



October 2021

Security Policy

Policy Statement

This organisation recognises its duty to provide an environment where children, staff and authorised visitors will feel safe and secure.

Procedure

1. Objectives

- a. Protection and safeguarding of children, staff and authorised visitors.
- b. Avoidance of theft, loss or damage to goods, property, equipment, resources or records.
- c. Maintenance of parental confidence.
- d. Compliance with Legislation.

2. Appointment of Staff

This will be rigorous.

It is a statutory requirement that before formal appointment, all staff who are to work with children must undergo a satisfactory Disclosure and Barring Service (DBS) check.

References will always be asked for and will always be taken up. The identity of referees will be checked and verified.

3. Risk Assessment

The organisation's security risk assessment covers all areas and involves all staff. Issues covered in the risk assessment include:

- a. emergency evacuations and alarms
- b. fire
- c. child safety indoors and outdoors
- d. IT and Internet security issues
- e. petty theft

- f. serious criminal offences.

4. **Visitors**

It is important to prevent unauthorised entry to the premises at all times.

At Pear Tree Nursery and Pre-School, all visitors must ring the doorbell and wait to be greeted by a member of staff outside the nursery gates. At Lower Covey Montessori Nursery, all visitors must report to the admin office on arrival at the setting.

Visitors are monitored and are always escorted while on the premises.

If a visitor enters the premises and refuses to leave, this behaviour may give rise to a criminal offence. Staff will request the person to leave the premises but should not place themselves in a position of risk. If violence is threatened, if there is a breach of the peace, or a likelihood of this, the police will be informed by an emergency call.

5. **Special Considerations**

Young children need a high level of care and security. No child should be left alone with an adult who has not had a DBS check and staff should ensure that any adult collecting a child has permission and authority to do so.

6. **Arrival and Departure of Children**

Our procedure for the arrival and departure of children is as follows.

- a. On arrival, all children should be signed in with the time of arrival on the Family app.
- b. Staff and parents should be clear as to the moment when care is handed over to staff.
- c. Any child arriving after the usual time should also be signed in on the Family app.
- d. At leaving time, all children should be carefully supervised and only released into the care of their own parent or authorised adult.
- e. If parents want another adult to collect their child, they should inform staff via the office, the day before if possible. This person should then be added as a contact on the child's Family profile. A password should also be set between parents and staff members to use to identify this adult. The password will be noted on the child's profile in 'special notes'.
- f. Where parents are allowed into the premises with the children, the provider must ensure they are not left alone with children (unchecked persons must not have unsupervised access to children).
- g. No person under the age of 18 will be allowed to collect a child.
- h. All children must be signed out on departure, with the time on the Family app.
- i. Any children leaving early should also be signed out on the Family app.
- j. There is a separate procedure to follow if any child is not collected at the appropriate time.

7. Staff Training

The organisation makes every effort to ensure that staff are trained and instructed in appropriate security measures. Staff should:

- a. be aware of the need to safeguard valuables and personal possessions
- b. ensure that visitors and contractors are escorted at all times
- c. politely challenge any unescorted people that they do not recognise
- d. ensure that windows, doors and storage areas are shut and locked at the end of each day.

8. IT Security and Confidential Information

Confidential information is stored on paper, in electronic form or in people's memories.

Written material should never be left lying around. The organisation operates a clear desk policy and filing cabinets must be locked when not in use.

Password access is provided for computers and these should be turned off when not in use. Passwords are held securely, but are accessible to the manager. Electronically recorded data is regularly backed up.

Staff are reminded that their employment contract terms include a confidentiality clause, a breach of which would make them subject to the normal disciplinary procedures.

9. Reporting and Recording Breaches of Security

Any breach of security or potential breach of security should be reported immediately to a senior member of staff who should then launch a thorough investigation and take appropriate action.

Signed: _____

Date: _____

Policy review date: _____