# Data Protection, Confidentiality and Information Sharing Policy

**Policy status:** Statutory / Operational

**Effective from:** September 2026

**Review date:** September 2027, or earlier if legislation or statutory guidance changes

**Applies to:** All children, parents/carers, staff, agency staff, students, apprentices, volunteers, contractors and visitors

**Related policies:** Safeguarding and Child Protection, Complaints, Whistleblowing, Safe Recruitment, SEND and Inclusion, Social Media, Health and Safety, Records Retention, Privacy Notice and Staff Code of Conduct

## Policy Statement

At St.Nicholas Nursery , we recognise that we collect, use and hold personal and confidential information about children, parents/carers, families, staff, students, volunteers and other individuals.

This information is essential to enable us to:

- safeguard and promote children's welfare;
- meet children's individual care, learning, development and SEND needs;
- maintain accurate attendance and registration records;
- administer funding, fees and contracts;
- maintain emergency contact information;
- manage children's health, allergies, dietary and medication requirements;
- communicate effectively with parents and carers;
- fulfil our statutory and regulatory responsibilities;
- work with appropriate external agencies and professionals;
- manage staff employment and safeguarding records; and
- monitor and improve the quality and safety of our provision.

St.Nicholas Nursery is committed to protecting personal information and respecting the privacy of children, families and staff.

However, **confidentiality must never prevent the sharing of information where this is necessary to protect a child or promote their welfare**.

Where there is a safeguarding concern, the child's safety and welfare take priority. Staff must follow the **Safeguarding and Child Protection Policy** and report concerns to the Designated Safeguarding Lead (DSL) without delay.

KCSIE 2026 makes clear that **data protection is not a barrier to safeguarding** and that information should be shared and recorded when necessary to protect a child.

**Legal and Statutory Framework**

This policy is informed by and should be read alongside the current legislation and statutory guidance applicable to St.Nicholas Nursery, including:

- **Early Years Foundation Stage (EYFS) Statutory Framework for Group and School-Based Providers 2026**;
- **Keeping Children Safe in Education (KCSIE) 2026**, where applicable to the setting and its safeguarding arrangements;
- **UK General Data Protection Regulation (UK GDPR)**;
- **Data Protection Act 2018**;
- **Data (Use and Access) Act 2025**, where applicable;
- **Children Act 1989**;
- **Children Act 2004**;
- **Working Together to Safeguard Children**;
- applicable statutory information-sharing guidance;
- **Freedom of Information Act 2000**, where applicable to the organisation;
- applicable employment and safeguarding record-keeping requirements; and
- guidance and requirements issued by the **Information Commissioner's Office (ICO)**, Ofsted, Lambeth Council and other relevant statutory bodies.

The EYFS framework requires providers to maintain appropriate records and information to support children's safety, care, learning and development. The current EYFS framework was updated on 1 September 2026.

**Data Protection Principles**

St.Nicholas Nursery will process personal information in accordance with the UK GDPR principles.

Personal information must be:

1. **Lawful, fair and transparent** – individuals should understand how and why their information is being used.
2. **Collected for specified purposes** – information must be used for legitimate and clearly defined purposes.
3. **Adequate, relevant and limited** – only information necessary for the purpose should be collected or shared.
4. **Accurate and up to date** – inaccurate information must be corrected promptly.
5. **Kept only for as long as necessary** – records must be retained in accordance with the nursery's retention requirements.
6. **Kept secure** – appropriate technical and organisational measures must protect information from loss, misuse, unauthorised access or disclosure.
7. **Accountable** – St.Nicholas Nursery must be able to demonstrate that it complies with data protection requirements.

These are the core UK GDPR principles identified by the ICO.

**Data Protection by Design and Default**

Data protection must be considered whenever St.Nicholas Nursery introduces a new process, system, activity or method of collecting or sharing information.

This includes:

- new digital systems or applications;
- changes to children's records;
- photographic or video recording;
- communication platforms such as Famly;
- sharing information with external professionals;
- staff monitoring systems;
- CCTV or security systems;
- online forms;
- websites and social media;

- data collected for funding or local authority purposes; and
- any new third-party provider handling personal information.

