**Principle**

In order to work effectively, Little Buds needs to gather and process relevant information (data) about the committee, staff, parents, children and professionals and others (data subjects) involved in the day-to-day running of the setting.

A designated person ((Maura McCleary) data controller) will decide what information is required and how it is to be obtained. This information will be handled by (a) person(s) (data processor) acting on the instructions of the data controller.

**Policy**

The setting has implemented this policy to ensure committee members and staff are fully aware of procedures for handling data.

By adhering to this policy, Little Buds will ensure that data is handled properly and confidentially at all times. This applies to data held on paper and by electronic means Little Buds recognizes its responsibility to ensure that all persons acting on behalf of the group are made aware of this policy and receive any necessary training.

**Responsibility**

The management team is responsible for ensuring that all staff and volunteers act in accordance with this policy with delegated responsibility to the leader in charge/manager to follow through.

**Purpose and Remit of Policy**

* Data collection.
* Data storage/security.
* Data updates.
* Data disclosure.
* Data access.
* Data disposal/destruction.

The management team of Little Buds will review this policy annually to ensure that:

* Data is collected fairly.
* Data is adequate, relevant and not excessive.
* Data is accurate and up to date.
* Data is stored securely.
* Data is only retained as long as is necessary.
* New staff/parents/committee are made aware of the policy.

**Data Protection Procedure**

1. Little Buds will comply with:

The terms of the 2018 Data Protection Act and any subsequent relevant legislation

Any guidance on or update to this policy notified by Early Years – the organization for young children.

1. Data Collection

Only relevant personal data will be collected. The person(s) from whom it will be collected will be informed of its uses and of any possible disclosures that may be made.

Systems will be put in place to facilitate updating information held.

1. Data Storage/Security

Manual data will be stored in a secure place only accessible to those with a legitimate reason to view/use that data.

Electronic data (if applicable) will be protected by password. If the computer is connected to the internet, a firewall system will be used.

The computer (if applicable) will be positioned to ensure that information is not visible to a casual observer.

Sensitive personal data, eg medical records/child protection records/interview material, will be stored using a coding system and access will be strictly limited (need to know basis) and recorded.

1. Data Update

Forms will be issued to staff/parents/others to ensure that data held is up to date and accurate (See appendix 3).

Data held will be updated promptly on receipt of the appropriate form. If incorrect or out of date data has been disclosed to a third party, the recipient will be informed of corrected data and this will be recorded.

1. Data Disclosure

The consent of the data subject will be obtained before the group discloses personal information to any organization or individual.

All requests for disclosure will be in writing and telephone enquirers advised accordingly.

In cases of child protection, the law requires the disclosure of information, without consent, to relevant Health and Social Care Trust personnel and PSNI officers.

If a request for information relating to child protection is received by telephone, steps should be taken to ensure that such information is disclosed to identifiable personnel (ie seek verification of identity) and only if the individual is entitled to receive that information (authorization). It is advisable to disclose such information only to those known to be involved in child protection. If doubt exists, ask the enquirer to route enquiry through a known channel. Always call an enquirer back and be very alert if the number given is that of a mobile telephone.

Requests from parents for a printed list of children’s names/addresses will be politely refused. On occasion, first names may be given for Christmas cards or party invites.

Personal data (including images) will not be used in newsletters, websites or in other media without the consent of the data subject. The conditions outlined in will be adhered to strictly.

A record will be kept of any data disclosed so that the recipient can be informed should data be updated/altered at a later date.

1. Data Access

Data subjects have the right to access any personal data held about them.

Any person(s) wishing to exercise this right must make a request in writing to the Data Controller.

The Data Controller will issue the appropriate form.

On receipt of the completed and signed form, the designated Data Controller will make the information available. The information will be made available as soon as possible and within the 28-day period recommended by the Information Commissioner.

Any delay occasioned by the necessity to consult with an appropriate healthcare professional in relation to a data subject’s medical information will be explained in writing to the individual making the request.

1. Data Disposal/Destruction

The Data Controller(s) will review personal data regularly and delete information which is no longer required for the purposes of the group.

The Data Controller(s) will keep a deletion file and record the type of deletion and the date on which it occurred.

The Data Controller(s) will seek advice from the Labour Relations Agency before deleting information regarding the recruitment and selection of employees.

The Data Controller(s) will not delete information relating to accidents on the premises or child protection issues until the required statutory period has expired.

1. Data Breach

In the event of a data breach, all persons whose information is involved will be notified with 72hrs of the breach.

**Information management**

Only information that is required to comply with the regulations of minimum standards will be held by Little Buds:

* Registration forms
* Permission slips
* Observations
* Accident sheets
* Incident sheets
* Complaints

**Document Retention**

Little Buds will only hold on to information until it is deemed unnecessary or is no longer required. The committee has put a time frame on the following documents, which means that they must be destroyed when they have reached the period of time.

* Registration forms, permission slips, observations and complaints- 7 Years
* Accident/incident sheets- until the child has reached the age of 21 years
* Photographs- once the child leaves the group.

**The Disposal of Documents**

When any document is no longer required by Little Buds they will be disposed of by either being shredded on the premises or put in a sealed bag and sent to Restore Data Shred.

**Monitoring**

This policy will be reviewed annually by the management team to ensure it

remains fit for purpose.

This policy was adopted by Little Buds management team.

Signed: ………………………………………………………………………………….

(on behalf of the management team)

Position: ………………………………………………………………………………….

Date: ………………………………………………………………………………….

Reviewed on:

Date: ……………………... Signed: ………………………………………….

Date: ……………………... Signed: ………………………………………….

Date: ……………………... Signed: ………………………………………….