General Data Protection Regulation Policy

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

GDPR states that personal data should be ‘processed fairly & lawfully’ and ‘collected for specified, explicit and legitimate purposes’ and that individuals’ data is not processed without their knowledge and are only processed with their ‘explicit’ consent.

GDPR covers personal data relating to individuals. KEYFS is committed to protecting the rights and freedoms of individuals with respect to the processing of children's, parents, visitors and staff personal data.

GDPR means that KEYFS must;

- Manage and process personal data properly.
- Protect the individual’s rights to privacy.
- Provide an individual with access to all personal information held on them.

KEYFS is registered with the ICO. (Information Commissioners Office)

GDPR includes 7 rights for individuals:-

1) The right to be informed.

KEYFS is a registered Childcare provider with Ofsted and as so, is required to collect and manage certain data. We need to know children’s’ full names, addresses, date of birth. We are also required to know parent’s names, addresses, telephone numbers and email addresses for ease of contact and date of birth and National Insurance numbers for parents claiming the free extended nursery entitlement. This information is sent to the Local Authority via a secure electronic file transfer system.

There is a Privacy Notice outlining this requirement from Worcestershire County Council on our notice board.

We are required to collect certain details of visitors to our setting. This may include visitors names, telephone numbers, addresses and where appropriate company name. This is in respect of our Health and Safety and Safeguarding Policies.

As an employer we are required to hold data on our employees; names, addresses, email addresses, telephone numbers, date of birth, National Insurance numbers, photographic ID such as passport and driver's license, bank details. This information is also required for Disclosure and Barring Service checks (DBS) and proof of eligibility to work in the UK. This information is sent via a secure file transfer system to GBG for the processing of DBS checks.

2) The right of access.

At any point an individual can make a request relating to their data and KEYFS will need to provide a response (within 1 month). KEYFS can refuse a request, if we have a lawful obligation to retain data i.e. from Ofsted in relation to the EYFS, but we will inform the individual of the reasons for the rejection. The individual will have the right to complain to the ICO if they are not happy with the decision.

3) The right to erasure.

You have the right to request the deletion of your data where there is no compelling reason for its continued use. However, KEYFS has a legal duty to keep children's and parents details for a reasonable time. KEYFS retain these records for 3 years after leaving pre-school, children's accident and injury records for 19 years (or until the child reaches 21 years), and 22 years (or until the child reaches 24 years) for Child Protection records. Staff records must be kept for 6 years after the member of staff leaves employment, before they can be erased. This data is archived securely offsite and shredded after the legal retention period.

4) The right to restrict processing.

Parents, visitors and staff can object to KEYFS processing their data. This means that records can be stored but must not be used in any way, for example reports or for communications.

5) The right to data portability.

KEYFS requires data to be transferred from one IT system to another; such as from KEYFS to the Local Authority, to shared settings and to Tapestry' Online Learning Journal. These recipients use secure file transfer systems and have their own policies and procedures in place in relation to GDPR.

6) The right to object.

Parents, visitors and staff can object to their data being used for certain activities like marketing or research.

7) The right not to be subject to automated decision-making including profiling. Automated decisions and profiling are used for marketing based organisations. KEYFS does not use personal data for such purposes.

Storage and use of personal information.

Information about individual children is used in certain documents, such as, a weekly register, medication forms, referrals to external agencies and disclosure forms. These documents include data such as children's names, date of birth and sometimes addresses. Paper copies of children's and staff records are kept in a locked filing cabinet. Members of staff can have access to these files but information taken from the files about individual children is confidential and apart from archiving, these records remain on site at all times. These records are shredded after the retention period.

A large amount of personal data is collected every year including; names and addresses of those on the waiting list. These records are shredded if the child does not attend or added to the child's file and stored appropriately. Information regarding families' involvement with other agencies is stored both electronically on an external hard drive and in paper format, this information is kept in a locked filing cabinet on site. These records are shredded after the relevant retention period.

Upon a child leaving KEYFS and moving on to school or moving settings, data held on the child may be shared with the receiving school. Such information will be delivered by hand or sent securely electronically.

KEYFS stores personal data held visually in photographs or video clips or as sound recordings, with consent obtained via the registration form. No names are stored with images in photo albums, displays, on the website or on KEYFS's social media site.

Access to all Office computers and Tapestry Online Learning Journal is password protected. When a member of staff leaves the company these passwords are changed. Any portable data storage used to store personal data, e.g. USB memory stick, are password protected and/or stored in a locked filing cabinet.