Where appropriate, a **Data Protection Impact Assessment (DPIA)** will be completed before a new processing activity begins.

St.Nicholas Nursery will use the principles of **data protection by design and default**, meaning privacy and security are considered from the beginning rather than after a process has been introduced.

**Information Held by St.Nicholas Nursery**

Depending on the purpose, St.Nicholas Nursery may hold information including:

**Children's information**

- name, date of birth and address;
- parent/carer and emergency contact details;
- attendance and registration information;
- medical, allergy and dietary information;
- medication records;
- developmental and learning information;
- observations and assessments;
- SEND information;
- individual support plans;
- safeguarding and child protection records;
- accident, incident and injury records;
- photographs and videos where appropriately authorised;
- funding information;
- communications with parents/carers;
- information received from health, education, social care or other professionals.

**Family information**

- contact details;
- parental responsibility information;
- emergency contacts;

- relevant family circumstances where necessary to safeguard or support the child;
- correspondence and communications.

**Staff information**

- recruitment and safer recruitment records;
- identity and qualification information;
- DBS and suitability information;
- training records;
- employment records;
- absence and attendance information;
- supervision and performance information;
- safeguarding records where applicable;
- health information where legally required and appropriately processed.

**Lawful Processing**

St.Nicholas Nursery will identify an appropriate lawful basis before processing personal information.

Consent may be used where appropriate, but **consent is not required for every use of personal information**.

Information may be processed because it is:

- necessary to comply with a legal obligation;
- necessary to perform a contract;
- necessary for legitimate interests where applicable;
- necessary to protect vital interests;
- necessary for a public task where applicable; or
- based on consent where consent is the appropriate lawful basis.

Special category information, such as health information, safeguarding information and certain SEND information, requires additional protection and an appropriate condition for processing.

Staff must not assume that consent is always required before information can be shared.

**Confidentiality**

All staff, agency workers, students, apprentices, volunteers and contractors have a responsibility to maintain confidentiality.

Information must only be accessed, discussed or shared where there is a legitimate reason to do so.

Staff must:

- only access information required for their role;
- only discuss children and families with colleagues who need the information for their work;
- avoid discussing confidential information in public areas;
- never discuss confidential information with friends or family;
- never share confidential information through personal social media;
- not photograph or copy confidential records onto personal devices;
- not use personal email accounts to send confidential information;
- ensure screens and records cannot be viewed by unauthorised people;
- securely dispose of confidential paperwork;
- follow the nursery's procedures for digital information; and
- immediately report any suspected data breach to the Nursery Manager or designated data protection lead.

Confidentiality applies both **inside and outside working hours**.

A breach of confidentiality may result in investigation and disciplinary action.

**Need-to-Know Principle**

Information will be shared on a **need-to-know basis**.

This means that a member of staff should only receive information where it is necessary for them to:

- safeguard a child;

- provide care;
- meet a child's learning, developmental or SEND needs;
- administer medication or respond to health needs;
- manage attendance;
- fulfil their professional responsibilities; or
- comply with a statutory or legal requirement.

The need-to-know principle does not mean that safeguarding information should be withheld from professionals who require it to protect a child.

**Safeguarding and Information Sharing**

Safeguarding takes priority over confidentiality.

If a member of staff believes that a child:

- is at risk of harm;
- may be experiencing abuse or neglect;
- may require children's social care intervention;
- may require early help;
- is missing or absent in circumstances that raise concern;
- has disclosed information indicating a safeguarding concern; or
- may be at immediate risk,

the concern must be reported to the DSL or Deputy DSL **without delay**.

Staff must not wait for parental consent before reporting a safeguarding concern.

Where necessary to safeguard a child, information may be shared with:

- children's social care;
- the police;
- health professionals;
- the local authority;
- Ofsted;
- the Local Authority Designated Officer (LADO), where appropriate;
- other education or childcare settings;
- relevant safeguarding partners; or

- another appropriate statutory or professional body.

The DSL will consider:

- what information needs to be shared;
- who needs to receive it;
- why it needs to be shared;
- the lawful basis for sharing;
- whether consent is required or appropriate;
- the potential impact of sharing or not sharing;
- whether the information is accurate and relevant; and
- what record needs to be made of the decision.

