Confidentiality Policy

Principals

The nursery's work with children and their families will bring us into contact with confidential information. It is a legal requirement for the nursery to hold information about the children and families using the setting and the staff at the nursery. This information is used for registers, invoicing and emergency contacts. However, all records will be stored in a locked cabinet in line with data protection registration. Regulations on information sharing of the women that is accessing multiple services through Brighton Women's Centre will be outlined in our GDPR Policy.

It is our intention to respect the privacy of children and their families, and we will do so by:

- Storing confidential records in a locked filing cabinet
- Ensuring that all staff, volunteers and students are aware this information is confidential and only for use within the nursery.
- Ensuring all parents have access to files and records of their own children, but not those of any other child.
- Gaining parental permission for any information to be used other than the reasons above.
- Ensuring all staff, through their close relationships with both the children and families learn more about the families using the nursery
- Ensuring that all staff are aware that this information is confidential and only for nursery use. If any of this information is requested, the parent's permission is always sought.
- Ensuring staff do not discuss personal information given by the parents with other members of staff, except where it affects planning for the child's needs
- Ensuring all staff and volunteers inductions include an awareness of the importance of confidentiality in the role of the key person. If staff breach any confidentiality provisions, this may result in disciplinary action, and in serious cases, dismissal. Students on placement in the nursery are advised of our confidentiality policy and required to respect it
- Ensuring staff, students and volunteers are aware of and follow our social networking policy in relation to confidentiality
- Ensuring issues concerning the employment of staff remains confidential to the people directly involved with making personnel decisions
- Ensuring any concerns/evidence relating to a child's personal safety are kept in a secure, confidential file and are shared with as few people as possible on a "need-to-know" basis. If, however, a child is considered at risk, our safeguarding policy will override confidentiality.
- Gaining parental permission for any photographs of the children to be used within the nursery.
- Ensuring that staff, student and volunteer inductions include an awareness of the importance of confidentiality.
- Ensuring that staff, students and volunteers are aware of, and follow, the nursery's social networking policy in relation to confidentiality.

- Ensuring that any concerns/evidence relating to a child's personal safety are kept in a secure, confidential file. This information must be shared with as few people as possible on a need-to-know basis. If however, a child is considered at risk, the nursery's safeguarding children policy will override confidentiality.

All the undertakings above are subject to the paramount commitment of the nursery, which is to the safety and well-being of the child.

Staff Agreement

- All areas of confidentiality must be adhered to at all times. At no time whilst in employment and after termination of employment with ToyBox are you to divulge any of our clients' details, working practices, policies or financial dealings to any other party.
- When taking on any private baby-sitting arrangements you must remain professional and ensure that confidentiality of the nursery is considered at all times.
- No information regarding other children or problems within the organisation is to be discussed with parents when baby-sitting is privately arranged.
- When feedback is given at the end of each child's session you must ensure that it is done in a professional way, giving the parent all the information that they need to know about their child's day.
- You must ensure you are aware of and follow our social networking policy which can be found in our staff handbook in relation to confidentiality.

If staff, students or volunteers in the nursery are to breach any of the confidentiality provisions, including the above agreement, it is considered gross misconduct. Any staff found to have committed gross misconduct will result in a disciplinary action, and in serious cases, immediate dismissal without notice.

Policy and Procedure reviewed by Gemma Turner June 2023
Date of next review:

Appendix 1

Staff are to follow the 7 Golden Rules to information sharing set out be the

1. GDPR Isn't a Barrier to Sharing Information
   With GDPR coming into effect in 2018, it's assumed that this statutory requirement doesn't allow you to share information. This isn't the case. The Data Protection Act isn't a barrier to sharing information, but it provides a framework which ensures that personal information about living individuals is shared appropriately.

2. Be Open and Honest
   You need to be open and honest with the child, young person and/or their family where appropriate about why, what, how and with who you will or could share information with. You also need to seek their agreement unless it's inappropriate or unsafe to do so.

3. Seek Advice
   If you're ever in any doubt about sharing or disclosing the information concerned, seek advice from other practitioners such as your school or college's Designated Safeguarding Lead (DSL). You should try to do this without disclosing the identity of the individual where possible.

