

Working together



*to make our church communities safer*

# **Safeguarding Records: Joint Practice Guidance for the Church of England and the Methodist Church.**

**Published: 24 June 2015  
Review Date: May 2016**

## Preface

This joint practice guidance is intended to support the work of Safeguarding Advisers and those working with children and adults experiencing, or at risk of abuse or neglect, where record keeping is required. It complements both churches' approach to record keeping and addresses those special issues that relate to safeguarding. It is in response to requests by a number of Districts and Dioceses and has been developed through the Joint Safeguarding Working Group comprising Methodist and Church of England Safeguarding Advisers.

This joint practice guidance has been approved by the Methodist Church and the House of Bishops, and as such it is recommended that you follow this guidance. Failure to do so could invalidate your insurance cover.

We hope you find this useful in your practice.

Yours in Christ's fellowship,

+ *Paul*

*Liz*

**Bishop Paul Butler**

Bishop of Durham

Joint chairs of the joint safeguarding group

**Revd Dr Liz Smith**

Chair Leeds District

## Joint Working

The Church of England and the Methodist Church of Great Britain entered into a covenant commitment in November 2003 after conversations lasting several years<sup>1</sup>. One of the expressions of this covenant is to develop joint safeguarding arrangements.

Methodist Church and Church of England Practice Advice Papers are approved by the Joint Safeguarding Working Group of the Methodist Church and the Church of England to assist in the development of local safeguarding arrangements. This is jointly chaired by the Bishop of Durham for the Church of England and Dr Elizabeth Smith for the Methodist Church.

## Statement of Safeguarding Principles

The Church of England and the Methodist Church work in partnership with other Christian Churches and other agencies in delivering safeguarding. The following statement of principles appears at the head of each safeguarding policy:

We are committed to:

- The care, nurture of, and respectful pastoral ministry with, all children, young people and all adults;
- The safeguarding and protection of all children, young people and all adults
- The establishing of safe, caring communities which provide a loving environment where victims of abuse can report or disclose abuse and where they can find support and best practice that contributes to the prevention of abuse

To this end:

- We will carefully select, support and train all those with any responsibility within the Church, in line with the principles of Safer Recruitment.
- We will respond without delay to every complaint made, that any adult, child or young person may have been harmed, cooperating with the police and local authority in any investigation.
- We will seek to offer informed pastoral care and support to anyone who has suffered abuse, developing with them an appropriate ministry that recognises the importance of understanding the needs of those who have been abused, including their feelings of alienation and/or isolation.
- We will seek to protect survivors of abuse from the possibility of further harm and abuse.
- We will seek to challenge any abuse of power, especially by anyone in a position of respect and responsibility, where they are trusted by others.
- We will seek to offer pastoral care and support, including supervision, and referral to the appropriate authorities, to any member of our church community known to have offended against a child, young person or adult who is vulnerable.

In all these principles we will follow legislation, guidance and recognised good practice.

---

<sup>1</sup>[An Anglican Methodist Covenant](#).

<b>Contents</b>	<b>Page</b>
Preface	2
Joint Working	3
1. Introduction	4
2. Principles of a Good Safeguarding Record	5
3. Information Sharing	5
4. What should be recorded?	7
5. Safeguarding Records: Storage, access, confidential emails / archive / retention policy and working with the statutory sector	8
Suggested Model Templates for Safeguarding Records	10

## 1. Introduction

1.1. This guidance seeks to set out what should be recorded in relation to safeguarding concerns. It sets out good practice concerning both the :

- nature of the actual recording
- requirements for the safe storage and processing of this data.

1.2. Whilst the guidance is aimed at Diocesan and District Safeguarding Advisers<sup>2</sup> it may also be useful, for example, to Ministers / Priests, Parish Workers and Circuit / Church Safeguarding Coordinators and anyone who may need to record a safeguarding matter. It may also be a useful training aid.

1.3. Good record keeping is an important part of the safeguarding task. Records should use clear, straightforward language, be concise, and accurate so that they can be understood by anyone not familiar with the case. They should clearly differentiate between facts, opinion, judgements and hypothesis.

1.4. In the 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.
- Allow for continuity when there is a change of personnel.

Example: When a minister moves between Parishes / Circuits, a youth worker moves to a different post, or there has been a change of safeguarding adviser, the availability of a safeguarding record is essential so that one can know what has happened in the past.

