Belton Playgroup

Data Protection Policy

Our Data Compliance Officer is Samantha Dexter

Data Protection Policy

This policy defines the arrangements at Belton Playgroup that assure compliance to the requirements of The General Data Protection Regulation as relevant to the Playgroup's charitable and business interests:

Introduction

- The GDPR states that personal data shall be 'processed fairly and lawfully' and collected for specified, explicit and legitimate purposes'.
- The GDPR covers the management and control of personal data within a setting.
- Personal data is defined as any information relating to an identifiable living individual; and will therefore, apply to the Playgroup's clients (children attending the Playgroup, and their parents/ carers), employees and suppliers.
- The GDPR applies to records kept in hard copy (paper) format, and in computer files.

Principles of data protection

1. The Playgroup is committed to the enforcement of the following code of good practice in relation to the data it keeps on the individuals associated with the playgroup: including children, their parents and carers, our employees and suppliers. In summary, data will:
   - Be fairly and legally processed;
   - Be relevant to the needs of the Playgroup setting;
   - Not be unnecessarily excessive in detail;
   - Be accurately maintained;
   - Not be kept longer than necessary, or required by law;
   - Only be used in accordance with the individual subject's rights;
   - Be securely stored.

Policy details

1. The Playgroup will require written consent from the child's parents/ guardian/ carer, for personal data to be collected and processed. In this respect it will be taken that consent is implied through the following:
   - Clients – by the parent/carer who signs the registration forms, acceptance forms and appropriate consent forms as a 'contract for Playgroup care' for their child/ children.
   - Employees – by completing the job application form and contract at onset of employment, and where the employee has not registered an objection to their data being used.
2. All individuals, parents, carers and employees have the right of access to paper and computerised records when concerning their personal data unless there is a legal and legitimate reason why it may not be accessed.
3. Where it is deemed necessary to divulge to a third party this will only be done with the express permission of the individual subject unless there is a legal and legitimate reason why it may be shared without consent.
4. Personal data and records will be maintained under appropriate conditions of security to prevent any unauthorised or accidental disclosure. Records can be hard copy (paper) format and computer files.
5. Where photos are shared by parents by email or Facebook once the photos have been printed they will be deleted from the computer.
6. Photos that have been taken during the Playgroup session are stored in an encrypted file on the laptop and printed for the children's learning journeys and then deleted.
7. Learning Journeys are stored in a locked cabinet.

Attention is paid to the following aspects of the record storage:

1. Hard copy file: all staff have access to the children's individual records which are stored in a locked cabinet.

2. Computer file: the manager and deputy manager have access to the encrypted Playgroup files in the Playgroup laptop, but the manager has sole access to sensitive data. The back-up hard drive is stored in the locked cabinet.

When personal data is being processed, staff will take reasonable precautions to prevent sighting of data by unauthorised persons:

- Personal record files are locked away when are not in use.
- The laptop is left on a screen saver (which would then need a password to access) when not in use.

Secure management of data

This summarises the arrangements in place at Playgroup that ensures the correct handling, use, storage and disposal of disclosure information provided by the DBS Disclosure Service.

1. As part of the staff recruitment process it is a critical requirement to obtain disclosure information from the DBS for each applicant for who a job offer will be made.

This has two key objectives:

- To assess the overall suitability of the applicant to work with the children, as reflected by the disclosure information provided
- To ensure that any applicant that has a criminal record is treated fairly, as appropriate to the nature of the criminal conviction identified.

2. Disclosure information will not be retained on site, but the number and date of issue will be kept in the individual staff file.
3. Disclosure information will only be used for the specific purpose for which it was requested and for which the job holders/applicants' full consent has been given.
4. Copying of disclosure information is not permitted under any circumstances.

Working from home

1. Explicit permission from parents will be obtained before a child's learning journey is taken from the setting.
2. The staff will only take the learning journeys home to update and will return immediately, they will not take the learning journeys in their cars to anywhere other than home.
3. Staff will be aware of data protection when completing the learning journeys – putting them away when not working on them or if visitors call.
4. The manager, when working on the laptop will ensure it is on protected screen saver when not in use and any printed documents are put straight into the laptop bag which is kept in a cupboard.
5. The second back up hard drive which is kept at the manager's home is locked away.

Control of Records

This summarises the systems and arrangements in place at Playgroup to control personal records and personal files in line with the requirements for OFSTED registration and the GDPR.

1. Each set of records will be maintained in a secure location within the Playgroup and in such a manner to prevent spoilage or deterioration.
2. Obsolete records will be processed as follows:
    - When archived, records will be labelled with the expiry date in line with appropriate and current legislation / regulations that govern the keeping of records and after that date, they will be shredded.
    - Disposal by shredding will require authorisation by the Playgroup manager.

Information Sharing

This defines what is meant by information sharing, providing an understanding of the relationships between confidentiality and the requirement to share information.

1. Information sharing is essential to enable early intervention. Such interventions help children who need additional services to achieve positive outcomes.
2. It is vital to safeguarding and promoting the welfare of the children.
3. Staff should explain, openly and honestly, what, how and why any information will be shared and seek consent from the person with parental responsibility. The only exception to this is if sharing information would put the child at increased risk of significant harm
4. Staff should ensure that any information shared is:
    - Accurate and up to date
    - Necessary for the purpose for which it is being shared
    - Shared only with people who need to see it
    - Shared securely.

When sharing information without consent:

1. Staff must always consider the safety and welfare of the children when making decisions on whether to share information about them.
2. Staff should, where possible, respect the wishes of the children and family who do not consent to share confidential information. However, information may still be shared if, in their judgement on the facts of the case, there is sufficient need to override that lack of consent.
3. Always seek advice when in doubt from LA Improvement advisers, Ofsted or the ICO depending on the situation.
4. If confidentiality is to be broken, the staff should share the information in line with Playgroup procedures. The decision to release information should be recorded as follows:
    - What information was provided, when and to whom

- The reasons why it was shared
- Evidence that a thorough risk assessment was undertaken
- Who authorised the disclosure of the record?

How this impacts on confidentiality:

1. All staff who have access to information about the children have a duty to preserve everyone's right to confidentiality.
2. Consent will need to be given before any information can be shared.
3. If information is disclosed which indicates that the child is at serious risk of harm, then confidentiality cannot be followed as safeguarding procedures must take precedence.

Breach of Data:

If there has been a breach of data, the Playgroup manager will:

1. Contact all individuals whose data has been breached and ensure them that procedures have been put into place to make sure it doesn't happen again
2. Contact the ICO within 72 hours of the incident (if the breach is thought to be of significant harm to individuals)
3. Investigate the breach thoroughly and record evidence on what steps have been taken to avoid this happening in the future

Clients, who have concerns about the data storage, sharing or believe there has been a breach of data can contact the Information Commissioner's Office at https://ico.org.uk/global/contact-us/

Please also see our Confidentiality Policy, Safeguarding Policy and Social Networking Policy.

This policy was adopted at a meeting of Belton Playgroup Association:

Held on: 28th April 2022

Signed on behalf of committee: EWood

Name and role of signatory: Emma Wood, Chair of committee

Review date: April 2023