# Sutton Outdoor Preschool

## Data Protection Policy

Reviewed October 2019

Reviewed by Elizabeth Leddy - Preschool Manager

**Introduction**

Sutton Outdoor Preschool is committed to safeguarding and promoting the welfare of children, and expects all staff, students and volunteers to share this commitment. We are required by the EYFS Statutory Framework to hold data concerning the children, staff, parents and other users of the setting and take our responsibilities of the safe management of such data very seriously.

**Policy Statement**

This policy details how we strive to protect those for whom we hold data as required by the Data Protection Act 1998 which regulates the use of "personal data" and "sensitive personal data". These mean data held either on a computer or in a paper-based filing system which relates to a living individual who can be identified from that data.

Data is information which:

a. is being processed by means of equipment operating automatically in response to instructions given for that purpose;
b. Is recorded with the intention that it should be processed by means of such equipment;
c. Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
d. Does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defines by Section 68 of The Act; or
e. Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

**Responsibilities**

In order to ensure the smooth operation of the setting and to meet the EYFS Statutory Framework, it is necessary for us to hold various data concerning the children, staff, parents and other users of the setting. Such data may include (but is not limited to):

- The full name and date of birth of each child;
- The name and address of every parent and/or carer who is known to our setting (and information about any other person who has responsibility for the child);
- Emergency contact details including the name, telephone numbers and address for each person (other than the parent/carer) named on our registration forms to collect the child in an emergency;
- The name, home address and telephone number of all staff, students and volunteers;
- Health and/or medical information relating to children, staff, students and volunteers;
- Employment information such as bank account details for staff.

Personal data relating to employees may be collected for the purposes of:

- recruitment, promotion, training, redeployment and / or career development, such as references, CVs and appraisal documents;
- administration and payment of wages, such as emergency contact details and bank/building society details;
- calculation of certain benefits including pensions;
- disciplinary or grievance issues;
- performance management purposes and performance review;
- recording of communication with employees and their representatives;
- compliance with legislation;
- provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers; and
- staffing levels and career planning.

Sensitive personal data includes information relating to the following matters:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health or condition;
- sex life; or
- the commission or alleged commission of any offence by you.

We are registered with the Information Commissioners Office (ICO) and process information and data according to the Eight Data Protection Principles, those being:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

**Processing of sensitive personal data**

Sutton Outdoor Preschool will process sensitive data primarily where it is necessary to enable the Sutton Outdoor Preschool to meet its legal obligations and in particular to ensure adherence to health and safety and vulnerable groups protection legislation or for equal opportunities monitoring purposes. In most cases, the Sutton Outdoor Preschool will not process sensitive personal data without your consent.

In conjunction with the Managing Directors, the Managers oversee and are responsible for the safe management of data held. Their responsibilities include:

- Keeping abreast of current legislation, making informed decisions about what records and personal information the setting will hold and how it will be held or used.
- Ensuring the setting remains compliant with the Data Protection Act 1998 and the relevant statutory regulations with regard to the processing of personal data i.e. will notify the Information Commissioners Office and pay the relevant fee.
- Sharing information with others on a strict need to know only basis.
- Ensuring staff are fully aware of what is good Data Protection practice and their roles and responsibilities in adhering to this.
- Ensure staff value and appreciate its sensitivity and are fully aware of what the consequences are of breaching the rules and procedures.
- Ensure everyone managing and handling personal information is appropriately trained to do so and appropriately supervised.
- Take appropriate technical and organisational security measures to safeguard personal information. This will typically include secure storage of data and staff training.
- Set out clear procedures for responding to requests for information.
- Regularly review and audit the way that personal information is held, managed and used.

**Accuracy of Data**

The Company will review personal data regularly to ensure that it is accurate, relevant and up to date.

To ensure the Company's files are accurate and up to date, and so that the Company is able to contact you or, in the case of an emergency, another designated person, you must notify the Company as soon as possible of any change in your personal details (e.g., change of name, address, telephone number, loss of driving licence where relevant, next of kin details, etc).

**Security of personal data**

The Company will ensure that personal data is not processed unlawfully, lost or damaged. If you have access to personal data during the course of your employment, you must also comply with this obligation. If you believe you have lost any personal data in the course of your work, you must report it to your manager immediately. Failure to do so may result in disciplinary action up to and including dismissal without notice.

Staff have open access to their own personal files but are not permitted to access any other files. In order to enforce this, personal files are stored in a lockable unit and can only be accessed with a manger present. Staff's personal files are kept for a period of six years after their employment with the company comes to an end.

The children's personal files, which hold their medical records, home address, parents contact details and dietary information, are kept for a minimum of three years after they leave the setting. Parents have the right to access their own child's record but cannot access any other child's.

Sharing or disclosure of personal information about children or staff would be carried out in accordance with our policy for Information Sharing.

In line with GDPR requirements, Elizabeth Leddy is the named Data Protection Officer for the setting.

| **Policy last reviewed on** | **Signed on behalf of the preschool** | **Date of next review** |
|---|---|---|
| *October 2019* | ***E.Leddy (Elizabeth Leddy)*** | *October 2020* |