Current statutory information-sharing guidance confirms that safeguarding information may need to be shared without consent where necessary to protect a child.

**Recording Safeguarding Decisions**

Safeguarding records must be:

- factual;
- accurate;
- dated and timed;
- written as soon as possible after the concern or incident;
- clear about what was observed, disclosed or reported;
- clear about action taken;
- clear about who was informed;
- clear about decisions made;
- clear about the rationale for significant decisions; and
- stored securely.

Staff must distinguish between:

**Fact:** what was seen, heard or reported.

**Professional information:** information provided by another person or agency.

**Opinion or interpretation:** professional judgement, which must be clearly identified as such.

*KCSIE 2026 specifically emphasises recording the concern, actions, decisions, rationale and outcomes*.

**Parents and Access to Information**

Parents/carers will normally be provided with appropriate information concerning their own child.

However, access may be restricted where disclosure:

- would place another child or person at risk;
- would disclose another person's confidential information;
- could prejudice a safeguarding investigation;
- is restricted by law; or
- is otherwise subject to a lawful exemption.

A parent does not automatically have the right to access every document in which their child is mentioned.

Requests for personal information must be referred to the Nursery Manager/designated data protection lead and handled in accordance with applicable data protection requirements.

**Subject Access Requests**

Individuals have rights in relation to their personal information, including the right to request access to information held about them.

A Subject Access Request (SAR):

- may be made verbally or in writing;
- does not have to use the words "Subject Access Request";

- must be referred promptly to the appropriate person responsible for data protection;
- must be verified where necessary; and
- must be handled within the statutory timescale.

The normal UK GDPR response period is **one month**, subject to applicable extensions and exemptions.

Requests concerning a child's information must be considered carefully, including the child's age, maturity, competence, best interests and any safeguarding considerations.

Staff must **not independently disclose records** in response to a parent or individual's request without following the nursery's procedure.

**Accuracy of Records**

St.Nicholas Nursery will take reasonable steps to ensure information is accurate and kept up to date.

Parents/carers will be asked to update information where necessary, including:

- addresses;
- telephone numbers;
- emergency contacts;
- parental responsibility arrangements;
- medical information;
- allergies;
- dietary requirements;
- authorised collection arrangements; and
- other information necessary to keep children safe.

Staff must report inaccurate information as soon as they identify it.

**Secure Storage**

Paper records containing personal information must be:

- stored securely;

- kept away from unauthorised access;
- locked where appropriate;
- not left unattended in public areas;
- securely transported where necessary; and
- securely destroyed when no longer required.

Digital records must be protected through appropriate measures including:

- individual passwords;
- secure systems;
- appropriate access permissions;
- device security;
- screen locking;
- secure networks;
- controlled user access; and
- appropriate backup arrangements.

Staff must not share passwords or allow another person to use their account.

**Famly and Digital Records**

Where Famly is used to record or communicate information about children, staff must:

- use their authorised account;
- ensure records are factual and professional;
- only record information relevant to the child;
- avoid unnecessary personal information;
- not share login details;
- not take screenshots of confidential information unless specifically authorised and necessary;
- not transfer confidential Famly information to personal devices;
- ensure messages are appropriate and professional; and
- follow the nursery's data protection and digital communication procedures.

Safeguarding concerns must be recorded and escalated through the nursery's safeguarding procedure and not relied upon solely through routine parent communication.

**Photographs, Videos and Children's Image**

Photographs and videos of children must only be taken, stored, used or shared in accordance with:

- the nursery's Privacy Notice;
- photographic and image permissions;
- data protection requirements;
- safeguarding procedures; and
- the Social Media Policy.

Staff must never use personal mobile phones or personal devices to photograph children unless specifically authorised under an approved nursery process.

Children's images must not be:

- posted on personal social media;
- shared with friends or family;
- stored on personal devices;
- transferred to personal cloud storage; or
- used for purposes unrelated to the stated purpose.

**Staff, Agency, Student and Volunteer Confidentiality**

All staff, agency workers, students, apprentices and volunteers must receive appropriate information about:

- confidentiality;
- data protection;
- safeguarding information sharing;
- acceptable use of digital systems;
- photography and mobile phone restrictions;
- secure record keeping;
- reporting data breaches; and
- professional boundaries.

