



Serving young people and the community

## **Patron: The Duke of Richmond and Gordon**

### **Confidentiality Policy**

It is our intention to respect the privacy of the children aged 8-18 and their parents/carers whilst they access high quality care and therapeutic nurture within our setting.

#### **Aims**

We aim to ensure that all parents/carers feel confident enough to share information on the understanding that it will only be used to enhance the welfare of their children and young people. Our procedures enable us to comply with legislation such as the Human Rights Act 1998 regarding protecting the individual's right to privacy. Our only justification to interfere with this right is where we believe a child may be at risk of significant harm or to prevent a crime. We also comply with the Data Protection Act 2018 and the General Data Protection Regulations (GDPR). This dictates how we gather, store and use the information about the families who use our setting. As an organisation that process personal data, we are registered with the Information Commissioner's Office (ICO). We will only share information about our families with other professionals or agencies on a "need to know" basis, with consent from the parent/carer or without consent in circumstances where there are safeguarding issues. We aim to ensure that all staff, volunteers, and students are aware that information about children and families is confidential and only for use within the setting and to support the child's/young person's best interests with parental permission.

#### **Method**

We keep personal records of children and young people in the setting. These include registration and admission forms, signed consents and correspondence concerning the child or family, an ongoing record of relevant contact with parents and observations by staff on any confidential matter involving the child i.e., developmental concerns or child protection issues. These confidential records are stored in a lockable filing cabinet and are kept secure by the person in charge of the setting, in the office or other suitably safe place. Parents have access to all written information about their child (except where data protection laws stipulate it is against the best interest of the child). A written request must be made to the person in charge of the setting for all personal files on the child. Parents do not have the right to access 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. Staff will also not discuss or partake in any discussion about any other child or their family with any other parents/carers. Staff, students and volunteer inductions include an awareness of the importance of confidentiality in the role of the youth team.

## **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. Students, when they are observing in the setting, are advised of our confidentiality policy, and are required to respect it at all times.

## **Sharing Information.**

There are times when we are required to share information about a child/young person or their family. These are when:

- There are concerns that a child/young person is or may be suffering significant harm.
- The 'reasonable cause to believe' a child is or may be suffering significant harm is not clear.
- There are concerns about 'serious harm to adults' (such as domestic violence or other matters affecting the welfare of the parents/carers).

We explain to families about our duty to share information for the above reasons during their induction to the setting. Where we have concerns such as above, we would normally gain consent from families to share. This does not have to be in writing, but we will record in the child's file that we have gained verbal consent as a result of discussing a concern that we need to refer to a social care agency. We do not seek consent from parents to share information where we believe that a child/young person, or sometimes a vulnerable adult, may be endangered by seeking to gain consent. For example, where we have cause to believe a parent may be trying to cover up abuse, or threaten a child. Where we make a decision to share information without consent it is always recorded in the child's personal file and a reason clearly stated. Where evidence to support our concerns are not clear we may seek advice from West Sussex Children's Social Care department. We only share relevant information that is both accurate, factual, non-judgemental and up to date. Access to personal records Parents/carers may request access to any personal records held on their child and family following the procedure below.

Any request to see the child's personal records by a parent or person with parental responsibility must be made in writing to the Chairman of the Trustees.

The Chairperson will send a written acknowledgement.

The setting commits to providing access within 14 days- although in some circumstances this may be extended.

The Chairperson will prepare the file for viewing.

All third parties are written too, stating that a request for disclosure has been received and asking for their permission to disclose to the person requesting it. A copy of these letters are retained on the child's file.

'Third parties' include all family members who may be referred to in the records. It also includes workers from any other agency, including social services, the health authority etc. It is usual for the agencies to refuse consent to disclose, preferring the individuals 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 Chairperson will go through the file and remove any information which a third party refused consent to disclose. This is best done with a thick black marker, to score through every

reference to the third party and any information they have added to the file. What remains is the information recorded by the setting, detailing work initiated and followed by them in relation to confidential matters. This is called a clean copy. The 'clean copy' is then photocopied for the parents who are then invited into the setting to discuss the contents. The file should never be given straight over, but should be gone through by the Chairperson, in order that it can be fully explained. Legal advice may be sought before sharing a file, especially where the parent/carer has possible grounds for litigation against the setting or another (third party) agency. Procedure for transporting confidential documents. There may be occasions where developmental records may need to be completed/updated outside of the setting. These will only be held by the Youth Development Leader, who will be responsible for ensuring the security of these documents and that they are the only person who can view them. On the rare occasion that personal records may need transporting to other agencies/professionals, they will be hand delivered by an authorised person at the setting. (We will ensure that we have parental permission to do this, except when to do so may result in serious harm to the child.) If personal files need to be relocated for any reason to another place of safety the chairperson of the trustees will transport the locked file with the key. The file will then be stored by the nominated person in a place of safety. Permission to store files offsite will be sought from Ofsted. Any confidential information no longer required will be disposed of by secure shredding.

### **Electronic messaging and social networking.**

No members of staff, students or volunteers are allowed to discuss children/young people, parents/carers or anything to do with the setting on any social networking sites. Emails containing information about parents/carers and children/young people should be kept brief and only initials used. Personal information about children/young people, parents or carers must not be looked at by students on placement unless specific consent has been given by a parent/carer for a specific reason. Care should be taken when speaking on the telephone that no information is given on a child unless speaking directly to the parents/carers, emergency contacts or professionals from other agencies such as social services. If you are ever in doubt, verify or seek advice and call back. Any breach in confidentiality will be regarded as a serious offence.

### **Mobile phone policy**

We do not allow the use of personal mobile phones during any club hours, on the premises either indoors or in the outside play area. Mobiles belonging to staff should be switched off and kept in a secure place away from the children. If staff do need to be contacted in case of an emergency, it is acceptable to use the settings phone number to do so. This ban excludes offsite trips where the youth team maybe separated and required to contact each other for the sole purpose of safeguarding the children/young people in the community. In this case the mobile phones will not be used to photograph the children. All parents and visitors will be advised of this policy during their induction into the setting. Parents and visitors will be asked to ensure they adhere to it at all times. Further information on the use of mobile phones is within the setting's Safeguarding Procedure.

Please read this policy alongside our:

Safeguarding children policy

Staff Conduct and Behaviour Policy

Social Media Policy

Data Protection Policy

Policy Date: 4 December 2024

Review Date: December 2025

Signed:

A handwritten signature in black ink, appearing to be 'M. D.', with a horizontal line extending to the right from the end of the signature.