DATA PROTECTION POLICY

1) The Daisy and Rainbow Childcare Board of Trustees supports the objectives of the Data Protection Act 1998. The GDPR 2018 have further given structure to our systems and procedures.
2) Our information systems are structured by reference to an individual or by criteria relating to them. An example of a relevant filing system would be an employee's personnel file or a Child's registration Document.
3) The Board of Trustees expects all employees to abide fully with this policy and the Data protection act principles.
4) Our settings will hold the minimum personal information necessary to enable them to perform their functions. This information will be erased once the need to hold it has passed. Every effort will be made to ensure that information is accurate, up-to-date and that any inaccuracies are corrected without unnecessary delay.
5) Personal information is confidential. Any Information held will only be disclosed with the written consent of that individual or, if a minor, his/her legal guardian's/parent's consent. The only exception to this will be in response to the direction of a Court Order or disclosure required by law for crime detection and prevention.
6) The charity is registered as a data Controller with the Information Commissioner's Office.
7) This policy should be read alongside the Daisy and rainbow childcare Privacy Notice
8) To inform our practice and ensure information is held appropriately over the appropriate timeframe we have devised and utilise a Data Records Table .

9) Electronic Data Storage
   - The computers at the settings are networked. Each person who accesses the computer has their own username and password to log in.
   - Separate secure drives are in operation for financial, child information and personnel with limited numbers of authorised personnel able to access these files.
   - Access to the;
     - Finance drive – CEO, Administration Manager.
     - Personnel drive – CEO, Administration Manager.
     - Children drive – CEO, Administration Manager, Setting Managers and Deputies.
   - All child protection records are loaded directly or scanned to the Childs own named folder on the secure Drive. These records are further password protected
   - All personnel information is entered directly or scanned to the employee / volunteer or student's own folder on the secure Drive.
   - Google Forms are used to gain data from parents regarding their child and their family – data is erased from this as soon as it is transferred successfully to Access and / or the Child's named folder on our secure drive.
   - We use Microsoft Access to collate and hold all raw data regarding the children this may be accessed by all managers and deputies.
   - We use iPhones in the settings to communicate directly with parents, the team, and other professionals. The iPhones are passcode protected, data is backed up to iCloud.
   - Laptops are linked to the Netowrk, password protected to access and locked away when the setting is closed.
   - Data saved on each physical server is backed up to a removable hard drive which is changed weekly and kept at the other setting.

10) Storage of Paper Records
   - The minimum of paper held records will be utilised, preference given to the use of electronic storage of data.

- Any necessary family contact data which is held in print form will be kept in a folder which is locked away when the building is closed.
- Attendance registers will be kept in a file in the office or lockable cupboard.
- Any paper records which need to be retained will be kept in one of the administration offices or in the Daisy store. Any records that become non-essential will be destroyed.
- The data held on the registration forms may be updated as parent / carers advise us of any changes.

Child Data

11) We use WhatsApp as our Primary means to share and receive photographs and written communication with the parent carers. This form of communication is end-to-end encrypted.
12) All images of children will be stored on a password protected computer and/ or saved to iCloud.
13) Any information about children which is taken legitimately out of the setting will be secured in a locked bag.
14) The current registers and Child Overview documents are held on 365, accessible only to Managers and Deputies as appropriate to each document.

Finance and Personnel

15) Payroll information will be password protected and only accessible by the CEO and Finance Manager.
16) All personnel will be aware how their data is used and will be aware when we make that information available to other parties – i.e. HMRC and the pension provider.
17) All staff undergo a DBS check – the clearance result is held on file on a Central secure record for Ofsted purposes. All other personnel information is held in a named folder on the secure Personnel computer Drive. Supervision records are held on the separate Childrens Drive.
18) Disciplinary action will be taken if unauthorised disclosure of information from computer input or output or from any other hand-written records, held within the setting, is made to another party.
19) Individuals have the right to view any information held about them or their children. Children's attainment records will be shared freely with the parents/guardians and via WhatsApp Parents/guardians will be responsible directly for completing child registration documents and family information forms.

Policy formulated on: _____
Policy last reviewed on: Nov 2018
Current Date Feb 24
Signed: M Parker