# Confidentiality Policy

(**Cross reference to Committee Policy, Child Protection Policy, Safe Recruitment Policy, Personnel Policy, Key Person and Partnership with Parents/Carers Policy, Learning and Development Policy, Behaviour Policy, Children in Care and Looked after Children Policy, SEND Policy, Staff Behaviour Policy, Supervision Policy and Health and Safety Policy)**

Busy Bees ensures and respects the privacy of the children, their parents/carers and staff in our duty to provide a high-quality childcare and education setting. As an organisation that processes personal data we are registered with the Information Commissioner's Office or ICO. Confidential information and records about staff, parents/carers and children are held securely and only accessible and available to those who have a right or professional need to see them. Busy Bees is aware of and fully compliant in our responsibilities under the General Data Protection Regulation 2018 (GDPR), Data Protection Act 1998 (DPA) and where relevant the Freedom of Information Act. This policy sets out how Busy Bees will follow the Principles of Accountability, by showing the systems in place and how we are complying with GDPR. Further guidance can be found on the website of the Information Commissioner's Office at: https://ico.org.uk/

Types of Data Personal data is any data that can be linked to a single person and which identifies them in some way. For example, a name and personal email address and/or information such as phone numbers, bank details, addresses and date of birth. Busy Bees keeps an audit of all the personal data that we hold. This includes data on parents/carers, children, staff and Committee members, and any other adults (potential new staff/visitors, students etc.) The audit includes where the information came from, what we do with it and who we share it with, how long we keep it and when and how it is destroyed or deleted. Busy Bees Data Audit is available on request.

## The lawful bases for processing data are:

- Consent: the individual has given clear consent to process their personal data for a specific purpose
- Contract: the processing is necessary for a contract with the individual
- Legal obligation: the processing is necessary to comply with the law
- Vital interests: the processing is necessary to protect someone's life
- Public task: the processing is necessary to perform a task in the public interest or for official function
- Legitimate interests: the processing is necessary for legitimate interests

**Following the Principles set out in Article 5 of the GDPR, Busy Bees will ensure:**

- We have a lawful reason for collecting the data and we will be fair and transparent on how we process it
- We will only collect data for a specified purpose and only use it for that purpose
- We must only collect the data that is necessary
- All data must be accurate and be kept up to date
- We must not keep the data for longer than is necessary
- We must keep it safe

Busy Bees will appoint a Data Protection Lead who must understand their role, must have a clear idea of what type of data is held, what it's used for, where it's stored, how long it's kept for and if it's shared anywhere else. Busy Bees Data Protection Lead is Jane Burris (Administrator).

## Record Keeping

Busy Bees will issue all parents/carers and staff with a Privacy Notice, detailing the six lawful bases for processing information, and consenting to Busy Bees continuing to hold and process their data and send information. The Privacy notice acts as an 'opt-in system' where parents/carers and staff can choose how they receive information about Busy Bees and our Committee. As Busy Bees cares for children under the age of 13 we will gain consent from whoever holds parental responsibility for the child. We will only use the personal information to enable us to provide an early year's education service and to pass on information to keep in contact with parents/carers and staff. Busy Bees will keep the information secure and will only share it as necessary and appropriate for funding purposes (e.g. to access 15 or 30 hours funding from Gloucestershire County Council) or if required by law (e.g. for safeguarding purposes). Parents/carers have access to all written information about their child (except where data protection laws stipulate it is against the best interest of the child). Parents/carers do not have the right to access information about any other child. Staff will discuss personal information given by parents/carers with other members of staff, on a need to know basis, and only if it affects the needs or development of the child. Staff will not discuss or partake in any discussion about any other child or their family with any other parents/carers. Staff induction includes an awareness of the importance of confidentiality in the role of the Key Person. Parents/carers and staff can ask Busy Bees to delete any data held at any time and we will comply in accordance with our statutory obligations. Although parents/carers and staff can withdraw consent if they wish to, this may affect Busy Bees being able to continue to care for the child or continue their employment.

## Personal Records

These confidential records are stored in a lockable filing cabinet in the office.

- Registration and admission forms

- Signed consents e.g. Permissions Form, Privacy Notice and Information Sharing Consent Form
- Correspondence concerning the child or family
- Reports or minutes from meetings concerning the child from other agencies
- An ongoing record of relevant contact with parents/carers and observations by staff and any confidential matter involving the child i.e. developmental concerns or safeguarding issues.

