



Data Protection Policy

1. Purpose

At Little Dragon's Day Nursery, we recognise that we hold sensitive and confidential information about children, families, staff, and others. This policy sets out our commitment to protecting personal data and how that commitment is implemented in respect of the collecting, processing, using, storing and sharing of personal data.

2. Legal framework

This policy relates to the following legal framework:

- Data Protection Act 2018
- General Data Protection Regulation – EU Regulation 2016 (GDPR)
- Freedom of Information Act 2000

This policy also relates to section 3.69 & 3.70 of the Statutory Framework for the Early Years Foundation Stage (2017)

3. Policy Statement

- We fulfil all our obligations under the Data Protection Act 2018
- The nursery's Partners are responsible for ensuring compliance with data protection regulation
- We are registered with the Information Commissioners Office (ICO)
- All Partners, staff and volunteers have undertaken training in data protection and are aware of their responsibilities in collecting, using and sharing data
- We have a privacy notice that sets out the lawful bases for processing the data, the legitimate interests for the processing, individuals' rights and the source of personal data
- We have a process in place to record any data breaches and a form for reporting breaches to the ICO and any investigations (see section 5.6)
- We have a procedure in place for the storage, retention and disposal of all documents containing personal data
- We have a data sharing procedure in place (see section 5.4)

4. Our obligations

We are aware that data protection legislation applies equally to all data subjects (including children, staff and other stakeholders). We adhere to the following data protection principles:

- Data must be processed fairly, lawfully and in a transparent manner
- Data must only be obtained for specified and lawful purposes
- Data must be adequate, relevant and not excessive (limited to what is necessary)
- Data must be accurate and up to date
- Data must not be kept for longer than necessary
- Data must be securely kept



We offer the following statutory rights of individuals:

- The right to be informed
- The right of access
- The right of rectification
- The right of erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling

5. Procedures

5.1. Data Protection Officer

As a private nursery provider, our current business activities mean we are not required to appoint a Data Protection Officer under data protection regulations. We will however pay regard to the legislation, and will appoint a DPO if our business activities change to:

- require large scale, regular and systematic monitoring of individuals
- consist of large-scale processing of special categories of data or data relating to criminal convictions and offences

Nevertheless, the nursery will ensure that it maintains the resources required to meet our obligations under data protection regulations.

The Partners are available to deal with any concerns or requests relating to data protection.

5.2. Data collection and retention

Personal data must only be collected where:

- Consent has been obtained
- There is a contractual purpose for collecting the data
- We have a legal obligation to collect the data
- It is necessary to protect the vital interests of the individual (data subject)
- It is necessary for a task carried out in the public interest (such as census)
- The nursery has a legitimate interest in the data and this interest is not overridden by the interests, rights or freedoms of the individual (data subject)

Where data has been collected that does not fall under the above criteria, a Partner should be informed immediately.

All personal data is collected using standardised forms and document templates. Where personal data is collected on a new or unique form, this should first be approved by a Partner. No forms or personal data will be kept for longer than is necessary.

5.3. Data storage and disposal



All physical copies of documents containing personal data must be stored in a locked drawer or filing cabinet and not left where unauthorised people could see them.

All electronically stored data must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be stored on designated drives or cloud computing servers/systems that are protected by strong passwords and only accessible to staff on a 'need to know' basis
- All computers containing data should be protected by approved security software and a firewall
- If data is stored on removable media (such as CD or DVD), these should be kept locked away securely when not being used. Where personal data is stored on a memory stick, the device must be encrypted.
- As the data controller, the nursery will receive written assurance from all data processors (such as electronic system suppliers) that they are compliant with relevant legislation

Secure Disposal Procedures:

- Physical copies must be securely disposed of by a designated secure waste provider, or cross shredded as a minimum
- Electronic copies will be permanently deleted (i.e. also deleted from any recycle bin or backup), when it comes to secure disposal

5.4. Data sharing

Personal data is only shared or accessible amongst nursery employees on a 'need to know' basis.

The nursery may be required, on occasions, to share personal data to external bodies such as the police, local authorities, or social services; where this is required, data must be transferred using the following procedures:

- Electronic Files must only be transferred using encrypted emails or encrypted memory sticks
- Physical copies must only be transferred once the receiving agency has signed a 'data transfer form'. The nursery will retain a copy of this form which will be attached as a document to the individual's (child or staff) profile.
 - If the transfer requires an employee to take the file off site, then the member of staff must sign to state the date, time and nature of the data that has been taken

Where there is a regular need to share personal data with an agency (such as Looked After Children, or where a child attends two nurseries) then the procedures set out in the 'Information Sharing Policy' should be followed, and an 'Information Sharing Agreement' must be signed by both parties.