---

<sup>2</sup> For the purposes of brevity and simplicity in this guidance, all roles are covered by the term ‘adviser’ and the guidance is applicable to both children and adults experiencing, or at risk of abuse or neglect. Advisers should be aware that there may be slight variations in related documents referred to, in Wales and Scotland.

## 2. Principles of a Good Safeguarding Record

**Proportionality** – Only record information that is relevant and necessary for your specific purpose, avoiding where possible repetition of written information.

**Accountability** – recording practice must comply with legislation, case law, professional standards / codes of practice and guidance.

**Transparency** – where information in a case record is classed as personal data pursuant to the Data Protection Act 1998 it is likely to be available to those about whom it is written, in accordance with the provisions of that Act (unless one of the exemptions apply). In any event, it is good practice for the information contained in the records to be available to the subjects of those records, whenever it is safe and possible to do so.

**Accessibility** – the written record is a vital tool and should be accessible to those who have a need to know this information. As an example, this means that the safeguarding adviser must ensure that an authorised individual from within the church is able to access the safeguarding records in the event that the safeguarding adviser is absent or otherwise unavailable.

**Accuracy** – the subjects of these records are entitled to expect that the safeguarding adviser's records are accurate. Under the Data Protection Act 1998, it is a requirement that personal data is accurate and where necessary kept up to date. Bear in mind that making such records accessible upon request (where it is possible to do so) is a good way of ensuring this accuracy.

**Security** – Records should be stored securely and measures taken to avoid loss, theft, damage and inappropriate access or onward disclosure. In an age of digital storage and exchange of information, this requires additional care, (see section 6 below entitled 6 'Safeguarding Records: Storage, access, confidential emails / archive / retention policy / and working with the statutory sector').

## 3. Information Sharing<sup>3</sup>

- 3.1. The Data Protection Act 1998 is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.
- 3.2. Be open and honest with the person (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. It may not be appropriate to inform a person that information is being shared, or seek consent to this sharing. This is the case if informing them is likely to hamper the prevention or investigation of a serious crime, or put a child at risk of significant harm or an adult at risk of serious harm.
- 3.3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible. Legal advice from the Diocesan Registrar and consultation with the Diocesan Secretary / Connexional Safeguarding Team / DSO must be sought, if there is any doubt as to whether or not you can share information.
- 3.4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgment on the facts of the case.
- 3.5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

---

<sup>3</sup> Department for Education [guidance on information sharing](#).

- 3.6. Justified, necessary, proportionate, relevant, 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 people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
- 3.7. Keep a record of your decision and the reasons for it, whether your decision is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.
- 3.8. When information is shared without the subject's consent or knowledge, it is recommended that the decision on sharing be discussed with the safeguarding adviser's Bishop or District Chair in consultation with a legal adviser to add a further level of protection should the decision to disclose in this way be challenged. A record of the decision to disclose and reasons for it must be endorsed on the safeguarding file.
- 3.9. If a child or adult is in **immediate** danger and / or requires immediate attention, call the emergency services on 999.
- 3.10. If there are concerns about a child or adult who is vulnerable this should be reported to the children or adult social care team who operate 24 hours. Any reports made should be also be reported to the safeguarding adviser.
- 3.11. The statutory authorities or others (e.g. the police or social services) may provide a safeguarding adviser with information which could be shared in order to manage a safeguarding risk. Where this occurs the following guidelines may be helpful:
  - The information provided must be in writing and agreed or confirmed in writing with the body or person supplying the information.
  - With whom the information can be shared must be agreed in advance.
  - A careful note of all these elements must be recorded on the relevant file and be evident to anyone else looking at the file.

The key in this situation is to decide whether the public interest in sharing the information overrides the interest in maintaining confidentiality. It is therefore important to weigh up what might happen if the information is shared against what might happen if it is not shared, (for instance, will the proposed sharing help to prevent any safeguarding risk?). Although each case needs to be decided on its own particular facts, generally, if there is a clear risk of significant harm to a child or serious harm to an adult, the public interest test will usually be satisfied. If unsure, seek advice.<sup>4</sup>

---

<sup>4</sup> The Data Protection (Processing Sensitive Personal Data) Order 2000 allows the processing (which will include sharing) of sensitive personal data (e.g. includes data about a person's sexual life or information about a person's commission or alleged commission of an offence) without consent, if it is in the substantial public interest and is necessary for the purposes of the prevention or detection of any unlawful act or where it is necessary for the protection of the public from "...dishonesty, malpractice, or other seriously improper conduct...".

