# Chapter 8: Management of safeguarding records, confidentiality and sharing of information

## Aim of the chapter

i. To outline the parameters of confidentiality
ii. To outline the principles for the management of safeguarding records
iii. To outline the processes for sharing information

## Confidentiality

Key principles:

- Personal and sensitive details about the lives of adults with whom they work and their families will never be the subject of gossip
- In our church context, it is important that confidentiality includes within a prayerful space; it is never appropriate to publicly pray for or ask for prayer for a situation that must be treated with confidentiality
- We all have a fundamental right to privacy of information and confidentiality
- Joymount Presbyterian Church must only hold a very limited amount of data that is applicable and relevant only to the activity and frequency of the activity

## Management of safeguarding records

All written records must be stored in a secure location and accessed by authorised personnel only – mainly the Designated Safeguarding Person/s and select members of the Kirk Session responsible for safeguarding.

Electronic records held on computers must also be appropriately secured by way of password protection and restricted access.

Information must be disposed of within timescales that are in keeping with the requirements of the General Data Protection Regulation (GDPR) 2018. It contains guidance in factors to consider when deciding whether or not to share personal data.

The PCI's central Safeguarding Office does not manage data protection guidelines.

## Sharing of information

- Information cannot be passed on to another party without good cause or reason. Information of a confidential nature must only be communicated when appropriate and necessary for the protection of others and, in most circumstances, with the consent of the adult

- In circumstances where there are concerns about an individual's safety and welfare or the safety of others, information must be passed on to the relevant statutory authority as per Chapter 5
- Where the decision is made to share information without consent, the organisation must ensure that the adult is clearly informed of what information will be shared, why it will be shared, and with whom it will be shared, providing this does not increase risk to the adult
- As per Chapter 5, it is usually the Designated Safeguarding Person or the Minister who will be sharing information; they must ensure that they make a record of this information sharing and why consent was not secured

## Access to information

Adults at risk must normally expect to see any information held by the organisation about them and must be so informed.

This applies to paper and electronic records and must extend to access of a care record, unless any of the reasons for limiting access apply.

With specific regard to safeguarding information, consider the following before sharing any information with an individual.

It may be necessary to limit access if:

- any part of the record contains confidential information about other people
- any information that was provided by another person or agency (such as doctor or other professional) and for which you have not been able to obtain their permission to share must not be shared
- there is any possibility that access would cause serious harm to the adult's or someone else's physical or mental well-being. If you are not able to make that assessment, ensure that you seek advice from a relevant individual who can assess the impact of potential harm

**CHAPTER END**