**DATA PROTECTION POLICY**

**Statement of Intent**

The pre-school’s work with children and families will sometimes bring us into contact with confidential information. We will respect the privacy of children and their parents and carers, while ensuring that they access high quality early years care and education in our setting. We aim to ensure that all parents and carers can share their information in the confidence that it will only be used to enhance the welfare of their children. There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the Data Protection Act and the Human Rights Act.

**1.0 Introduction**

1.1 This document sets out the role of staff responsible for collecting, storing and retrieving employee and service user records.

1.2 The Data Protection Act 1998 came into force on 1st March 2000. The organisation aims to ensure that all employee and service user data are processed in accordance with the Data Protection Act 1998.

**2.0 Data protection principles**

2.1 The 1998 Act lists eight data protection principles relating to the processing of personal data held on computer systems and manual (paper) filing systems which are structured by reference to individuals.

2.2 Records kept on personal files can be processed only if specific conditions are met. These conditions include:

* the data must have been obtained fairly and lawfully;
* the processing is necessary for the performance of a contract with the individual;
* the data must be adequate, relevant and not excessive in relation to the purpose or purposes for which it is kept;
* the data must be accurate and, where necessary, kept up to date;
* the data must not be kept for longer than is absolutely necessary;
* the data must be held in compliance with an employee’s rights of access to personal data, must not be processed in a way calculated (or likely) to cause damage or distress to an employee, and must be corrected, erased or destroyed if inaccurate or no longer relevant;
* the data must be protected (by the best available means) against unauthorised access or disclosure and against accidental loss, damage or destruction; and must be treated as confidential by the staff to whom they are entrusted; and
* the data must not be transferred to any country or territory outside the European Economic Area (EEA) whose data protection laws or codes are non-existent or less than adequate – unless the employee agrees otherwise or the transfer is necessary for employment purposes (e.g. a proposed transfer or secondment overseas).

**3.0 Sensitive data**

3.1 Generally, where data relating to an employee/service user are of a sensitive nature, explicit consent must be obtained from the employee/service user to process the data and hold them on the individual’s personal file. Sensitive data consist of information about an individual’s:

* racial or ethnic origin;
* political opinions;
* religious or other beliefs;
* trade union membership (or non-membership);
* physical or mental health;
* sex life or sexual orientation; or
* criminal convictions, proceedings or alleged activities.
  1. Further guidance can be obtained from the Personnel Department.

**4.0 Ensuring that records are accurate**

4.1 Employees have to be told what information is being collected, the purposes for which it will be used and whether it will be made available to anyone else.

4.2 The administration manager will send a copy of such personal data to each employee to sign and return at least once every two years. Employees are required to read this information carefully and inform the designated person at the earliest opportunity if they believe that any of their personal data are inaccurate or untrue, or if they are dissatisfied with the information in any way. A copy of the personal data to be sent is attached as appendix 1.

**5.0 Access to personal data**

5.1 Employees are allowed to have access to all personal data about them held on manual or computer records under the Data Protection Act (1998). The Act requires the organisation to action requests for access to personal data within 40 days.

5.2 Should an employee request access to their personal data, the request must be addressed in writing to the relevant line manager. The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The employee will be informed whether or not the request is to be granted. If it is, the information will be provided within 40 days of the date of the request.

5.3 In the event of a disagreement between an employee and the line manager regarding personal data, the matter should be taken up under the charity's grievance procedure.

5.4 Where employees make requests for access to their personal data which are granted, a fee of £10.00 will be charged which must be paid to the charity before a copy of the personal data will be provided.

* 1. The right of employees to see information held about them is extended to information held in paper record-keeping systems as well as computerised systems.
  2. There are some exemptions; for example employees will not be able to see employment references about them supplied in confidence, nor will people involved in negotiations with the data controller be able to see information about the data controller's intentions in relation to those negotiations.
  3. Employee data cannot be used for direct marketing (including fundraising) if the data subject objects. Approval to use employee data for marketing purposes must be sought from the Director of Communications.

**Legal Framework**

Data Protection Act 1998 **(**<http://www.legislation.gov.uk/ukpga/1998/29/contents>)

Freedom of Information Act 2000

Human Rights Act 1999

The Children Act 2004, 2006 (Every Child Matters)

**Statutory Framework**

Statutory Framework for the Early Years

Section 3: The Safeguarding and Welfare requirements 3.67-3.72

**Guidance**

Please see separate Safeguarding Children and Data Protection Policy.

Signed at trustees meeting.............................................................................................

Date...........................................................................

Adopted at staff meeting..............................................................................................

Date............................................................................

Review Date................................................................