

COMMUNICATIONS POLICY AND PROCEDURE

Introduction

Parish Nurses are registered nurses who are employed or appointed by the local church to lead whole person health ministry. Parish Nursing Ministries UK is a charity that provides training, coordination and resources to help and support this practice.

Parish nurses are accountable to the Nursing and Midwifery Council and as such have to follow the NMC Code of practice. This has strict guidance on confidentiality and communications to which the Parish nurse must adhere.

Policy Aim: To ensure professional and safe means of communication, noting that **the passing on of personal information always requires consent unless the information is required by law, or if harm is anticipated to the individual or to others.**

General communication

E-mail

- Computer access and e-mail accounts should be password protected. If computers are shared then each user should have a separate account and additional password.
- Passwords are the front line of protection and should not be simple words or combinations of numbers. Ideally use combinations of Capital and lowercase letters, numbers and symbols, e.g. M@r1time.
- Change passwords regularly and do not use the same one for different applications.
- E-mails are widely used to transport malware (e.g. viruses and spyware) which can corrupt data, cause machine malfunction and disclose personal details to third parties (identity theft). No anti-virus software is 100% effective. Never open attachments or click on links in e-mails from unrecognised senders. Delete the e-mail.
- Use separate e-mail addresses for business and personal use
- Downloading media from file sharing sites or portable storage drives increases the risk of computer infection

Great care is needed in the preparation and distribution of e-mail to preserve confidentiality, ensure data protection, protect copyright, maintain the reputation of the organisation and minimise inter personal conflict through misinterpretation.

- Limit e-mail transmissions to professional use and use appropriate language. Employ short, simple and objective phrases to ensure the content is unambiguous.
- Select recipients carefully on a “need to know basis”. Avoid carbon copies (ccs and bcc’s) unless absolutely necessary.
- Do not send anyone else’s email or their response to a new person unless you have the original sender’s permission.
- Restrict responses to the original sender unless otherwise instructed.

- When sending bulk mailings, list recipients for blind carbon copy (bcc) to protect individual confidentiality.
- Do not send identifiable personal or confidential information relating to yourself or other people by e-mail
- Do not send sensitive information or copyright documents outside the organisation.
- Review all emails before sending. Ensure the trail does not include other people's responses or email addresses unless you have their permission.

Social Networking

Social networking is a very powerful and popular means of communication but risks are associated with its use. For Parish nurses, referral should be made to the NMC guidance on this.

- Social networks usually presume ownership of information posted, offer little or no protection for it and can distribute without consent.
- Details about other people should not be posted without their consent and details of minors should never be posted.
- Work related information should not be posted to avoid compromising client confidentiality, data protection and copyright.
- Social networks facilitate "spamming", harassment and business piracy.

Mobile Phones

- Try to avoid using mobile phones for work related conversations in crowded public places. If this is unavoidable keep messages short or preferably use text
- Do not leave phones and particularly laptop computers in parked cars. Most insurance companies will not cover any loss from theft and the loss of data could adversely affect the organisation.

Information relating to clients:

In circumstances where it is absolutely necessary to transmit confidential or restricted information via email the sender must ensure the following checks are carried out before sending the information:

- The name and email address of all the intended recipient(s) are correct
- The subject line of the email should not contain the person's name
Only the minimum amount of confidential or personal information as is necessary is to be sent be addressed to individuals who have a right and a legitimate need to see the information.
- Only send confidential or personal information with individual/parent consent.
- Where practical check that the email message and information have been received by the intended recipient(s) (e.g. ask for a delivery receipt or phone the intended recipients to confirm receipt).
Email communication and telephone calls about a client should be documented.
- If you wish to use a password to protect information, it must not be sent along with the original email message.
- Stories or case studies for publicity purposes will not identify the geographical location of the client or church, and will only use an alternative first name for both Parish nurse/church worker and client. A statement indicating this change is to be added. Photographs of clients will only be used where there is written permission or where the nurse/church worker or photographer has confirmed that permission for public use has been obtained. Clients will not be named in these photographs unless they so wish.

Ownership of records: Parish nursing records are kept confidentially by the nurse, who is responsible for their safe storage. Permission must be obtained from the client if it is necessary to share information, the only exception being if it is judged that harm is likely to the client or others.

The records may only be accessed by church staff in the case of a request from a court of law.

Definitions of personal data and sensitive personal data used within the Data Protection Act 1998

Personal data

Personal data is information which relates to a living individual who can be identified:

- from that data
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and
- includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data

Sensitive personal data is personal data which consists of data related to the data subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, the commission of offences or criminal proceedings.

The data protection principles

Personal data must be:

- processed fairly and lawfully
- only obtained for specified and lawful purposes and not processed in a manner incompatible with those purposes
- adequate, relevant and not excessive in relation to the purposes for which it is held
- accurate and, where necessary, kept up to date
- kept for only as long as is necessary under NMC guidelines
- processed in accordance with the rights of data subjects under the act, including the data subjects' right of access and right to object to the processing of their data in certain circumstances
- protected from unauthorised and unlawful processing; accidental loss, destruction or damage by having appropriate technical and organisational measures in place

Methods of distribution.

Copies should be made available to all those working in any capacity on behalf of the charity

Review dates: May 2018, April 2019