# Data Protection Policy

This policy covers the General Data Protection Regulations and an individual's rights as set down in the Freedom of Information Act 2000.

The setting requests information from parents about their child and family, which will include personal data, to comply with current legislation and ensure the safety and welfare of the child. We are required to hold and use this personal data to comply with the Statutory Framework for the Early Years Foundation Stage, Ofsted, Department for Education and the local authority.

In all circumstances, we will request written parental consent to process data. Parents will be asked to sign permission forms so that they clearly understand exactly what they are giving consent for. Parents can also withdraw their consent at any time, for example, taking photos of their children.

**Security of information**

The setting will ensure that measures are taken to safeguard personal data and privacy in accordance with the General Data Protection Regulation (GDPR). Everyone connected with the setting has a personal responsibility to ensure that any information of a personal or sensitive nature, to which he/she has access during his/ her work, is protected from unauthorised access and disclosure.

The GDPR stipulates that anyone processing personal data must comply with six principles of good practice that are legally enforceable. To comply with these regulations, we will ensure:

1. The processing of personal data will be lawful and fair. We will be clear about what data we are collecting, and why, and seek your written consent.
2. Data will only be used for the purpose it is intended. It will not be used to market a product or service or be processed in a manner that is incompatible with the purpose for which it was collected.
3. Personal data processed must be adequate, relevant and not excessive in relation to the purpose for which it was processed. Only data appropriate for the purpose it was collected will be held.
4. Data collected must be accurate and up to date. Out of date data will be will destroyed. Parents will be required to check annually and confirm that the data held is still accurate. We are required by law to keep some data after a child has left the setting (see Data Protection Impact

Assessment). We have a review plan in place and ensure that any data is disposed of appropriately and securely.

5. Personal data will be kept for no longer than is necessary for the purpose for which it is being processed.
6. Personal data will be kept confidential and processed in a manner that ensures appropriate security. Electronic storage of such material will be password protected (firewall and virus protection software are in place), and paper copies of personal data will be held in locked secure cabinets. For any records stored using an online digital solution, we will ensure we have carried out due diligence to ensure they are compliant with GDPR.

The setting is registered with the Information Commissioner's Office (ICO),

**Subject access**
Parents have the right to request records held about their child at any time. This information will be provided within one month from the written request.

**Information sharing**
Information sharing is essential to meet the needs of the children and families who attend. Data may therefore be shared with and may be obtained from:

- Other childcare providers if a child also attends another setting.
- Central Bedfordshire Council regarding the childcare and early years entitlements (for Childcare Sufficiency and Nursery Education Funding data).
- Local Safeguarding Children's Board
- Assistants /students /volunteers. All assistants and volunteers must sign a confidentiality agreement, and understand the need to protect the privacy of children and families in their care; and will handle all information verbal, written or digital in a confidential manner.
- Ofsted may require access to our records at any time.

Information will not be shared with anyone without parents' consent, unless there is a child protection concern.

**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 written records of any data breach.
**Data which may be held includes the following:**

- List of names, addresses and home telephone numbers and emergency contact numbers of children attending and staff / volunteers / students / Committee members digital and paper records.
- Paper or computer based employee files containing employment records, bank account details and national insurance numbers
- Training records of staff
- Performance records of staff
- Information contained on email which may mention the individual's name
- Laptop computers holding personal data
- Children's assessment / observation records
- Information provided to, or received from, external sources

- Photographs
- Incident reports
  This list is not exhaustive and will be subject to change see GDPR schedule for specific, current details.

In particular, individuals must observe the following rules (see E-safety policy for further details):

- Electronic storage of such material should be password protected
- Paper copies of personal data must be held in secure cabinets
- Individuals must not disclose personal information except to authorised colleagues
- Particular care must be taken when exchanging information with third parties
- Information must not be used for purposes other than that for which it was intended
- If records are taken off site (e.g. on laptops), appropriate security measures should be taken (e.g. laptops should never be left unattended in vehicles, and they should be stored securely off site)
- Usage of the BabysDays App outside of the setting must be done sensitively so as to keep children's information secure and confidential.
- All employees / students / volunteers / committee members must sign a confidentiality agreement
- Where paper based documents are removed from records these must be confidentially shredded
- Personal data should not be retained for longer than necessary, see GDPR schedule
- Memory sticks, discs etc will be only used by authorised people and will be stored securely when not in use.

**This policy was adopted on:**.....

**Signed on behalf of the setting**……..

**Date of next review:**.....