Safeguarding Recording Policy & Procedures – ***including appropriate arrangements for the secure storage, retention and appropriate sharing of safeguarding information.***

Church Name:

Date Adopted:

Contents:

The purpose of this policy is to check that procedures are in place and to provide clarity about the roles and responsibilities of those trusted with recording and reporting safeguarding issues at ……..

It is to be read in conjunction with the Methodist Church Safeguarding Policy, Procedures and Guidance (2020).

To be reviewed annually

Respond promptly and appropriately to every safeguarding concern or allegation (pg 17)

Anyone who brings any safeguarding suspicion, concern, knowledge or allegation of current or former abuse to the notice of an officeholder within the Church will be responded to respectfully and actively.

All safeguarding work will be recorded with clarity and detail. All suspicions, concerns, knowledge or allegations that reach the threshold for reporting to the statutory authorities, will be reported. This will be done irrespective of the status of the person.

All officeholders and employees within the Church will work in partnership with the statutory authorities.

In responding to concerns or allegations of abuse relating to ministers, the Church will act in accordance with the requirements of criminal and civil law and the Constitutional Practice and Discipline of the Methodist Church, and so will respect the rights and uphold the safeguards afforded in these, both to the victim/survivor and the subject of concerns or allegations.

Recording

In a church context, safeguarding records are needed in order to:

- Ensure that what happened and when it happened is recorded
- Provide a history of events so that patterns can be identified
- Record and justify the action/s of advisers and church workers
- Promote the exercise of accountability
- Provide a basis of evidence for future safeguarding activity or formal proceedings
- Allow for continuity when there is a change of personnel.

When making records the following practice should be followed:

- Wherever possible, take notes during any conversation (or immediately after if more appropriate). Using the **CHURCH SAFEGUARDING CONCERN FORM** found on page 6&7 of this policy ensures that all relevant information is gathered.
- Ask consent to make notes, taking age and understanding into account.
- Explain why you want to take notes, and that they can have access to the information they have shared with you.
- Make sure your notes are legible, clear, concise, relevant, through and jargon free.
- Use the person's own words and phrases. Do not attempt to sanitise language or improve grammar.
- Ensure the notes are up to date, signed, dated and timed.
- Ask the person to review the notes and confirm that they are accurate.
- Pass records to the District Safeguarding Officer, Alison Hill, as soon as possible but at the latest by noon of the next day.

- Keep a log of all actions you have taken and details of referrals to statutory agencies. Please refer to page 7 for an example of the Case Note form we agree to use.

Retention of Safeguarding Information (pg82)

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

Item	Record Keeping	Retention
Record of a safeguarding concern or allegation relating to a child or vulnerable adult. This may be a member, volunteer, employee, role holder or minister. This includes risk assessments and safeguarding contracts and all related materials.	A record should be retained of the nature of the allegation or concern, actions taken and the outcome.	75 years after the last contact relating to the subject or any survivor
Other material held as part of safeguarding records.	This may include data supplied from other sources which may be subject to shorter retention periods if not forming part of a safeguarding record.	75 years after the last contact relating to the subject or any survivor

Storing Safeguarding Information (pg 83)

The following measures should be put in place if material containing special category 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 …….. Methodist Church the following people have access to Safeguarding Information on a routine basis:
    -
    -
    -

  In an emergency …….. 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 personnel listed in the access protocol.

- 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.
- 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. Choosing three random words for a password can be easily remembered by visualisation of the items together and will create an appropriately secure password. This can be enhanced further by using a capital letter, number and symbol.

Sharing Information (pg 133) (Pg 86)

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.

Practitioners should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children, whether this is when problems are first emerging, or where a child is already known to local authority children's social care (e.g. they are being supported as a child in need or have a child protection plan). Practitioners should share important information which may impact the child's safety or welfare about any adults with whom that child has contact.

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 (pg 134)

1. Remember that the 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 other practitioners 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, and where possible, respect the wishes of those who do not consent to having their information shared. 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.

CHURCH SAFEGUARDING CONCERN FORM

(Any person can complete this form)

PLEASE NOTE: If you are worried about contacting us and giving your details, please be assured that we will do what we can to support you. Please telephone your District Safeguarding Officer and they can talk with you about this. Your District Safeguarding Officer can also help you to complete this form or take details over the telephone.

We can arrange pastoral care for you if you would find this helpful. If you would like this, please tick here ___ or contact your District Safeguarding Officer.

Referrers details

Name:	
Role/Position:	
Tel:	
E-mail:	
Circuit/District:	

Details of the person you are worried about

Name:	
Address:	
	Postcode:
Tel:	
E-mail:	
Child or Adult:	**Approximate age or date of birth if known:**
Role (if applicable):	
Church/Circuit:	

If the person you are worried about is a child or vulnerable adult, it would be helpful if you could give some details about their carer.

Parent/Guardian/Carer

Name:	
Address:	
Tel:	
E-mail:	

Please tell us what you are worried about, when this happened and where:

Could you tell us what action has already been taken (if any)?

Please let us know of any other information you think would be helpful for us to know:

PLEASE NOTE:
We may need to share the information you have provided with other agencies to help ensure the person you are referring and others are safe. If the information is passed on to the statutory authorities your name may be disclosed to the person you are referring. If you do not wish for your name to be shared please make this explicit.

[NAME OF CHURCH/ CIRCUIT/DISTRICT] cares about your privacy and your trust is important to us. Our Privacy Notice explains how Local Churches, Circuits and Districts within the Methodist Church in Great Britain collect, use and protect your personal information. It also provides information about your rights (paragraph 9 of the Privacy Notice) and who to contact (paragraph 1 of the Privacy Notice) if you have any questions about how we use your information. You can find our Privacy Notice online (www.tmcp.org.uk/about/data-protection/managing-trustees-privacy-notice) or displayed [INSERT DESCRIPTION OF WHERE PEOPLE CAN FIND YOUR HARDCOPY}. [NAME] will try to deal with any questions as a local point of contact. Alternatively, if viewing this form on line **click here** to read our Privacy Notice.

Thank you for completing this form.

Ongoing Case Note Recording

Name *(person of Concern)*	
Name of Referrer	
Main Contact:	

Date & Time	*Day dd/mm/yyyy @ 00:00*
Contact Type	*For example: Phone call, emails, face to face meetings, minutes, documents etc*
Description	*Phone calls & face to face: summery of the conversations including any actions for either party.* *Emails: Simply cut and paste into this box.* *Minutes: Cut and paste or scan / photo graph into the box.* *Documents: Small documents can be cut and pasted in, larger documents should give the title and the location where they can be found.*
Add to Chronology?	*Please ignore this box – for DSO only*

Date & Time	
Contact Type	
Description	
Add to Chronology?	

Date & Time	
Contact Type	
Description	
Add to Chronology?	

Date & Time	
Contact Type	
Description	
Add to Chronology?	

Date & Time	
Contact Type	
Description	
Add to Chronology?	

Date & Time	
Contact Type	
Description	
Add to Chronology?	

Please continue to cut and paste tables as needed.