Confidentiality Policy

Policy Statement

It is Play Inclusion Project's intention to respect the rights and privacy of children, young people and their parents/carers along with our staff and volunteers whilst ensuring that we deliver a high-quality service. The company recognises that all staff and volunteers have a duty to act in a professional manner and maintain confidentiality. 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 child.

As part of our ethos, we take seriously our responsibility to ensure the protection, health, safety and wellbeing of our children, young people and staff. We expect our staff and volunteers to comply with this confidentiality policy and we will treat breaches of confidentiality as a serious matter.

Guidelines

- Although the emphasis of these guidelines is in relation to service users, the principles of confidentiality apply equally to any member of a service user's family, to information about volunteers, staff, trustees, to information about activities and sessions, and to privileged information about Play Inclusion Project. Responsibility of maintaining confidentiality lies equally with all those aforementioned.

- Maintaining confidentiality is central to recognising and respecting the rights, dignity and privacy of people. In providing care and support to service users, staff will have easy access to privileged and at times sensitive personal information. Whilst it is necessary in providing support to service users that staff and volunteers have ready access to information, it is also important that service users can expect that any personal information will be kept confidential. Whether the information is contained in paper or computer records, or has to be faxed, e-mailed or phoned through to a colleague, consideration must be afforded to maintaining confidentiality.

- All staff and volunteers have a responsibility to maintain confidentiality about any information relating to a service user, staff member, or other information that could give rise to embarrassment or which may be used to the disadvantage or detriment of an individual.

- It is important to recognise that there is a distinction between confidentiality and secrecy. All working relationships should be developed and maintained in

an open, honest and professional manner, sharing information when it is possible and appropriate to do so.

- Access to information should be limited to staff, volunteers and others that are directly involved in providing support to service users. This includes information discussed with the service user, in team meetings, with colleagues or that is contained in a report, care plan or other written document. Any information shared must be justifiable in order for staff and volunteers to perform their professional duties to support the child.

- To avoid accidentally disclosing information, conversations and discussions should be conducted in private and in a discreet manner out of earshot of others. Steps should be taken so as not to leave confidential information out where it may be read by an unauthorised person. Special care must be taken regarding DBS Disclosures.

- Parents and carers should always be asked if they are happy for information to be shared or discussed, and where possible they should take responsibility for sharing the information.

- If a service user wants information about them to be withheld from someone or an organisation, their wishes should be respected with the following exceptions -
    - When there is serious danger to the life of the service user, staff, volunteer or others.
    - When information is required by law e.g. case notes subpoenaed to court.
    - When there is risk of abuse or violence.

Where possible discuss with the service user the need for a breach of confidentiality and the reasons behind this.

- If you have any concerns about sharing confidential information or are unable/not in a position to obtain consent from the service user, you must seek advice from the CEO who will then take responsibility for passing information on to the relevant individuals. If you are unable to speak with the CEO, you must make a decision based on the particular circumstances and keep a note of the actions and reasons for your decision, recording any appropriate information in the service user's file.

- Information required by Play Inclusion Project to carry out an investigation should be made available on request, but only if a justifiable reason is presented. The designated member of staff is responsible for making the information available as necessary. On occasions it may be necessary to

divulge personal information to other relevant people, although a clear assessment should be made of who needs to know what information and in what circumstances. For example, any information about communicable diseases should be shared with those who work with or may come into contact with the service user, but only on a need to know basis.

- There may be circumstances when you receive confidential information, and you are obliged to divulge this information to an appropriate person or authority. For example, if the information were to concern something which would adversely affect a service user or relate to a safeguarding issue it must be reported. When receiving information that is described as confidential you must always explain that dependent on what the information is, you may not be able to maintain the information as confidential.

- Great care and attention should be afforded to record keeping and maintaining accurate records securely. It is not acceptable to record information under the guise of confidentiality that could not be discussed with the service user, their parent, guardian, advocate or key worker. Service users have the right to know what is being written and recorded about them. Information about a service user must never be kept secret from that service user, or their advocate.

- Personal information maintained centrally in the office or in the local service should be kept securely. The designated member of staff with responsibility for confidentiality is responsible for making arrangements about key holders, record keeping and other computer information and passwords. A list of passwords and records of key holders should be kept as appropriate.

- At the end of any working period all information that is of a confidential nature should be securely put away. Information should not be left out or on a computer screen (breaching confidentiality need not be intentional). Any personal information to be disposed should be placed in the Shred-It unit as per the Shred-It All Policy.

- In order to comply with the Data Protection Act, all computers that contain personal information must be secure or programmed so as to be incapable of being accessed, altered, lost or destroyed by an unauthorised person or accident.

- If any person or confidential information is accessed without authorisation or where there is suspicion of such, this should be recorded and reported to the CEO with appropriate remedial action to ensure this is not repeated. If there is a lapse or breach of confidentiality the designated member of staff is

responsible for investigating the matter and taking any necessary steps to limit the effect of such. Detailed records should be kept of any incidents of this nature.

- All employees have the same right to confidentiality in the workplace as service users. Area Managers will not discuss work performance with other staff members. If performance needs to be reviewed it will be discussed with the Recruitment officer and the CEO away from the setting.