October 2018

SHIRLEY CHILDREN'S CENTRE
CONFIDENTIALITY POLICY AND GUIDELINES

This policy links to the following:

- Whistleblowing Policy
- GDPR Policy

Document control

Amendment History

Version/Issue Number	Date	Author	Remarks/Reason for change	Review Date
1	October 2014	Eyullahemaye Henry-Miller	To be ratified by the governing body	October 2015
2	October 2015	Eyullahemaye Henry-Miller	Review	October 2016
3	October 2015	Eyullahemaye Henry-Miller	Review	October 2017
4	October 2018	Nicky Cook & Katie Coomber	Reviewed	October 2019

CONFIDENTIALITY GUIDELINES & POLICY

Statement of Intent
It is our intention to respect the privacy of the children and families who have access to Shirley Children's Centre, whilst they have access to high quality service provision within our centres.

Aim
We aim to ensure that all professionals, parents and carers can share their information in the confidence that it will only be used to enhance the welfare of the children. Details of other people should only be shared on a "need to know" basis. Any details of a personal nature will only be disclosed with the consent of the person involved. Information is gathered by staff members during the course of their work and in some circumstances this information will not be stated as confidential and staff members may have to exercise common sense and discretion in identifying whether information is expected to be confidential. If a staff member is in doubt they will always seek the advice of their line manager.

Methods
The children's centre holds two kinds of records on children and their families attending the centre.

Personal Records
These include registration forms, signed consents and correspondence concerning the child or family, reports or minutes of meetings from other agencies or staff concerning the child, an ongoing record of relevant contact with parents and observations made by staff on any confidential matter involving the child such as developmental concerns or safeguarding issues.
All confidential records are stored in a lockable cabinet and are kept secure by the centre manager and other centre staff. Ultimate accountability lies with the children's centre manager.
Parents have access to the records in accordance with the Freedom of Information Act in relation to records of their own child, but do not have access to information about any other child or family.
Staff will not discuss personal information given by parents with other staff members, except where it affects planning for the child's needs, or where there are concerns for the child's safety.
All members of staff sign to say they have read and understood Shirley Children's Centre Confidentiality Policy and Confidentiality Statement

eStart Records
Parents and carers of all children attending the children's centre complete a Best Start registration form. At the bottom is an agreement that parents sign to permit Shirley Children's Centre to store information on the eStart database. Attendance at all sessions in the children's centre is recorded on paper registers and this information is transferred onto the database. Attendance records are kept for Health and Safety and monitoring purposes and are kept securely.

Other Records
Issues to do with the employment of staff, paid or voluntary, remain confidential to the people directly involved with making personnel decisions.
Students on recognised qualifications and training are both CRB checked and advised of the confidentiality policy and have to sign to agree to adhere to it.

Maintaining confidentiality
It is important that all sensitive information is properly respected at all times.

Storage
Any sensitive information should not be left unattended in areas with public access. Confidential information should be locked files when not in use. Restricted information should be kept in a secure location and only unlocked for authorised use. Such information should be held away from general information such as personal files.

Electronic Information
This should always be password protected and portable storage devices holding confidential information should be locked away. Any person seeking access to personal data about themselves should request access from the Data Protection Officer at Croydon Council. Electronic information should be sent using a secure email such as EGRESS.

Written communication
If you send confidential information internally it should be in a closed file or envelope marked “confidential” and if possible delivered by hand. Information delivered that is marked “confidential” or “private and confidential” should be opened by the centre manager only. If the centre manager is away, the delegated person should open the information. If the information is marked “personal” it must be given to the addressee only.

If you hold public access files you must remove any unnecessary reference to sensitive confidential information before files are made available. You should not code confidential information on files, nor record judgmental comments about a person. Professional judgements must be marked as such.

In administering, filing, printing, typing or faxing confidential information you should ensure that it is undertaken by a person who understands the confidentiality procedures. It is essential that confidential material is not left in machines after processing.

All confidential documents should be disposed of by shredding and documents awaiting shredding kept in sealed bags (locked away if unattended).

It is important that out of date documents are removed and shredded from files regularly.

Restricted documents should not be taken from the children’s centre without agreement for transport and storage. They must not be left unattended in cars or opened on public transport. Restricted files should never be kept at home unless arrangements have been made for secure storage. Storage at home should be secure and away from other household members.

Meetings, courses and conversations should observe the same standards as written information, making levels of confidentiality clear or seeking clarity, if you are not told of the confidentiality level. On training courses this should be explicit from the outset.

Care should be taken when providing or receiving information by telephone. It is your duty to ensure that you are speaking to the appropriate person. If contacting clients by phone you should check with the client that it is secure and agree procedures for leaving messages.

All confidential conversations should take place in privacy where no one else can see or overhear. This applies to spoken and signed conversations.

Non English speaking/writing families
All translation and interpretation staff handling sensitive information must have been trained to maintain confidentiality. They are expected to follow published confidentiality arrangements and as far as possible should be of the gender/ethnicity requested by the family.

Confidentiality regarding Staff Health
Managers need to know how long and why a staff member is absent but they do not need specific medical details. However, where the absence will require changes to working arrangements, more detailed information may be required. Employee's consent will be sought before this information is passed on.

Colleagues do not need to be informed of the reasons of a person's absence however; they will need an indication of the absence period.

Managers should remind staff of the confidentiality requirements if speculation or rumours begin.

All paperwork related to health issues is confidential. It must not be disclosed by staff with legitimate access unless authorised to do so and must not be left open or unattended in files or desks. All personal records should be locked away.

Lost information/Stolen information
A log will be kept of lost, stolen or unauthorised access to confidential documents. Any theft should be reported to the police, emphasising the confidential nature of the documents.

Data Protection Act (GDPR)
Information regarding individuals, whether kept on computer or paper, falls within the scope of the Data Protection Act and must comply with the data protection principles. This personal data must be:

- Obtained and processed fairly and lawfully
- Held only for specified purposes
- Adequate, relevant and not excessive (update check completed every 2 years)
- Accurate and up to date
- Not kept longer than necessary
- Processed in accordance with the act

- Kept secure and protected
- Not transferred out of Europe
- Sharing of information will be in line with the new GDPR regulations

Breach of confidentiality
Employees who are dissatisfied with the conduct or actions of colleagues should raise this with their line manager in the first instance, using the grievance procedure if necessary and not discuss their dissatisfaction outside of Shirley Children's Centre

Staff members accessing unauthorised files or breaching confidentiality may face disciplinary action and possible dismissal. Ex employees breaching confidentiality may face legal action. Final responsibility for breach of confidentiality rests with Shirley Children's Centre

Whistleblowing
Should any member of staff or volunteer have concerns regarding bad practice which may impact on the service delivery of the children's centre they may refer directly to the Whistleblowing Policy

Monitoring Arrangements
This policy will be monitored by the children's centre manager and will be reviewed in line with the document history review date

It is intended that by adopting this policy and keeping staff, volunteers, families and the management committee informed, trained and up-to-date with procedures, the centre can avoid the need for complaints.

However, the Children's Centre Manager is the first point of contact should you have any queries over this policy and its related procedures

Policy Endorsement
This policy is agreed and signed by the governing body of Forest Academy School