## Development Records

We aim to ensure that all parents/carers and staff feel confident enough to share information on the understanding that it will only be used to enhance the welfare of the children. Parents/carers are required to give written permission for Busy Bees staff to record observations and assessments of their child's progress, and to share this information with any other settings that the child may attend. Busy Bees will ensure we keep parents/carers fully informed of their children's progress and development and will give verbal feedback to parents/carers about their child's time with us. We only share information about our families and staff with other professionals or agencies on a "need to know" basis, following consent from the parent/carer. These include:

- Photographic and written observations of children, summary development reports and progress checks that are completed using Learning Journey.
- Paper records such as My Plans/My Plan Plus and EHCPs are stored securely in a locked filing cabinet
- Records are shared with other professionals when required (following written parental consent) and are sent securely using Egress Switch or posted and marked private and confidential in a sealed envelope

## Personnel and staff records

We retain Personnel and staff records, whether paid or unpaid in line with statutory requirements and to aid each staff members personal development. All personnel records remain confidential to the people directly involved with making personnel decisions.

## Sharing Information

- We will not share personal information with any other organisations without parental consent (unless the child is at risk of significant harm)
- Our Registration and Permissions form clearly state what information will be shared with other organisations, the reason for sharing the information and parents/carers are asked to give consent for the information to be shared. The information will be shared to help with the safe and efficient management of Busy Bees and to help us to meet the child's individual needs following the EYFS framework
- If we become aware of a data breach of a third-party processor we must notify the ICO within 72 hours

- Where evidence to support our concerns are not clear we may seek advice from GSCB
- We only share relevant information that is both accurate factual, non-judgmental and up to date
- Care should be taken when speaking on the telephone that no information is given about a child unless speaking directly to the parents/carers, emergency contacts or professionals
- Students, when they are observing in the setting, are advised of our confidentiality policy and are required to respect it at all times. Personal information about children, parents/carers or staff must not be looked at by students on placement unless specific consent has been given by a parent/carer for a specific reason.

Our procedures enable us to comply with legislation such as the Human Rights Act 1998 regarding protecting the individual's right to privacy. Our only justification to interfere with this right is where we believe a child may be at risk of significant harm or to prevent a crime. We do not seek consent from parents/carers to share information where we believe that a child, or sometimes a vulnerable adult, may be endangered by seeking to gain consent. For example, where we have cause to believe a parent/carer may be trying to cover up abuse or threaten a child. When we make a decision to share information without consent it is always recorded in the child's records and a reason clearly stated. Busy Bees will only share information with other professionals working with the child (e.g. the police, social services and Ofsted) without consent when:

- There are concerns that a child is or may be suffering significant harm
- The 'reasonable cause to believe' a child is or may be suffering significant harm is not clear.
- There are concerns about 'serious harm to adults' (such as domestic violence or other matters affecting the welfare of the parents/carers).

## Procedure for transporting confidential documents

All reasonable measures are taken to ensure personal information is stored and where needed transported and transferred securely at all times.

- There may be occasions where developmental records may need to be completed/updated outside of Busy Bees. These will only be held by the child's Key Person, who will be responsible for ensuring the security of these documents and that they are the only person who can view them
- All personal documents are clearly marked 'Private and Confidential' and will be posted or hand delivered by a member of staff or by the child's parents/carers
- Personal documents will be emailed using Egress Switch where available or will be password protected and only include the child's initials
- Any confidential information no longer required will be disposed of by secure shredding. Digital records, website, electronic messaging and social networking.

- Busy Bees staff, volunteers or students are not allowed to discuss children, parents/carers or anything to do with the setting on any social networking sites

## Retention of records:

To meet certain regulations, some records relating to individual children, staff and Committee members must be retained for a required or recommended period of time after they have left the provision. All retained documents are stored securely in a locked area of the filing cabinet. After this time, the documents are securely shredded. For more information, please refer to the Retention periods for records document https://www.preschool.org.uk/sites/default/files/retention_periods_for_records_aug_13.pdf (A copy of this document is also available in our Data Protection file).

## Data Subject Access Requests Policy and Procedures

Parents/carers and staff have the right to ask to view any information that Busy Bees holds about them, and we will comply in accordance with the General Data Protection Regulations 2018:

- Data Subject Access requests may be submitted in any form, but Busy Bees may request that the individual confirms the request in writing (this can be by email or letter)
- The request will be forwarded to Louisa Dingley as Data Protection Lead for Busy Bees Playgroup
- Jane Burris will consider if the request can be refused. It can only be refused if it is 'manifestly unfounded or excessive'. For more information on 'manifestly unfounded or excessive' requests please see the ICO website
- We may request evidence of identity to ensure data is being disclosed to the correct individual
- There is no fee for processing a Data Access Request unless the request is 'manifestly unfounded or excessive'. Even if this is the case the fee will only cover administration costs. It is permissible for us to charge a fee for additional copies of the same information
- We will respond without undue delay and within 1 calendar month from the initial request. If requests are complex or numerous this can be extended to 3 months, but this must be fully explained within the 1-month deadline
- If the request is extremely broad, we may seek clarification on the exact scope of the data required
- A decision will be made on what systems and files should be searched for relevant personal data. We will keep a note of this as evidence of the steps taken in case a complaint is made by the individual to the ICO.

