

Safeguarding and Welfare Requirement: Child Protection

Providers must have and implement a policy, and procedures, to safeguard children.

Playpen Pre-school

10.12 Data Protection Policy

Policy statement

In order to provide a quality early years and childcare service and comply with legislation, we need to request information from parents about their child and family and from employees. Some of this will be personal data.

1. We must have a lawful reason for collecting personal data, and must do it in a fair and transparent way. We will be clear about what data we collect, and why.
2. We must only use the data for the reason it is initially obtained.
3. We must not collect any more data than is necessary. We will only collect the data we need to hold in order to do the job for which we have collected the data.
4. We will ensure that the data is accurate, and ask parents to notify us if the data held changes.
5. We will not keep data any longer than needed and to complete the tasks it was collected for or to comply with statutory requirements.
6. We must protect the personal data by ensuring that all staff charged with using the data, processes and stores it securely.
7. We will be accountable for the data. This means that we will be able to show how we comply with the law.

Procedures

- We are registered with the Information Commissioner's Office, the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
- We expect parents to keep private and confidential any sensitive information they may accidentally learn about the Pre-school or the other children and families attending the Pre-school setting, unless it is a child protection issue.
- We will be asking parents for personal data about themselves and their child/ren in order to deliver a childcare service (see privacy notice). We are required to hold and use this personal data in order to comply with the Statutory Framework for the Early Years Foundation Stage, Ofsted, Department for Education and the Local Authority.
- If we need to send personal data this will be done in a secure tracked form.

Subject access

Parents have the right to inspect records about their child (see our Confidentiality and Client Access to Records).

Storage

We keep all paper-based records about children and their families securely locked away. Records relating to individual children stored on computers, externally or in cloud storage including digital photos or videos, is stored securely in password-protected files, on password protected devices to prevent viewing of the information by others with access to the computer/devices.

Backup files are stored on an external hard drive which is locked away when not being used. Firewall and virus protection software are in place.

If I store any records using a digital solution such as Tapestry, we carry out due diligence to ensure they are compliant with GDPR.

Information sharing

See *Information Sharing Policy*

Record keeping

See *Children's Records Policy, Provider's Records Policy, Transfer of Records to School Policy*

Safe disposal of data

See *Children's Records Policy*

We are required by law to keep some data for some time after a child has left the setting. We have a review plan in place and ensure that any data is disposed of appropriately and securely.

Suspected breach

If we suspect that data has been accessed unlawfully, we will inform the relevant parties immediately and report to the Information Commissioner's Office within 72 hours. We will keep a record of any data breach.