Agency workers and temporary staff are subject to the same confidentiality and data protection expectations as permanent staff.

**Data Breaches**

A data breach may include:

- sending information to the wrong person;
- losing a device containing personal information;
- leaving confidential paperwork unsecured;
- unauthorised access to records;
- sharing information through an incorrect email address;
- inappropriate disclosure of safeguarding information;
- loss or theft of a device;
- unauthorised screenshots or photographs; or
- accessing records without a legitimate reason.

Staff must report a suspected breach **immediately** to the Nursery Manager or designated data protection lead.

Staff must not attempt to conceal or delete evidence of a suspected breach.

The nursery will assess the incident, take immediate steps to contain it and determine whether notification to the ICO, affected individuals or another authority is required.

**Data Retention and Disposal**

Personal information will not be retained indefinitely.

St.Nicholas Nursery will maintain appropriate retention periods for different categories of records, taking account of:

- legal requirements;
- regulatory requirements;
- safeguarding needs;
- contractual requirements;
- financial and audit requirements;
- the purpose for which the information was collected; and
- the potential need to retain information for legal proceedings or safeguarding purposes.

Information must be securely destroyed or deleted when it is no longer required, unless there is a lawful reason to retain it.

The ICO states that organisations should establish and document retention periods wherever possible and regularly review information that they hold.

Safeguarding records must not be destroyed simply because a child has left the nursery where there is a lawful or safeguarding reason for retaining them.

**Information Sharing with External Agencies**

St.Nicholas Nursery may share relevant information with external organisations where this is necessary and lawful.

This may include:

- Lambeth Council;
- children's social care;
- health visitors;
- speech and language services;
- SEND services;
- educational psychologists;
- schools;
- Ofsted;
- police;
- safeguarding partners;
- other early years providers;
- funding authorities; and
- other relevant professionals.

Before sharing information, we will consider:

1. **What information is needed?**
2. **Why is it needed?**
3. **Who needs it?**
4. **Is there a lawful basis?**
5. **Is consent required or appropriate?**
6. **Would not sharing create a safeguarding risk?**

7. **Is the information accurate and proportionate?**
8. **How will the information be transferred securely?**

Where information is shared for safeguarding purposes, the decision and rationale should be recorded.

The statutory information-sharing guidance applicable from September 2026 reinforces the importance of appropriate information sharing across organisations involved in safeguarding children.

**Information Sharing Without Parental Consent**

Parental consent is not an absolute requirement for sharing information.

Where there is a safeguarding concern, information may be shared without parental consent where:

- obtaining consent would cause unreasonable delay;
- seeking consent could place a child at greater risk;
- the information is required to protect a child;
- there is a legal requirement to share;
- a statutory agency requires the information; or
- another lawful basis applies.

The DSL will make the decision where appropriate and will record the rationale.

Staff must never use data protection as a reason to delay reporting or sharing information where a child may be at risk.

**Freedom of Information**

St.Nicholas Nursery is not automatically subject to the Freedom of Information Act 2000 simply because it is an early year's provider.

Where an information request is received, it should be referred to the Nursery Manager/appropriate organisational lead so that the organisation's legal status and applicable requirements can be established.

Personal data requests should normally be considered under applicable data protection rights rather than being treated automatically as Freedom of Information requests.

**Staff Personal Information**

Staff personal information will be handled confidentially and only accessed by those who have a legitimate reason to do so.

Staff records may include:

- recruitment information;
- DBS and suitability information;
- qualifications;
- training;
- employment records;
- absence information;
- supervision and performance records;
- safeguarding-related records where appropriate; and
- other information required for employment or legal purposes.

Staff may request access to their personal information in accordance with applicable data protection rights.

**24. Children's Higher Protection**

St.Nicholas Nursery recognises that children require particular protection when their personal information is processed.

Information about children will therefore be handled with particular care, especially where it concerns:

- health;
- SEND;
- safeguarding;
- family circumstances;
- photographs and images;
- behaviour;

- developmental information; or
- information that could place a child at risk if disclosed.

The ICO recognises that children merit specific protection when organisations handle their personal information.

