Walton Parish Nursing

Confidentiality Policy

Walton Parish Nursing is an organisation based on trust where confidentiality is the norm, because preserving the privacy and confidentiality of clients, staff and volunteers is essential in respecting autonomy. The professional management of confidentiality, which is about preventing the unauthorised disclosure of identifiable sensitive information, is core to the way we operate.

All staff and volunteers are expected to follow the procedures set out in the *Modus Operandi* produced by the Management Team, including the appendix on electronic data. Guidance from Parish Nursing Ministries UK should also be taken into account.

Annex 1: Modus Operandi

1. Obtaining the consent of the client is paramount when resolving any dilemmas over confidentiality. Disclosure may also be authorised by their legal proxy or the law. Communications made on the basis of client consent do not constitute a breach of confidentiality, however any disclosures of client confidences should be undertaken in ways that best protect the client's trust and respect client autonomy.

2. Exceptional circumstances may prevent anyone dealing with clients from seeking client consent to a breach of confidence due to urgency or the seriousness of the situation; for example, preventing the client causing serious self-harm or harm to others. In such circumstances we have an ethical responsibility to act in ways which balance the client's right to confidentiality against the need to communicate with others. People working under the auspices of Walton Parish Nursing should expect to be ethically accountable for any breach of confidentiality and willing to be accountable to their clients and to their profession for their management of confidentiality in general and particularly for any disclosures made without their client's consent. We would regard this situation as a "legitimate interest" within the General Data Protection Regulations (GDPR).

3. Volunteers receive regular supervision from our Parish Nursing professionals. The Parish Nursing professionals receive regular supervision from a professional mentor and Line Manager while each church involved in Walton Parish Nursing has a representative minister on the trustees. In an extreme case any necessary breach of confidentiality should be kept within this framework and where possible with the client's consent.

4. All client information is confidential and should not be discussed with other members of the congregations or anyone else. Some clients may ask for prayer, or prayers for them might be offered. It is vital that their consent is obtained and that it is clear what information may be shared, what is to be prayed for, when it may be shared and where it may be shared. Prayer requests should be anonymous unless the consent of the person/family being prayed for has been gained.

5. Regarding dual roles and multiple contexts where Walton Parish Nursing staff and volunteers meet clients in another context (e.g. at work, in church, as friends) it is important as far as possible to keep roles separate. Something shared in a Parish Nurse setting, should not be relayed outside that setting even if the people move in the same social or friendship

circle.

6. The same principles should apply to any testimonies that clients agree to share. Photographs of clients may only be used with their consent.

7. Enquiries from other agencies and authorities, e.g. by telephone, must be referred to a member of staff in the Walton Parish Nursing team.

8. Clients' paper files and all relevant information are to be stored in a locked cabinet with only the Parish Nursing professionals having access. Notes are to be kept for seven years after the final entry and then destroyed. Clients may request removal of their records/data at any time.
   For electronically stored data see Appendix A.

9. This policy applies both during and after a person's involvement with Walton Parish Nursing.

Annex 2: Electronic Data

With the increase in communication using a variety of newer technologies, it is important to maintain the same principles set out above. It is important to be careful to keep stored data where it remains confidential. All actions will be taken within GDPR.

Data storage on Computers.

When a computer is passed on, sensitive and confidential data from the hard drive should be permanently deleted. Security software can be purchased to do this. Alternatively hard drives should be removed from equipment being disposed of and mechanically destroyed.

Where data is stored in such a way that there is shared access, proper use of passwords should be made to limit access to appropriate persons. This is true of those whose computers are based at home and used by family members, as well as those who work in an office.

Cloud Storage

Due to the inherent vulnerabilities of cloud storage any confidential data should not be stored in this manner.

CDs, DVDROMs, Memory Sticks etc.

When data is stored on portable media, including: CD and DVD ROMs, USB drives, mobile phones and laptops, care needs to be taken to password protect files and machines.

Email:

In families and in offices, it is not unusual for people to have shared mailboxes, allowing general access. Where possible, in-boxes should be password protected.

(Any email that contains personal data about a third party should only be sent with their permission and should be treated with the same care and attention as any other written information being passed on.). When sending an email to multiple recipients, who have not agreed to their email address being shared, these should be sent using the blind copy facility to hide the individual's email addresses.

Protecting contents of emails.

When sending documents that contain sensitive information, they should be secured against accidental or deliberate alteration by converting them into a more secure format such as PDF and XPS.

Mobile Phone Technology.

The same care should be taken in passing on texts (or any social media equivalent) as when using any other method of passing on information. It is important not to discuss personal details of individuals whilst using a mobile phone in a public place.

Documents, images, sound recordings and videos can easily be made and passed on using various kinds of mobile technology. If sending data by Bluetooth or Near-Field-Communication it is important to remember that unintended people may have their connectivity set to 'on' and therefore be able to receive information. It therefore makes sense that when sending confidential or potentially sensitive data it is important to target a particular device (phone or laptop), rather than use a general broadcast, which may be picked up by other devices within range.