- We will consider if all the data should be disclosed. There are very limited exemptions where disclosing the data would 'adversely affect the rights and freedoms of others'. This is most likely to mean redacting the information to take out anything identifying a third party or if the data is related to a criminal offence.
- A copy of the data to be disclosed will be sent to the requestor. Where possible, and certainly if the request was made electronically the data will be provided electronically in a commonly used electronic format. If it is a paper copy it will be sent recorded delivery, if via email a delivery receipt will be requested as evidence that it was sent.
- A covering letter/email will also be sent containing the following information.
- The categories of their personal data being processed by us (e.g. Fees)
- The purposes for which the processing happens (e.g. Fee payment)
- To whom the data may be disclosed (e.g. GCC, HMRC)
- Details of the source of the data (e.g. Registration Form, Childcare Choices Portal)
- How long the data is retained by us
- The right to have inaccurate data corrected
- The right to make a complaint to the Data Protection Commissioner
- If automated decision making applies meaningful information about how these decisions are made will be supplied (most settings do not use automated decision making).
- If we are refusing to comply with the request, we will send the requestor a letter explaining our decision and outlining their right to complain to the Information Commissioner.
- A record will be kept of our efforts to comply with the request, the date that we provided the information and any correspondence in case of future investigations by the ICO.

## Data Breach Procedure

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes both accidental and deliberate events. Parents/carers and staff can make a complaint to the ICO if they feel their individual rights have been breached.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

## Responsibilities of Busy Bees staff, Committee members and volunteers

All staff, Committee members and volunteers will:

- Take steps to ensure the security of personal data at all times.
- Know how to recognise a personal data breach.
- IMMEDIATELY report any data breach of which they become aware to the Data Protection Lead (Jane Burris). Prompt action is essential, because reports to the Information Commissioner's Office must take place within 72 hours of the breach being discovered.
- Record the nature of the breach and the action they have taken on a Data Breach Form.

## Responsibilities of the Data Protection Lead

Dealing with a personal data breach must be treated as an urgent priority and given adequate resources.

1. Assessment Assess the severity and likelihood of the potential adverse risks of the breach – *'Level of Risk'. This assessment will include:
2. • Nature of data involved
3. • Sensitivity of data
4. • Security mechanisms in place e.g. password protection
5. • Information which could be conveyed to a third party about the individual
6. • Number of individuals affected by the breach

2. External Reporting Based on the assessment, decide whether the breach requires external reporting to the Information Commissioner's Office (ICO). If it needs reporting, this must be done within 72 hours of the initial discovery of the breach even if full details are not yet known. Reasons must be given for any delay. Failure to notify the ICO when required to do so can result in a significant fine. The individual/s concerned will also be notified directly and without undue delay. We will also notify other Data processors/Data controllers

## Reports to the ICO must include:

- A description of the nature of the personal data breach, including:
- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of Busy Bees DPL.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken or proposed to be taken to deal with the breach, including measures to mitigate any possible adverse effects.

## Reports to individuals must be in clear and plain language and must include:

- The name and contact details of the Busy Bees DPL.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken or proposed to be taken to deal with the breach, including measures to mitigate any possible adverse effects.
- Reports to data processors and data controllers must be according to their contracts.

3. Containment and Action Decisions will be made on what action needs to be taken to contain the breach and by whom, what action can be taken to recoup losses and/or limit damage caused by the breach and all relevant individuals will be informed of the action they need to take.

4. Internal Investigation and Review We will:

- Carry out an internal investigation into how the data breach occurred.
- Determine whether the breach was a result of human error or a systemic issue.
- Identify ways of preventing a recurrence e.g. through better processes or training.
- Review and update processes as appropriate.
- Review and update training and information for staff, volunteers and Trustees/Committee members as appropriate.

5. Recording and Internal Reporting We will:

- Record full details of the breach, its effects and all decisions and action taken on a Data Breach Reporting Form.
- Provide a written report on the breach to the Committee/Trustees/Senior Management team.

## <u>Responsibilities of Trustees/Committee Members</u>

• Individual Trustees/Committee Members have the same responsibilities as employees and volunteers, as stated above.

• The Trustees/Committee Members are responsible for advising the DPL, for receiving and making reports on data breaches, and for reviewing the Busy Bees response to data breaches.

## Level of Risk Low:

Low risk breaches may lead to possible inconvenience to those who need the data to do their job, such as the loss of, or inappropriate alteration of a telephone list. These should be dealt with internally but not reported to the ICO.

High:

These are risks which may have adverse effects on individuals such as emotional distress and physical or material damage. They may include:

- Loss of control over personal data
- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation
- Significant economic or social disadvantage