**PRACTICE TIPS – DATA PROTECTION WHEN WORKING WITH CHILDREN, FAMILIES AND OTHER PROFESSIONALS – March 2019**

These tips have been compiled to assist practitioners in ensuring compliance under the General Data Protection Regulations – GDPR, when working with children, Young People and their Families, and other Agencies.

A key component of the work that we do is based around information, how we gather it, what we do with it, how and who it is shared with, and how it is stored. Each of these stages must be compliant with the GDPR and Data Protection Principles

* **Gathering Information**

Information should only be gathered if there is a need to do so. It must be reasonable, proportionate and relevant. You must be able to justify why the information was being sought. This is about recognising information is private and therefore needs to be dealt with respectfully.

Information should only be gathered with consent from the individual unless there is a safeguarding matter which could place a child at risk of harm. If an inadequate referral is made which requires further enquiries this is the responsibility of the referrer, we do not have the authority to undertake enquiries unless there is a need to do so to safeguard a child.

If a referral or event occurs which is borderline safeguarding and the parent refuses consent for seeking more information, then a Strategy Discussion can be used to determine if the threshold is met for overriding such consent.

Families have the right to know what you will do with their information, there is a need for honesty and transparency. They need to know who it will be shared with, for what purpose and whether there are any potential implications for the family from doing this. – In cases where there is violence, or risk of harm a safety plan should be discussed with the victim about information sharing.

* **Sharing information**

South Glos Privacy Statement - http://intranet/content/CEandCR/Sections/IG/doc/PrivacyStatement.pdf

Clarity and transparency around how the information is going to be used is a key principle within the Data Protection requirements.

When working with a child/ Young Person we need to be clear about who will hear their voice, their worries and dreams. They need to be consulted with in terms of who will know, what they will be shown and when. There is a need to recognise that sharing ‘voices and worries’ may cause fear and anxiety in the child and reassurance, respect and sensitivity is required. A parent has the right to know what is said to their child, however a judgment must be made as to what if any the level of risk to the child will be , should that information be shared at that particular time. Providing the child with space to talk is one of the most helpful things we can do, how we then use that information needs to be thought about carefully in order to preserve all working relationships and primarily safety. Supporting parents to give their child permission to talk and space to reflect upon is a powerful message, as it generates trust and hope for the child when previously they may have felt it was missing.

A Young Person age 14 plus may not want certain information shared with the parent, this requires careful planning and honesty as to how this will or will not happen. An awareness of the Fraser/ Gillick competences are required at this stage.

https://www.proceduresonline.com/southglos/cs/user\_controlled\_lcms\_area/uploaded\_files/gillick-competency-factsheet.pdf

Discussions with family members about how information will be used is essential if they are to feel respected and engaged in a process. Practitioners must consider what the possible consequences may be of sharing such information and ensuring a contingency plan is in place should it be needed.

This is particularly important in situations where there is violence or risk of harm

Information obtained from other agencies needs to be shared under the parameters of is it necessary, proportionate and relevant. The same rules apply in terms of clarifying what and how this information is going to be used. This is particularly important when intelligence is shared from the police. This information cannot be referred to or used in reports unless a strategy discussion has clarified how it will be used, and even then it must be treated with particular care and consideration of such things as the degree of detail that is required to be included and ensuring it is not copied across inappropriately into other documents and records. Sometimes an agreement can be made on the specific wording of a statement which does not compromise any investigation or the ability to safeguard someone.

**Conversations**

We all have conversations with different people at different times, some of these are planned and some are not. Within these conversations we need to be mindful of who we are talking to and what we are talking about.

We do not have conversations with families about other people unless this has been agreed upon via strategy discussion. We can encourage Families to make use of the legislation in order to inform their decision making ie Sarah’s Law, & Claire’s Law . Families have the right to contact the police and request assistance under these laws in respect of individuals with records for Sexual Offending and Domestic Violence

**The key principles** for Data Protection Compliance are –

* Information is Proportionate, relevant and necessary
* Information is securely stored
* Consent is obtained to use and share information
* Sharing of information needs to be proportionate and necessary
* Inform people what will be done with the information/ data
* IT safety and security must be in place at all times.

**Report Writing**

Reports need to be factually accurate with opinions highlighted as opinions

3rd party information, ie information about someone else, needs to be redacted or used in a manner where consent has been obtained.

Copying over data from previous reports is possible however they must be scrutinised for 3rd party information. There is a risk when pulling through previous referrals to assessments that they may contain police intelligence, or other confidential information– this must be removed from the assessment.

Confidential information can be placed on a child’s record to inform decision making and risk analysis, however it cannot be shared unless permission has been obtained to do so.

All reports should be QA’d by a manager prior to being shared and or circulated.,

**Paper notes**

Paper notes once electronically recorded need to be shredded unless they are specific records of a disclosure or an allegation.

A disclosure or allegation made and recorded on paper needs to be kept and scanned onto Mosaic as a scanned document. – this may later be required as primary evidence within an investigation. A typed case note will need to be created to confirm the information/data and the fact that the original is stored at a specific locality.

Paper notes must not be left in a car or the homes of families that are visited, they need to be securely locked up where access is restricted. If notes are left in a public place it is the responsibility of the practitioner to notify the TM as a matter of urgency.

Security of information is a fundamental principle in Data Protection.

**Electronic records**

Information is often shared via email. Sensitive information should only be sent via secure email.

http://intranet/content/CEandCR/Sections/ICT/new/service/security.htm

You must not use your personal email accounts, only your council one.

Cutting and pasting emails into case notes needs to be done carefully to ensure that only relevant information is secured on the child’s records.

Email Guidance link - <http://intranet/content/CEandCR/Sections/IG/doc/EmailGuidance.pdf>

Corporate Records Guidance - http://intranet/content/CEandCR/Sections/IG/doc/CorporateRecordsManagementPolicy.pdf

**Legislation**

Whilst it may initially appear that we can’t do anything for fear of breaching legislation, it is important to remember that the Children’s Act supersedes all other pieces of legislation in terms of safeguarding children. The protection of children is the paramount principle behind information sharing, therefore ask yourself do I need to know or find this out in order to keep a child safe? If the answer is yes, discuss this with the manager and ensure the rationale behind the actions of seeking and using information without either the wishes or knowledge of the family is recorded on a Case Direction. – An example of when this might be necessary is when there is a risk of FGM/ HBV or flight

Data Protection Guide for Staff - http://intranet/content/CEandCR/Sections/DataProtectionFoI/Docs/DPstaffleaflet.pdf

**Consequences of Data Breaches**

Data breaches are serious and as such the penalties and consequences can also be so. The Information Commissioner may investigate and issue a Local Authority a significant fine, and in some cases may pursue a criminal case against the individual.

HCPC may review SW or other health professional’s registration status. - http://www.hpc-uk.org/standards/standards-of-proficiency/operating-department-practitioners/

Local Authorities may pursue the disciplinary processes with employees.

Families may be exposed to more risk, disappear or abscond.

Children may become more vulnerable and possibly unseen

Data Protection is more than keeping information safe, it is about how do we use it appropriately, proportionately and reasonably to keep children safe.

March 2019