**Staff Training and Responsibilities'**

All staff must receive appropriate data protection and confidentiality information as part of induction.

Training will cover:

- confidentiality;
- UK GDPR principles;
- secure handling of information;
- safeguarding information sharing;
- recording safeguarding concerns;
- use of Famly and other digital systems;
- photographs and mobile devices;
- social media;
- data breaches;
- subject access requests; and
- professional boundaries.

Staff must immediately report any concern about data protection or confidentiality.

The Nursery Manager and/or designated data protection lead will monitor compliance and ensure that appropriate actions are taken where concerns are identified.

**Accountability and Monitoring**

St.Nicholas Nursery will maintain appropriate evidence that it manages personal information responsibly.

This may include:

- privacy notices;

- data protection policies;
- staff training records;
- confidentiality agreements;
- data protection impact assessments;
- information-sharing records;
- data breach records;
- retention schedules;
- secure disposal records;
- access controls;
- data processing agreements with relevant third parties; and
- records of safeguarding information-sharing decisions.

The effectiveness of this policy will be monitored through:

- staff supervision;
- audits;
- safeguarding reviews;
- incident and data breach reviews;
- training;
- management checks; and
- policy review.

**Relationship Between Confidentiality and Safeguarding**

Confidentiality is important, but **it is not absolute**.

The following principle must be understood by all staff:

***Information should be kept confidential where there is no legitimate reason to share it. However, information must be shared appropriately where this is necessary to safeguard or promote a child's welfare.***

**Example**

**Appropriate confidentiality**

A practitioner learns that a parent has changed their personal telephone number. The information is relevant to the child's emergency contact records. The

practitioner updates the appropriate nursery system but does not discuss the parent's personal circumstances with colleagues who do not need the information.

**Safeguarding information sharing**

A practitioner receives information that causes concern about a child's welfare. The practitioner reports this immediately to the DSL. The DSL may need to share relevant information with children's social care or another safeguarding agency. The information is shared because it is necessary to protect the child, even if parental consent has not been obtained.

This is not a breach of confidentiality. It is **appropriate and lawful safeguarding information sharing**.

**Breaches of this Policy**

Failure to comply with this policy may place children, families, staff or the nursery at risk.

Depending on the circumstances, a breach may result in:

- additional training;
- supervision;
- management action;
- investigation;
- disciplinary action;
- referral to a professional or regulatory body;
- notification to the ICO or another statutory authority; or
- other action required by law.

Any safeguarding-related breach will also be managed under the Safeguarding and Child Protection Policy.

**Policy Review**

This policy will be reviewed at least annually and sooner where:

- legislation changes;
- EYFS requirements change;

- KCSIE changes;
- ICO guidance changes;
- new digital systems are introduced;
- a significant data breach occurs;
- safeguarding learning identifies a need for change; or
- organisational procedures change.

The policy will be reviewed alongside the nursery's Privacy Notice, Records Retention arrangements, Safeguarding and Child Protection Policy and related digital/data security procedures.

**Key statutory principles for staff**

All staff should remember:

**Protect information.**
Only access and share information when there is a legitimate reason.

**Keep records accurate.**
Write factual, clear and professional records.

**Share when safeguarding requires it.**
Data protection is not a barrier to protecting children.

**Ask the DSL when unsure.**
Do not delay reporting a safeguarding concern because of uncertainty about confidentiality.

**Use secure systems.**
Never use personal devices, personal email or social media to share confidential nursery information.

**Think before sharing.**
Share information that is relevant, necessary, proportionate and lawful.

**Record important decisions.**
For safeguarding information sharing, record what was shared, with whom, why, the decision made and the rationale where appropriate.

**Related Documents**

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- SEND and Inclusion Policy
- Complaints Policy
- Whistleblowing Policy
- Safe Recruitment Policy
- Social Media Policy
- Mobile Phone Policy
- Health and Safety Policy
- Medication Policy
- Privacy Notice
- Records Retention Schedule
- Data Breach Procedure
- Information Security/Digital Systems Procedure
- Staff Code of Conduct

| **This policy was adopted on** | **Signed on behalf of the nursery** | **Date for review** |
|---|---|---|
| *Sept 2026* | Anjana Shah | *August 2027* |

- 