Confidentiality and Information Sharing Guidelines

Confidentiality refers to guidelines within bowls about when information can be shared, with whom and rules around when it is not appropriate to share information.

Every effort should be made to ensure that confidentiality is maintained for all concerned. However, there are circumstances when it is important that information is shared including to report or prevent harm to a child or an adult at risk. The BDA Safeguarding policies for children and adults at risk contain details of the confidentiality and disclosure requirements to support safeguarding of both groups.

Information should be handled and disseminated on a need-to-know basis only.

This includes the following people:

- Club and/or County Safeguarding Officer
- NGB Safeguarding Officer
- Parents/carers of the person who is alleged to have been abused (if the concerns relate to the parent or carer, seek advice from the NGB Safeguarding Officer, who will liaise with Children's Social Care services, about sharing information)
- Person making the allegation
- Children's Social Care / Adult Social Care / Police

Information should be stored in a secure place with access limited to designated people, in line with data protection laws (e.g. that information is accurate, regularly updated, relevant and secure). Referrals through to the NGB Safeguarding Officer and/or the BDA Lead Safeguarding Officer will be stored using 'My Concern'.

Data Storage

When you're storing data, you must comply with the Data Protection Act 2018. The Act requires that you keep your clients' personal data secure, 'with appropriate technical organisational measures taken to protect the information'. In practice, this means you should encrypt personal data and protect it with a password, as well as taking physical precautions to keep it safe - lock away computers at night and secure servers and external hard drives with anti-theft cables. In summary:

- The Act requires that you take steps to keep personal data secure
- Encrypt sensitive data with a password
- Take physical precautious to keep data safe

The Seven Golden Rules of Information Sharing – source:

Information sharing: advice for practitioners (publishing.service.gov.uk)

1. The General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing but provide a framework to ensure that personal information about living individuals is shared appropriately.

2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and upto-date, is shared in a timely fashion, and is shared securely (see principles).

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.