Data Handling Policy

This policy covers the Data Protection principles and an individual's rights as set down in the Data Protection Act 1998.

Data which may be held includes the following:

- List of names, addresses and home telephone numbers and emergency contact numbers of children attending and staff, volunteers, students whether on spread sheet, paper or card indexes
- Paper or computer based employee files containing employment records, bank account details and national insurance numbers
- Training records of staff
- Performance records of staff
- Information contained on e-mail which may mention the individual's name
- Laptop computers holding personal data and memory sticks
- Children's assessment, observation records
- Information provided to, or received from, external sources
- Photographs
- Incident reports

This list is not complete and will be subject to change

Sharing of information

Information sharing is essential to meet the needs of the children and families who attend. Data may therefore be shared with and may be obtained from:

- Staff members / students / volunteers
- Schools
- Local settings and other childcare providers
- External agencies such as Local Safeguarding Children's Board, Local Authority etc.

Security of information

We will ensure that measures are taken to safeguard personal data. Each individual has a personal responsibility to ensure that any information of a personal or sensitive nature to which he/she has access in the course of his/ her work is protected from unauthorized access and disclosure. In particular, individuals must observe the following rules:

- Electronic storage of such material should be password protected
- Paper copies of personal data must be held in secure cabinets
- Information should be labelled as 'personal'
- Individuals must not disclose personal information except to authorized colleagues Particular care must be taken when exchanging information with third parties.
- Information must not be used for purposes other than that for which it was intended
- If records are taken off site (e.g. on laptops/memory sticks), appropriate security measures should be taken (e.g. laptops should never be left unattended in vehicles, and they should

be stored securely off site)

- All employees/ students/ volunteers must sign a confidentially agreement
- Where paper based documents are removed from records these must be confidentially shredded.
- Personal data should not be retained for longer than necessary
- Memory sticks, discs etc. will be only used by authorized people and will be stored securely when not in use.