

# **CONFIDENTIALITY POLICY**

## **Statement of intent**

It is our intention to respect the privacy of children and their parents and carers, whilst ensuring that they access high quality early years care and education in our setting.

## **Aim**

We aim to ensure that all parents and carers can share their information in the confidence that it will only be used to enhance the welfare of their children.

## **Methods**

We keep two types of records on children that attend our setting:

### **1. Developmental records**

- These include observations of children in the setting, samples of their work, summary developmental reports and records of achievement.
- They are kept in a secure cupboard, and can only be accessed, and contributed to, by staff, the child and the child's parents.

### **2. Personal records**

- These include registration and admission forms, signed consents, and correspondence concerning the child or family, reports or minutes from meetings concerning the child from other agencies, and observations by staff on any confidential matter involving the child, such as developmental concerns or child protection matters.
- These confidential records are stored in a lockable file in our secure cupboard and are kept secure by the playgroup leader and the playgroup manager. Information will not be shared without the consent of parent/carer, unless required to do so by law.
- Parents have access, in accordance with the access to records procedure, to the files and records of their own children but do not have access to information about any other child.
- Staff will not discuss personal information given by parents with other members of staff, except where it affects planning for the child's needs or when there are concerns about the child's welfare. Staff induction includes an awareness of the importance of confidentiality in the role of the key person.

## **Other records**

Issues to do with the employment of staff, whether paid or unpaid, remain confidential to the people directly involved with making personnel decisions.

### **Access to personal records**

Parents may request access to any records held on their child and family following the procedure below:

- Any request to see the child's personal file by a parent or person with parental responsibility must be made in writing to the Playgroup Manager.
- The setting commits to providing access within 14 days - although this may be extended.
- The Playgroup Manager and Key Person prepare the file for viewing.
- All third parties are written to, stating that a request for disclosure has been received and asking for their permission to disclose to the person requesting it. Copies of these letters are retained on the file. 'Third parties' may include all family members who are referred to in the records.
- It also includes workers from any other agency, including social services, the health authority, etc. It is usual for agencies to refuse consent to disclose, preferring the individual to go directly to them.
- When all the consents/refusals to disclose have been received these are attached to the copy of the request letter.
- A photocopy of the complete file is taken.
- The Playgroup Manager and the Key Person go through the file and remove any information which a third party has refused consent to disclose. This is best done with a thick black marker, to score through every reference to the third party and information they have added to the file.
- What remains is the information recorded by the setting, detailing the work initiated and followed by them in relation to confidential matters. This is called the 'clean copy'.
- The 'clean copy' is photocopied for the parents who are then invited in to discuss the contents. The file should never be given straight over, but should be gone through by the Playgroup Leader, so that it can be explained.
- Legal advice may be sought before sharing a file, especially where the parent has possible grounds for litigation against the Playgroup or another (third party) agency.

All the undertakings above are subject to the paramount commitment of The Community Playgroup's staff members and volunteers, as our main priority is the welfare and well being of the child. Please see our Safeguarding Children policy.

### **Confidentiality Issues Regarding Safeguarding**

All staff members have attended the Safeguarding Foundation Level Training, which has equipped them with the knowledge and understanding that the child's welfare is paramount, and that the child is our main priority at all times.

Under no circumstances should disclosure information be kept confidential. The Playgroup Manager must be informed immediately, and it is the Managers duty to then contact Social Services and make a referral.

Disclosures must be dealt with on a 'need to know' basis, and the Playgroup Manager will inform the relevant parties. Therefore disclosures should not be discussed with any other members of staff, children or parents, and should not be shared with friends, spouses etc.

### **Confidentiality Issues Surrounding Personal Property**

All personal property items and their contents, such as coats or bags etc, must remain confidential to the owner. Personal property belonging to staff should not be left in an area which is accessed by the children or their parents and carers.

The Community Playgroups reserves the right to carry out spontaneous personal property searches. Any personal property searches will be carried out by the Playgroup Manager, and will be done in the presence of the items owner and another member of staff as a witness.

All members of staff must be vigilant in ensuring that items of personal property and their content remain private and confidential to the owner. Members of staff and volunteers need to be aware that failure to do so will result in disciplinary action being taken against them, and possibly legal action.

### **The Data Protection Act**

The Data Protection Act's rules are quite complex, but at the heart of it are eight common sense rules known as the 'data protection principles'.

These principles require any organisation, corporation or governmental body that collects personal information to handle it safely. Anyone collecting personal information must:

- fairly and lawfully process it
- process it only for limited, specifically stated purposes
- use the information in a way that is adequate, relevant and not excessive
- use the information accurately
- keep the information on file no longer than absolutely necessary
- process the information in accordance with your legal rights
- keep the information secure
- never transfer the information outside the UK without adequate protection

All organisations collecting and using personal information are legally required to comply with these principles. The law provides stronger protection for more

Document last revised: June 2017

To be reviewed June 2018

sensitive information - such as your ethnic background, political opinions, religious beliefs, health, sexual life or any criminal history. It is enforced by an independent information commissioner, who can take action against any company or governmental body that fails to protect your information, or that abuses its right to collect and hold that information.

**The Freedom of Information Act - the right to see a wide range of public information.**

The Freedom of Information Act gives you the right to ask any public body for all the information they have on any subject you choose. Unless there's a good reason, the organisation must provide the information within 20 working days. You can also ask for all the personal information they hold on you. Everyone can make a request for information - there are no restrictions on your age, nationality, or where you live. You can ask for any information at all - but some information might be withheld to protect various interests which are allowed for by the Act. If this is case, the public authority must tell you why they have withheld information. If you ask for information about yourself, then your request will be handled under the Data Protection Act.

**The Community Playgroups will securely store and deal with any requests for confidential information in accordance with the Data Protection Act 1998, and the Freedom of Information Act 2000.**