

12. Guidelines for Good Practice in Confidentiality and Pastoral Care

Within these Guidelines the expression 'Pastoral Worker' refers to lay, ordained, paid and voluntary persons who exercise a pastoral role within or on behalf of the Methodist Church.

12.1. In order to establish a relationship of trust within a pastoral relationship and within the wider church community, it is important that the things people share are treated in confidence. There are three exceptions to this.

- If someone specifically gives the pastoral worker permission to pass on something they have said (eg, they give permission for a situation they are facing to be mentioned in the intercessions at church).
- If a person discloses information that leads a pastoral worker to think that that person or another person is at risk.
- If a person indicates that he has been involved in or is likely to become involved in the commission of a serious criminal offence.

12.2. In the second and third cases information should be passed on to the appropriate person or agency. Wherever possible the person disclosing information should be supported in sharing that information himself or herself. If that is not possible they should be encouraged to give permission for the information to be passed on.⁴⁴ Only if this is not possible should the pastoral worker disclose the information to the appropriate third party without permission. A child would not necessarily be expected to disclose information themselves, but they should be carefully consulted.

Guidance on the safeguarding of Children, Young People and vulnerable adults can be found on the Methodist Church website.⁴⁵

12.3. When a person indicates that what he or she is saying is to be kept confidential, it should be understood that it will remain so, subject to the circumstances outlined above. There is a further responsibility on behalf of the person offering care in the pastoral context to assume confidentiality even without this being explicitly raised. Seeking the permission of the person disclosing information as to whom it might be shared with and in what circumstances is an important part of building up trust and demonstrating that they and their story are valued. A trust that is born of a community in which confidentiality is normally maintained will lead to confidence that those who offer care are able to exercise proper judgement on those rare occasions when confidentiality needs to be broken.

12.4. Supervision

All those in a recognised pastoral relationship should be supported through a structure of formal reflective practice (called 'supervision'). Each church or Circuit should have a supervision system in place for their pastoral workers, providing someone they can talk to, seek advice from and share with, in confidence, issues and concerns about a visit or a series of visits. This may be an experienced pastoral visitor, pastoral secretary, a lay pastoral worker, a presbyter, deacon or a professional

44. Care must be exercised to not prejudice or risk prejudicing any possible police investigation. See, for example, SO 022A(7B) for guidance.

45. www.methodist.org.uk

With Integrity and Skill

supervisor. Details about possible models of supervision can be found on the Methodist Church website.⁴⁶

12.5. Self-Awareness

If the pastoral worker has an urge to pass on information, what is their motivation? Has the information shocked, alarmed or offended them? Has the information caused painful memories to surface from their own history? Is there a sense of power connected to knowing this information when others do not? On the other hand, would it help the person or people in the midst of a pastoral situation to pass the information on? If so, the person disclosing should be encouraged to share their own story, or give permission for it to be told. Three simple headings can help those in a pastoral relationship to develop their self-awareness in regard to confidentiality.

12.6. **When to tell**

When permission has been given by the 'owner of the story'.

When an individual/individuals will be at risk of harm if the information is not passed on.

When information has been disclosed about a serious criminal offence that has taken place or is planned.

In the context of supervision, with the prior knowledge of the individual that this may take place.

12.7. **What to tell**

What are the facts of the story? These need to be told without gloss or 'spin'. Only sufficient information should be passed on to enable the giving of support, practical help or informed prayer. Avoid sharing more than is needed.

In a supervision context it would be usual practice not to give details of names, but an outline of the situation and the pastoral worker's response.

12.8. **Who to tell**

Identify the most appropriate person (if any) to pass the information on to. Who can help or has the resources or access to support for the person concerned? Who will most appropriately support the pastoral worker in reflecting on what they have heard?

Identify any persons or groups who should not be told. It should not be assumed that the person concerned has told their family or friends.

It is not good practice for pastoral workers to share pastoral information about third parties with members of their family. People would not expect a GP to pass on to her spouse confidential medical information, yet often assumptions are made that to tell a pastoral worker information will lead automatically to their partner knowing. Boundaries of confidentiality need to be made clear to all concerned, and the family members of the person offering care should not be expected to carry the responsibility of holding such information.

46. Ibid.

12.9. Prayer Support

People's names and situations should only be mentioned in public worship and contexts of open prayer if they have given express permission. This applies to prayers written in books, hung on prayer trees and passed on to prayer chains and networks.

