The Methodist
Church in Sheffield

Sheffield Methodist Circuit Policy for:

Arrangements for the Secure Storage, Retention and Sharing of Safeguarding Information.

To be read in conjunction with the **Methodist Church Safeguarding Policy, Procedures and Guidance (July 2023)** and **Procedures for the Management of Safeguarding Information (July 2023)**

Storing Safeguarding Information

The following measures should be put in place if material containing confidential or criminal data is retained:

- Access provision should be carefully planned
  Only those that are required to see and use records should have access to them.

For Sheffield Methodist Circuit the following people have access to Safeguarding Information on a routine basis:

- **Revd Romeo Pedro, Superintendent Minister**
- **Revd Debora Marschner, Superintendent Minister**
- **Debbie Wheeler, Circuit Safeguarding Officer**

  In an emergency Maryke Turvey (Chair of the Safeguarding Committee) is also permitted to view documents.

  Data held on personally owned computers can be lost if unforeseen personal circumstances arise. This should never be the sole source of safeguarding records.

- Digital files should be subject to regular back-up.
  If the data is stored on a stand-alone computer. The provisions for back-up should be away from this source to ensure that there is another copy if hardware is lost or corrupted beyond recovery. A secure server is the best option for back-up, where available but again access to safeguarding files should be limited to dedicated personnel. **In the Sheffield Methodist Circuit all electronic safeguarding incident records are password protected. The password is known to Revd Romeo Pedro, Superintendent Minister, Revd Debora Marschner, Superintendent Minister, Debbie Wheeler, Circuit Safeguarding Officer and Maryke Turvey (Chair of the Safeguarding Committee)**

- Pen drives or removable media must be encrypted if they are being used to store safeguarding records. However, the risks of loss of such items are higher than less mobile storage so great care should be taken in use.

- Software which identifies viruses, malware and phishing must be installed on systems storing safeguarding records. It must be regularly updated and the provision must include a regular scanning facility.

- Hard copy material must be stored in lockable cupboards or cabinets. Where available, these should be fire-proof. **In the Sheffield Methodist Circuit these documents are stored in a fire-proof safe within the circuit office.**

- If material is scanned for digital retention, care should be taken to ensure that all parts of the document are contained in the scan, particularly the edges of documents. It is important to retain the integrity of the document, in case it is needed for proceedings at a later date.

- If plans are made for archiving safeguarding material with another institution, that organisation must be informed of the Methodist Church's requirements relating to retention of safeguarding records to ensure that records are not destroyed in error at a later date.

- Passwords must not include personal data which is easily identifiable e.g. a name, address, place or date of birth.

Retention of Safeguarding Information

The following table provides information about retention periods relating to safeguarding data:

Type of Record	How long to keep it for	What to do with it
Clear DBS certificate	The information on the DBS certificate should only be stored for up to 6 months from the recruitment decision. The exception to this is the date for renewal reminders. The certificate itself is retained by the applicant.	Destroy
Risk Assessment recommendations and a management plan in the event of	Retain for 75 years after appointment / employment	Destroy

an unclear or blemished DBS disclosure	ceases / confirmation of blemished DBS details	
Records of other safeguarding adults or child protection concerns either within the church / circuit, church / circuit related activity, or within a family by an individual where the church was the reporting body or involved in care or monitoring plans that is any sex offender risk assessments and monitoring agreements.	Retain for 75 years after the conclusion of the matter	Destroy
Records of any children's activities, Sunday School / Junior Church / Youth Club registers and related general safety risk assessments. Any communication from parents or other parties in relation to the above.	Retain for 75 years after the conclusion of the matter	Destroy
Personal records of individuals with contact with children and vulnerable adults including all documents concerning any allegations and investigations regardless of findings.	Retain for 75 years after the conclusion of the matter	Destroy

Sharing Information

Working Together to Safeguard Children 2018 states that sharing information is an intrinsic part of safeguarding and the decision about what to share and when can have a huge impact on individuals' lives. The early sharing of information is the key to providing effective early help where there are emerging problems and at the other end of the scale, can be essential in putting in place effective child protection services.

Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare, and protect the safety, of children, which must always be the paramount concern.

All the above applies as much to adults as to children.

In the document The Protection of Children in England: a progress report, Lord Laming recommended that all staff in every service from statutory services to the voluntary sector should understand the circumstances in which they may lawfully share information. There have been many examples where poor information sharing has led to serious harm

including the deaths of vulnerable individuals, and poor or non-existent information sharing is repeatedly flagged up in government reviews of serious incidents where death has occurred.

Seven Golden Rules of Information Sharing

1. General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from the Regional Officer for safeguarding if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Where possible, share information with consent. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear about the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.
5. Consider safety and well-being. Base your information-sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Signed: ---------- **Chair of Circuit meeting**

Name: Romeo R. Pedro

Date: 26/03/26