

Data Protection Policy

This policy covers the General Data Protection Regulations and an individual's rights as set down in the Data Protection Act 1998 and the Freedom of Information Act 2000.

Heath Barn Preschool 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

We 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 Out of date data will be destroyed.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 (please refer to Privacy Notices). 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.