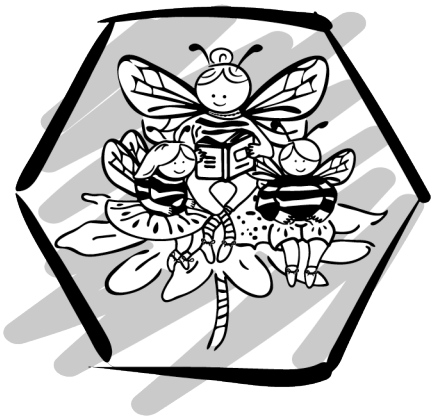

BEES KNEES NURSERY SCHOOL

Data Protection Policy

Bees Knees is required under the Data Protection Act to collect and hold only that data which enables the organisation to carry out its day to day operations.

To ensure that all staff are aware of the obligations for the safe storage, usage and destruction of data the following **Golden Rules** must be observed**:**

- Treat everyone as you would wish to be treated: fairly, politely and without discrimination.
- Be open in all your work, while respecting justifiable confidentiality.
- Only ask for personal information if you really need it and ensure that individuals understand the purposes for which information about them will be used.
- Do not disclose such information to others without good reason. If in doubt, seek advice from the manager.
- Make sure all decisions (especially those that deny someone something) can be seen to be fair and reasonable:
- Avoid expressing opinions about people – orally or on paper, on computer or elsewhere - that cannot be substantiated by the facts.

1. **Responsibilities**
    a. The Manager will be responsible for full compliance of the nursery with the Data Protection Act. Personal data stored anywhere else must be afforded the same level of compliance as that stored in the files in the store cupboard.
    b. All staff will be expected to be working towards compliance at all times and regular review of personal data held should be undertaken.

2. **Good Practice for Processing data**

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to countries without adequate protection.

a. Some definitions within the meaning of the act are:

Personal Data- Data, either factual or opinion, relating to the individual who can be identified by that data.

Processing - Data that is collected, stored or retrieved by an employer

b. Information used for future planning such as pay review or other management forecasting is excluded.

3. Sensitive Data

Sensitive data may not be held about a staff member or service user without their express permission unless it is in compliance with our legal obligations e.g. health and safety, or to protect the employees vital interests. Such information may also be retained as long as necessary for defending a complaint of unlawful discrimination or as a means of monitoring, promoting or maintaining our Equal Opportunities Policy.

4. Access to Data

If a member of staff, a volunteer, service user or other person has concerns about the nature, content, accuracy or relevance of personal data held about them they may write asking Busy Bee to provide:

- A description of the data.
- An explanation of the purpose for which the data is being held.
- The names of persons in the organisation to whom the data is routinely OR occasionally disclosed.

Such requests will be dealt with by the Data Protection Officer who will provide a response within 40 days.

Staff members can request in writing that certain information be deleted from their personal data files on the basis that retention or processing such information could lead to substantial and unwarranted damage or distress.

5. Failure to Comply

Failure to comply with the 8 principles of the Data Protection Act may result in enforcement notices being served on an employer by the Data Protection Commissioner. Failure to comply with any such notices issued is an offence. It is an offence to obstruct the Data Protection Commissioner or his/her Officers in the execution of their powers.

6. Housekeeping Procedures

Managers must undertake a regular 'spring clean' of files to ensure that the data they contain is:

- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary

The Manager must check the contents of files for 'sensitive' data. If sensitive information is found then it should be removed or the employee must be advised and given an explanation, if necessary, for the reasons for keeping such information. Written permission must be given by the employee to continue to keep such information.

- Managers should ensure staff understand their rights under the Data Protection Act.

7. Data Protection in Practice:

a. Staff and Volunteers

Staff members and volunteers should familiarise themselves with this policy and should be aware that failure to comply with it may result in formal disciplinary action.

b. Service Users

The Data Protection principles also apply to data held on service users. Exemptions may apply in specific circumstances and you should seek further guidance from the Data Protection Officer where appropriate.

Particular difficulties apply where data is shared between a number of agencies or service providers. The Manager will be responsible for ensuring that appropriate operational guidance on data protection is prepared for each project and that data protection compliance is achieved.