Care should be taken when a worship leader or preacher invites topics for intercessory prayer that people understand that they should only share information about people that is given with their permission.

12.10. Church Meetings

The limits of confidentiality within any church meeting need to be identified and kept to – not by implicit assumption but by explicit and agreed policy. Applying the general principles that information is only passed on when permission is given and that the person involved knows the context in which it will be shared will enable meetings to remain in good order.

Groups discussing the status of an individual need to be reminded of the confidential nature of their business.

Disciplinary proceedings of the Church operate under strict rules of confidentiality, which are fully explained in 'Complaints and Discipline in the Methodist Church: A Step by Step Guide to the Standing orders on Complaints and Discipline'.⁴⁷

12.11. Dual Roles

The boundaries of a pastoral relationship can be blurred. A pastoral visitor may also be a former nurse and a volunteer visitor at the local hospital. This may give her access to church members as patients, in which case it is important that she and the church member are both clear about which 'hat' she is wearing. It may be that pastoral support would need to be offered by a different member of the church or Circuit.

Sometimes the person offering care has dual responsibilities on behalf of the Church (eg, a Chair of District who is responsible for pastoral care of ministers as well as their discipline and their stationing). In such situations the status of the conversation should be made as clear as possible from the outset. The speaker should be asked to state what his or her expectations are. The listener should make it clear whether he or she is willing to be bound to complete confidentiality in advance and explain in what circumstance they would feel an obligation to share or use the information given.

47. Clifford Bellamy, *Complaints and Discipline in the Methodist Church: A Step by Step Guide to the Standing Orders on Complaints and Discipline*, Third Edition, MPH, to be published September 2008.

With Integrity and Skill

If during the course of a pastoral conversation a listener realises that there is material that might need to be used in a context beyond pastoral support, the speaker should be told.

12.12. Multiple Contexts

A pastoral worker may have privileged knowledge of an individual from another context (eg, barrister, GP, counsellor). Best practice is that information disclosed by an individual remains within the geographical or professional context in which it was disclosed.

If a person has given permission for their situation to be prayed about by a prayer group and a member of that group has contact with them in another pastoral setting, it is not appropriate for that information to be shared in that other setting without permission being sought.

12.13. Multiple Needs

Where there are multiple parties within the church or within a family with a range of needs, different sources of pastoral support for those parties will need to be offered. This is particularly the case in a situation of abuse, where victim and perpetrator should not have the same pastoral supporter. It may also be that a church's pastoral system has visitors that care for particular groups within the life of the church, such as young people.

Confidentiality and Technology

12.14. Data storage

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.

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.

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

If using a Wireless Local Area Network (WLAN) to store, send or receive confidential information, it is important to ensure that a high level of security encryption is enabled.

12.15. Social Networks and Websites

Sites such as Facebook and MySpace are increasingly popular and are used by many people as a source of support and friendship. People are often quite relaxed about the amount of information they disclose about themselves and possibly about others. It is important to apply the principle about 'who owns the story' in what is shared about others online.

12.16. Remote printing and faxing

If using fax machines or printers that are networked from a computer into another room, in a busy office for instance, it should be ensured that sensitive information is not left unattended.

12.17. Photocopiers

Originals of sensitive material should not be accidentally left on the photocopier; the next person to use the machine may not understand the confidential nature of what has been left for all to see. Some copiers retain a scan of a document until the next document has been copied. If a print run is interrupted (due to lack of ink or paper) it may be that the next person to use the machine finds that the outstanding copies print out when they have stocked up the paper or ink.

12.18. 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. It is important to take care not accidentally to 'reply to all' if the contents of your reply to an email should not appropriately be seen by the wider group. When emailing a group, if the members have not given permission for their details to be circulated within the group they should be mailed using the 'blind carbon copy' (ie bcc) facility.

12.19. Protecting contents

When sending documents, secure the contents against accidental or deliberate alteration by converting documents into a secure format such as PDF.

12.20. Mobile Technology

The same care should be taken in passing on texts 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 it is important to remember that unintended people may have their Bluetooth connectivity set to 'on' and be able to receive information. 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.

12.21. Shredding

The increase in cases of identity theft has brought to light the need for careful disposal of sensitive or personal information. Documents containing personal details or confidential information should be shredded before binning or recycling.