DATA PROTECTION

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR), which replaces the Data Protection Act 1998. The emergence of the internet, search engines, social media, smartphones, and cloud computing has led to the need to update the rules on data protection.

The settings policy on the processing, use, storage, and disposal of all data held on children, families, visitors, and staff is robust and is designed to ensure that it is kept confidential.

There are two main roles under the GDPR; the **data controller** and the **data processor**. As a childcare provider, we are the **data controller**. The data is that which we have collected about the staff, children and their families. We have contracts with other companies to process data, which makes them the **data processor**. The two roles have some differences but the principles of GDPR apply to both. We have a responsibility to ensure that other companies we work with are also GDPR compliant.

For the majority of data we collect, the lawful basis for doing so falls under the category of 'legal obligation' such as names, date of birth and addresses as we have a legal requirement to obtain this data as part of the Statutory Framework for the Early Years Foundation Stage.

Some data we collect, for example, photographs, requires parents to give consent for us to do so. Where this is the case, parents will be required to sign a consent form to 'opt in' and are made aware that they have the right to withdraw their consent at any time.

We may also be required to collect data as part of parent's contract with the setting or local authority, for example, for us to claim government funding.

Staff are required to complete online training to ensure they are up to date with the requirements around GDPR and how it relates to this policy and every day working practice.

STORAGE OF DATA

We keep data secure and aim to protect data against unauthorised change, damage, loss, or theft. All data collected is only accessed by authorised individuals. All paper forms are kept locked away and all computers and tablets are password protected.

Data is kept in both in the office in a unit that is locked when no one is present in the office during opening hours, at night/at weekends, the building is also securely locked at night, weekends and an alarm system is set which is linked to the manager and owners' mobiles, plus the fire service. Data is also stored online on a secure server that is managed by Dropbox, Online Office System and Parent app, plus on iCloud which is managed by Apple.

Staff members can only view this information onsite or when working from home with consent from management. This is recorded on the sensitive data access log.

PROCESSING OF DATA

All data processed that we collect must follow the GDPR principals* and will be collected and used for the reasons given at the time we collect it from staff or parents. It will then be processed by those appointed to use it for its intended use, such as setting up the child's online digital learning journey, billing and accounts or emergency logs.

PORTABILITY OF DATA

If staff members need to access data off the premises, they will ensure they only take what is needed and management will oversee this with the Sensitive Data Access Log to decide if there is any risk to anyone's data and sign off on the reason it is being accessed. Staff will also need to sign hard copies of data in and out of the building using the same Sensitive Data Access Log. Where applicable the

setting will make it clear to parents that this will happen and if required seek permission to do so as detailed in the privacy notices.

When sending data, which can identify a child and their family's personal details to other professionals via post, management will use recorded delivery to track the document in the post until it has reached the correct destination. Documents may also be delivered by hand, the recipient who takes the sealed envelope will be asked to sign a receipt to say the envelope will be passed on to the correct person. All envelopes will have 'private and confidential' written on them.

When emailing data, staff/management will send this information via secure email (if available) unless explicit consent is sort for the transition of data securely.

PRIVACY NOTICES FOR PARENTS, STAFF

All parents and staff are informed of our procedures around how and why we collect data, information sharing, security, data retention, access to their records and our commitment to compliance with the GDPR act 2018. Privacy notices differ depending on who's data is being collected and the reason for collection and use. This is explained when they are signing permission forms, registration, enrolment, job application, medical declaration, photo, video, and email consent. It can be explained both verbally and in writing.

Retention Period and Disposal of Data

We will store all paper copies for up to 1 year after a child or staff member have left the setting, after this period this data will be scanned and stored in a secure cloud-based server and then all hard copy paperwork will then be destroyed. The scanned data and any other digital data will be deleted after the end of the applicable retention periods within a processing time frame. Retention periods vary depending on the type of data as does the time frame for disposing of or removing data when requested. See the GDPR Retention Periods for Records for the length of time different data is stored.

FINGERPRINT ENTRY SYSTEM

Parents and staff fingerprints will be taken as part of the enrolment process; your name and child's name will be registered on the database which is stored locally on the desktop computer and communicates with the door entry system within the settings intranet. Fingerprints are not stored or used for any other purpose and will not be used or shared with any third parties and can be removed on request at any time following an agreed time frame.

***GDPR PRINCIPLES**

GDPR condenses the Data Protection Principles into 8 areas, which are referred to as the Privacy Principles. They are:

1. You must have a lawful reason for collecting personal data and must do it in a fair and transparent way.

2. You must only use the data for the reason it is initially obtained.

3. You must not collect any more data than is necessary.

4. It must be accurate and there must be mechanisms in place to keep it up to date.

5. You cannot keep it any longer than needed.

6. You must protect the personal data.

7. You must have appropriate measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction/damage to personal Data.

8. Personal Data shall not be transferred to any outside agency or country within the EU that does not comply with the new General data protection regulations.

The GDPR provides the following rights for individuals:

§ The right to be informed.

§ The right of access.

§ The right to rectification.

§ The right to erase.

§ The right to restrict processing.

§ The right to data portability.

§ The right to object.

§ Rights in relation to automated decision-making and profiling.

Carousel Nursery School is registered with the Information Commissioner's Office ICO.