4. Share With Consent Where Appropriate
   Where possible, respect the wishes of those who don't give consent for you to share their confidential information. However, depending on the nature of the situation and what a child or young person has disclosed, you may still share information without consent.

5. Consider Safety and Well-being
   Base your information sharing decisions on considerations of the safety and well-being of the child or young person - as well as anyone else who may be affected by their actions.

   his is if there's a good reason to do so in your judgement, such as where safety can be at risk.

   Base your information sharing decisions on considerations of the safety and wellbeing of the child or young person - as well as anyone else who may be affected by their actions.

6. Necessary, Proportionate, Relevant, Accurate, Timely and Secure
   Ensure the information you share is necessary for the purpose for which you share it. You should share it only with those people who need to have it, your information is accurate, up-to-date, shared in a timely fashion and also shared securely.

7. Keep a Record
   Regardless of the decision you make, keep a record of it and the reasons why you made that decision. If you decide to share following a disclosure, then record what you've shared, with who and for what purpose.

Even with the government's seven golden rules for sharing information, it can be challenging in a real-life situation when you need to make the tough decision on whether or not you should share information.

To help make that process easier, here's a flowchart of key questions for information sharing to help you make the right call if you're ever in that situation.

Appendix 2

BWC GDPR Practical Matters

- Whilst you should always apply a common-sense approach to how you use and safeguard personal data, and treat personal data with care and respect, set out below are some examples of dos and don'ts:
- Do not take personal data out of the organisation's premises (unless absolutely necessary).
- Only disclose your unique logins and passwords for any of our IT systems to authorised personnel (e.g. IT) and not to anyone else. Please refer to the Acceptable Use Policy for more information on password management.
- Never leave any items containing personal data unattended in a public place, e.g. on a train, in a café, etc. and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.
- Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.
- All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet. This includes mass storage devices such as USB drives.
- All drawers and cabinets containing personal data should be kept locked at all times when access is not required, and the keys not left in the locks.
- Computers must be locked when the desk is unoccupied and completely shut down at the end of the work day.
- Laptops, tablets, and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet.
- Do password protect laptops, mobile devices and removable storage devices containing personal data.
- Do password protect documents and databases containing personal data.
- Never use removable storage media to store personal data unless the personal data on the media is encrypted.
- When picking up printing from any shared printer always check to make sure you only have the printed matter that you expect, and no one else's
- Use confidential waste disposal for any papers containing personal data. Do not place these into the ordinary waste.
    - Please shred confidential waste using the shredder in the front office.

- Once a year staff will be required to go through annual data deletion and destroy all digital and paper files that we should no longer keep, according to the data retention policy.
    - In this instance staff should put all confidential data to be deleted in the red sacks provided by the office admin.
    - The red sacks will be locked up each night in the Archive room by the office admin.
    - At the end of the time allotted for data deletion (normally a week) the Office Admin who will call paper round to collect the sack and securely dispose of the paper.
- Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.
- When in a public place, e.g. a train or café, be careful as to who might be able to see the information on the screen of any device you are using when you have personal information on display. If necessary move location or change to a different task.
- Do not use public Wi-Fi when accessing company systems
- Do ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working in the office. Personal data should only be accessed and seen by those who need to see it.
- When speaking on the phone in a public place, take care not to be overheard when exchanging personal or confidential data.
- Do not hold confidential calls in range of a Virtual Personal Assistant (e.g. Alexa; Echo)
- Never act on instructions from someone unless you are absolutely sure of their identity and if you are unsure then take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.
- Do not transfer personal data to any third party without prior written consent of your supervisor/manager.
- Do notify your supervisor/manager immediately of any suspected security breaches or loss of personal data.
- If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately.
- If sending an email to multiple external recipients, use “blind copy – bcc” not “carbon copy -cc”.
- With the exception of the police, under no circumstances whatsoever allow any unauthorised person to view cctv images.
- Observe a “clean desk” policy at all times. Only have personal data on your desk or in your work area while you need it, and return it to its secure location when you’ve finished with it.