, where the breach is likely to result in a **high risk** to their rights and freedoms. There is no 72-hour deadline for notifying individuals; the requirement is that they are told without undue delay.
Record the breach in our breach log, whether or not it is reportable, including the facts, its effects, and the remedial action taken.

We review all breaches to identify lessons learned and to prevent recurrence.

PHOTOGRAPHS AND VIDEO

Images of staff and children may be captured at appropriate times and as part of educational activities, for use within the nursery only.

Parents/carers are given annual opportunities to review and update their consent preferences for photographs and videos. Consent is voluntary and is not a condition of a child's place, and it may be withdrawn at any time.

Unless prior consent from parents/carers or staff has been given, the nursery shall not use such images for publication or communication to external sources.

It is the nursery's policy that external parties may not capture images of staff or children during such activities without prior consent.

Screen use at the nursery is governed by our **Screen Use Policy**, which should be read alongside this policy.

LOCATION OF INFORMATION AND DATA

Hard copy data, records and personal information are stored out of sight and in a locked cupboard. The only exception is medical information that may require immediate access during the nursery day. This is stored with the nursery files but accessible to the first aider.

Sensitive or personal information and data should not be removed from the nursery site. However, the nursery acknowledges that some staff may need to access data away from the nursery in order to work in the evenings and at weekends, or when attending offsite meetings or nursery visits with children. In these cases, data is accessed through the nursery's encrypted, access-controlled cloud storage with multi-factor authentication, and the staff guidelines in the Data Security section apply.

DATA DISPOSAL

The nursery recognises that the secure disposal of redundant data is an integral element of compliance with legal requirements and an area of increased risk.

All data held in any form of media shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of data shall be logged, with clear records maintained to demonstrate compliance with data protection requirements.

Disposal of IT assets holding data shall be in compliance with **ICO guidance on IT asset disposal**.

The nursery has identified a qualified source for the disposal of IT assets and collections. The nursery also uses **Shred-it**to dispose of sensitive data that is no longer required.

ROLES AND RESPONSIBILITIES

Role	Responsibility
Headteacher	Acts as the data protection contact, ensures this policy is implemented and reviewed, and handles escalated complaints and subject access requests.
Nursery Manager	Ensures day-to-day compliance, supports staff training, and reports concerns to the Headteacher.
Nursery Administrator	Maintains records, processes subject access requests and consent records, and manages the retention schedule.
All staff	Follow the guidelines in this policy, report suspected breaches immediately, and complete annual data protection training.
Contracted third parties	Process data only on our written instructions and under a data processing agreement.

MONITORING AND REVIEW

This policy is monitored by the Director and reviewed on any change to data protection legislation, or every two years, whichever is sooner. The next scheduled review is **October 2028**.