**DATA HANDLING POLICY**

This policy covers the Data Protection principles and an individual’s rights as set out 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 spreadsheet, 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.
* Children’s assessment/observation records.
* Information provided to, or received from, external sources.
* Photographs.
* Incident reports.

This list is not exhaustive and will be subject to change.

Sharing of information

Information and 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.
* External agencies such as Local Safeguarding Children’s Board, local authority etc.

Security of information

Oscar Club 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 unauthorised 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 will be labelled confidential.
* Individuals must not disclose personal information except to authorised 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 (eg. on laptops), appropriate security measures should be taken (eg. laptops should never be left unattended in vehicles and they should be stored securely off site).
* All employees/students/volunteers must sign a confidentiality 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 authorised people and will be stored securely when not in use.

Signed on behalf of the Voluntary Management Committee \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Review Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_