Confidentiality & Data Protection Policy

Confidentiality

Any information given to the Tithe Barn Preschool, either verbally or in writing, regarding your child or your family, will be treated as confidential.

We will not discuss your child with others unless we have permission from you, for example sharing information with outside agencies (Speech & Language, Educational Psychologist, etc). We will however divulge confidential information to Social Services, the Police and to Ofsted if there appears to be a protection issue.

Parents will have access to their own child's records at any time but not to the files of other children. All documentation relating to your child is stored in a file, which is not accessible to any other party.

Data Protection

The General Data Protection Regulation (GDPR) is a new EU law that came into effect on 25 May 2018 (updates checked regularly at www.ico.org.uk) . It replaced the Data Protection Act 1998 and the changes will remain in place even after the UK leaves the EU in 2020. GDPR will give individuals greater control over their own personal data.

The Data Protection Principles are split into six areas, which are referred to as the Privacy Principles. They are:

1. Preschool must have a lawful reason for collecting personal data and must do it in a fair and transparent way.
2. Preschool must only use the data for the reason it is initially obtained.
3. Preschool must not collect any more data than is necessary.
4. It has to be accurate and there must be mechanisms in place to keep it up to date.
5. Preschool cannot keep it any longer than needed.
6. Preschool must protect the personal data.

These privacy principles are supported by a further principle – accountability. This means that our setting must not only do the right thing with data but must also show that all the correct measures are in place to demonstrate how compliance is achieved.

There is also an expectation that staff will be trained on data protection. Documentation on policies, procedures and training is going to be a key part of any effective compliance programme.

Data protection officer — Mrs Samantha Fisher & Mrs Cathy Lea will act as the lead on data compliance.

Privacy notices — When we collect any data we must tell you exactly how we are going to use it, who might you share it with, how long you will keep it as well as information on consent and complaint.

Individual rights — You will have new and enhanced rights on the collection, access and deletion of your data so Preschool must ensure our setting has mechanisms to allow individuals to exercise these rights.

Consent — GDPR will require early years providers to have a legitimate reason for processing any personal data. Preschool rely on consent for processing data and can demonstrate that the consent was freely given by parents actively opting-in on our Permission Forms.

Data agreements — Early years providers will now be obliged to have written arrangements with anybody processing data for them. Providers must make sure that anyone processing data will meet GDPR requirements.

Breach notification — Preschool will be obligated to notify the Information Commissioner's Office (ICO) of a data breach within 72 hours of becoming aware of the breach.

All data that is collected and stored by the Tithe Barn Preschool is kept in a locked filing cabinet on the premises. Parents are allowed access to their file at any time and can change the information we have stored if necessary. Parents are required to complete and sign the Permissions Form before their child starts Preschool. These forms include information about who we may share their child's details with e.g. OFSTED, Health Professionals and Primary Schools. Parents are made aware that as part of our Safeguarding Policy, there are occasions when we do not need parent's permission to share their personal details e.g. in cases of Child Protection concerns.

Data that is logged on the computer system or iPads are locked with a password or passcode. Where Staff are concerned, their personal information is kept locked in the cabinet in their own files and information is stored on the Single Central File held on the Manager's computers. Their payslips are sent encrypted via email to protect their personal information.

All records are kept for three years and will then be destroyed permanently.

Written September 2016

Reviewed annually

Signed: