Looking After Data

Data Governance Info Session Notes

March 2017

Record Keeping – Bear in mind that the person may put in an access request to your records and will be able to read all your comments. **Keep records, honest, accurate and professional**.

Handwritten notes must be **legible** and there should be **no anacronyms or confusing abbreviations**. If they would have to be explained to a layperson they are not good records.

Keep **separate records** for individuals in family groups – where possible.

Records Audit – make regular audits of what information you have, where it is kept and who is responsible for it. This includes online records. Information should be removed from emails and stored elsewhere.

Sharing data

- Internal emails will be secure**. Do not use personal emails or home computers.**
- **Social Media –** ignorance of platforms i.e who can view posts is not a defence in law.
- **Faxing –** the riskiest method of transfering data – best not to use.
- **Secure posting** is currently deemed more secure than email, by law.
- **Consent –** when someone asks for their data to be shared with them document it and make sure they give you the email address and that you have it down correctly

Explicit Consent – soon legislation will say that explicit, rather than implied, consent will be needed legally. People should sign to say that they understand their data may be shared with specific groups/individuals, under what circumstances and how it will be shared. Leaflets can be useful to make sure people have more information they can absorb at home.

If consent is given verbally document this. Conversations must explicit and they must state that they understand. It is best to get a signature.

You are Individually Responsible for all information that you sent out by email, post, phone conversations etc.

Also for any information that you may inadvertently see – even if it does not fall within the usual scope of your work.

Organisations must have clear Consent Policies & Procedures of which all staff are aware. Individuals consent form must be stored somewhere and consent should be checked with the individual on a regular basis - 6-12 months depending on the service and if information is being used in a new way (onward referrals etc.). The review must be documented and signed by the individual.

If things go Wrong. If information gets into the wrong hands apologise, initiate investigations, be open with the service user about how it happened and how you will ensure it will not happen again**.** Make sure you have a proper **reporting system** in place. **Apologies go a long way.**

Clear Desk/ Clear Screen Policy – never leave any personal or sensitive information lying on your desk, unattended in the printer tray or up on your screen where others may chance upon it.

Passwords/Access protocols – you are responsible for anything entered on your system or anything sent in an email, or other communication, with your name on it – regardless of who enters or sends this information. Make sure you have **secure passwords**, don't share them, change them regularly.

Do not have them written down where others can see or find them.

Think: "Would I be happy for my confidential information to be handled this way?"