5.5. Subject Access Requests

The Data Protection Act 2018 enables individuals to submit a Subject Access Request which is a formal request to exercise their rights regarding data protection. A Subject Access Request may be used by an individual to be informed about, access (receive copies of), or erase any of their personal data.

A Subject Access Request must be submitted in writing (e.g. email or letter) to a Partner, who will acknowledge, log and act upon the request within one calendar month. The individual that submitted the request will be kept informed throughout the process and will be notified if the request is going to be delayed beyond one calendar month, along with the reason for the delay. All communications and documents will be sent to the individual using the method the request was received (e.g. electronically/paper copies), unless otherwise agreed.



5.6. Data breaches

All breaches in data protection legislation will be dealt with and monitored by a Partner. The Partners will log any breaches with the details of the breach, whether the ICO or data subject were notified (and the reasons), measures taken, and any remedial actions that resulted from the breach.

This version of the policy was originally approved by K.McLeod on the 05.07.21		<i>Version 1</i>	
Reviewed by:		Review date:	
Reviewed by:		Review date:	
Reviewed by:		Review date:	



Information Sharing Policy

1. Purpose of sharing information

The effective sharing of information between Little Dragon's Day Nursery and other agencies relating to children in our care is essential to support the learning, welfare and safeguarding of children. This policy sets out the type of information that may be shared; the legal grounds for information sharing; the retention, deletion, and security of information; and what to do if there is a breach of confidentiality.

2. Legal basis for sharing information

Little Dragon's Day Nursery and any partner agency must ensure that all information sharing complies with the Data Protection Act 2018, the Children Act (1989 & 2004), the Human Rights Act (2000) and any subsequent replacement legislation.

The Government's [Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers \(2018\)](#) document should be used as a basis of all information sharing arrangements.

3. Information to be shared

Only information that is relevant to the purposes (which must be clear and legitimate) should be shared with those who need it to do their job effectively and make sound decisions. The most common purposes that will require sharing information with other agencies are:

- Issues relating to the safeguarding of children
- Issues that relate to the learning and care of children, particularly relating to SEND

All information should only be shared with the consent of the individual (or person with parental responsibility), where a statutory duty exists, or if it is to protect the vital interests of the individual but consent can't be given

4. Keeping information secure and confidential

- The nursery may issue and receive information through the Partners, Nursery Manager, Designated Safeguarding Leads, or SENDCo, depending on the purpose of the information
- The nursery and partner agencies must ensure that their employees are able to access only the shared information necessary for their role and are appropriately trained so that they understand their responsibilities for confidentiality and privacy
- The nursery and partner agencies must protect the physical security of the shared information
- Sensitive information must only be sent electronically via encrypted email or other secure platforms

5. Data retention and deletion



- All data held by the nursery or a partner agency must be stored, retained and disposed of in line with their own records retention and security policies which must comply with the requirements of the Data Protection Act 2018, the Freedom of Information Act (2000), and any subsequent replacement legislation
- If information is found to be inaccurate, it is the responsibility of the organisation that identified the inaccuracy to update their records and notify their partner agency of the corrected information
- If an individual would like to exercise any of their right under the Data Protection Act 2018 or any subsequent replacement legislation, it is the responsibility of the organisation in receipt of the notification to act on the request and inform the partner agency if appropriate

6. Complaints

- The nursery and partner agencies should use their standard organisation policies and procedures to deal with complaints from the public arising from information sharing under this protocol

7. Breach of confidentiality

- Any information breaches (e.g. theft, loss, damage or inappropriate disclosure of information) relating to shared information must be reported to the nursery's Partners (information below)
- The Partners will liaise with the partner agency and help to ensure that the data breach is reported appropriately, and the necessary reporting requirements and timescales are adhered to

Contact details of the Partners:

- Neil McLeod (Partner) neil@littledragonsnursery.com 07813005256

This version of the policy was originally approved by K.McLeod on the 05.07.21		<i>Version 1</i>	
Reviewed by:		Review date:	
Reviewed by:		Review date:	
Reviewed by:		Review date:	