Data Protection Policy

This policy defines the arrangements in The Parachute Club that assures compliance to the requirements of The Data Protection Act, 1998, as relevant to The Parachute Club's business interests:

Introduction

1. The data protection act 1998 addresses certain requirements for all organisations that collect and process personal data as part of their on-going business operations. Personal data is defined by: information relating to an 'identifiable living individual' and will therefore, apply to The Parachute Club's clients (children attending club and their parent/guardians) and employees.
2. The data protection act 1998 applies to any data recorded in a filing system that allows personal data to be easily accessed.
3. The data protection act 1998 applies to records kept in hard copy (paper) format or computer files.

Principles of data protection

1. The Parachute Club is committed to the enforcement of the following code of good practice in relation to the data it keeps on its children and employees. In summary the data will:
    a. Be fairly and legally processed
    b. Be relevant to the needs of the club
    c. Not be unnecessarily excessive in detail
    d. Be accurately maintained
    e. Not be kept longer than necessary or required by law
    f. Only be used in accordance with the individual subjects rights
    g. Be securely stored
2. The following policies are also relevant
    a. Safeguarding Policy
    b. Managing Allegations against staff and Volunteers

Policy details

1. The Parachute Club will require written consent from each individual child's parents/ carer. In order for personal data to be collected and processed. In this respect it will be taken that consent is implied through the following.
    a. Clients – the parent/ carer who signs the registrations forms and other consent/ booking in forms
    b. Employees – by completing the job application form at the onset of their employment and has not registered and objection to their data being used.
2. All individual parent/carers and employees have the right of access to manual and computerised records when concerning their personal data.
3. Where it is deemed necessary to divulge to a third party this will only be done with consent of the client/ employee

4. Personal data and records will be maintained under appropriate conditions of security to prevent any unauthorised or accidental disclosure. Records can be hard copy or computer files. Particular attention is paid to the following aspects of record storage

    a. *Hard copy file*
        i. Identification of storage
        ii. Identification of those employees who have access
    b. *Computer file*
        i. Password protection for access to data sensitive files
        ii. Who is authorised to have knowledge of these passwords
        iii. Back up, control and management of what are essentially copies of personal data
5. When personal data is being processed, staff will take reasonable precautions to prevent sighting of data by unauthorised persons:
    a. Record files are locked away when not in use
    b. Where practical computer screens should be tilted towards the user and away from general view

This policy will run in hand with the new General Data Protection Regulation Policy