Information Governance – Key Points

This document provides a useful summary of the key points made in our IG policy. However, it is important that you also read, understand and comply with the policy in full.

Caldicott Principles

These are questions you should ask yourself before processing or disclosing personal information. You should:

1. Justify the purpose(s) of using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need-to-know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law (Data Protection Act 1998)

The 8 Data Protection Principles

Personal data must be:

1. **Processed fairly and lawfully**
   Inform data subjects (mums and families) why you are collecting their information, what you are going to do with it, who you may share it with.

2. **Processed for specified purposes**
   Only use personal information for the purpose(s) for which it was obtained.
   Only share information outside your local team if you are certain it is appropriate and necessary to do so. Share information only when there is permission and it is appropriate.

3. **Adequate, relevant and not excessive**
   Only collect and keep the information you require. Only hold information when you have clear plans for its use. Do not collect information "just in case it might be useful one day!" Destroy extra information if not needed. Explain all abbreviations. Use clear legible writing. Stick to the facts, avoid personal opinions and comments

4. **Accurate and kept up-to-date**
   Have mechanisms to ensure information is accurate and up-to-date. Check you are contacting the right person about the right thing. Avoid creating duplicate records by checking existing records thoroughly before creating new records

5. **Not kept for longer than necessary**
   Follow the BfN Records Retention schedule. Ensure regular spring cleaning of your information. Do not keep "just in case it might be useful one day!". Dispose of your information correctly and securely.

6. **Processed in accordance with the rights of data subjects**
   Information given is still controlled by subjects (mums and families). Information must not be passed to a third party without consent. Information can be rectified/blocked/erased. Mums and families should have access to any information we may hold

7. **Protected by appropriate security (practical and organisational)**
   ALWAYS keep confidential papers locked away. Have a clear desk policy. Ensure confidential conversations cannot be overheard. Do not work with personal information in a public place (e.g. library, Internet café). Have different and strong passwords for different systems or websites. Keep your password secret. Ensure information is transported or transferred securely.

8. **Not transferred outside the EEA without adequate protection**
   Always check with the IG lead before sending any information outside the EEA. Check where your information is going e.g. where are your suppliers based? The EEA comprises: EU member states plus Iceland, Liechtenstein and Norway.

Top five tips [1]

1. **Tell people what you are doing with their data**
   People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.

2. **Make sure your staff and volunteers are adequately trained**
   New employees and volunteers must receive IG training (as outlined on page 13 of the IG policy) to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff and volunteers.

3. **Use strong passwords**
   There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves. Also, if a box pops up asking if you would like to save the password, click No.

4. **Encrypt all portable devices**
   Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted. BfN equipment should be used wherever possible, other devices should be approved prior to use via your Line Manager. Information on encryption methods is available from the staff IG lead.

5. **Only keep people's information for as long as necessary**
   Make sure everyone knows about our Records Retention schedule and set up a process for deleting or destroying personal information once it is no longer required.

Think Privacy! [1]

It's our responsibility
We need personal information about volunteers, mums and families, supporters and employees to run our organisation successfully. We are trusted to look after this essential information. Each and every volunteer and employee has a responsibility to comply with the appropriate Data Privacy laws. Think Privacy.

It's our reputation
Reputations are hard won and easily lost. Handling our volunteer, supporter, mums and families and employee data with care and respect is critical to protect our reputation. YOU are our best defence against reputational damage. Think Privacy.

It's about respect
The choices our volunteers, supporters, mums and families and employees make about how their personal information is used must be respected if we are to maintain the trust they place in us. Think Privacy.

It's in your hands
We are all responsible for ensuring that personal information about volunteers, supporters, mums and families and employees is kept secure and confidential. Extra care must be taken with any information that needs to be sent or taken off-site. Think Privacy.

Always
You must **always** keep personal information secure, this means:
- locking your desk drawers or filing cabinets
- keeping your desk clear of personal data
- locking your computer screen
- disposing of personal data securely (shredding)
- avoiding collecting or storing any personal information unless you can justify the reason it is being collected or stored.

A useful question to ask yourself is **"How would I feel if someone were doing this with MY personal information?"**

Please remember that we are here to support everyone - no question is too big or too small - if you are not sure if what you are doing is right then please ask by contacting your Manager, Supervisor or the staff IG lead clare.farquhar@breastfeedingnetwork.org.uk.

References 1 The Information Commissioners Office https://ico.org.uk/for-organisations/charity/