Example: The Police, Probation Service or maybe another church may assist by disclosing details concerning sexual offences committed by an individual. However, the disclosure may be limited to the safeguarding adviser and the priest / minister. This should be recorded on the file.

It may be necessary to provide an edited version of the information to a support group, congregation or other person with a valid interest. The terms of this disclosure should be agreed with the person / body who first provided the information.

Full disclosure should be considered if at all possible. The omission of material by an editing process may be challenged and therefore a record justifying why material has been removed should be kept. The record of this justification should be included in the disclosure itself. Further, what might appear at first to be non-significant material and not disclosed may later become significant<sup>5</sup>.

#### 4. What should be recorded?

4.1. A choice of two model templates for recording case information and ongoing case management action is included at Appendix 1.

4.2. The following approach is helpful in considering what should be written.

- **A written record** of the event or conversation should be made as soon as is practicable (after the event or conversation but always within 24 hours).
- **Who** is it about? (the names of all key people including any actual / potential witnesses).
- **What** happened? (use exact quotes where possible, in quotation marks).
- **How** did it happen? (for example, if someone is alleged to have assaulted a child, did they use an implement? Or was it a kick? Or a hit?).
- **Where** did it take place?
- **When** did it take place?
- **Why** did it happen? (this allows you to record any explanations offered to you by the people involved. It is not the place for your own analysis).
- **What should happen next** (what action will follow, for example, what are you going to do next, what is X going to do next, making sure it is in the diary in Y days time as a reminder).
- **Recording what did happen next and the checks made to ensure effective follow up** (did X do what they said they were going to do?).
- **Include the views / perspective of the child or adult who is vulnerable.**
- **Analysis.** The safeguarding adviser should analyse all the information gathered to decide the nature and level of the child's needs / the needs of the adults experiencing, or at risk of abuse or neglect and the level of risk, if any, they may be facing.
- **Records must always be dated and the author identified.**
- **Indexing.** The safeguarding adviser should ensure that District / Diocesan records are able to be searched or indexed so that previous names and concerns can be easily retrieved.
- **Summary.** The safeguarding adviser should ensure, if a church worker has a separate personnel file, that a summary of any concerns and the outcome is filed on the personnel file.

4.3. Facts and professional judgments (analysis) should always be distinguished in the record and the record must not be disrespectful to the subjects. Always bear in mind they may well be read by the subject(s) who have a right of access to their files – see 6.3 below.

---

<sup>5</sup> Most Social Service Departments and Police Public Protection Units would be happy to have an initial 'advice' conversation concerning an issue without identifying a 'victim' or 'suspect'

In the example below concerning an allegation of a youth worker assaulting a child, facts and professional judgement are not separated.

Jon Smith's mother came in on Monday 23<sup>rd</sup> September and claimed that Brian had kicked Jon last week and Jon had a bruise on his thigh. I don't think this happened. Brian and Jon get on well and Mrs Smith seemed to be overwrought and drunk and shouted that she would go to the police.

However, a more effective record differentiates between facts and professional judgement which is based on evidence.

On Monday 23<sup>rd</sup> September 2013 a woman came to the youth club at the beginning of the session and told me that Brian King, a youth worker, had kicked her son, a child, named Jon Smith, at the youth club last week. As a result Jon had sustained a large bruise on his thigh. From my reading of the records and discussion with Jill and Peter, the other workers on duty last week, it seems unlikely that this happened at the youth club. There is no record of an incident and Jill and Peter recalled that Jon had been engaged happily in activities with Brian during the evening.

When she came to the youth club on 23<sup>rd</sup> September Mrs Smith appeared to me to be visibly distressed. I asked her to sit and talk further with me about the alleged incident but she left the youth club shouting "I'll take this further just you wait – the police will be knocking on your door".

## 5. Safeguarding Records: Storage, access, confidential emails / archive / retention policy and working with the statutory sector

- 5.1. The Church of England publishes a number of [Document Management Guides](#).
- 5.2. The Methodist Church also has advice in [Guidance of Best Practice in Retaining Records](#).
- 5.3. The Information Commissioner's Office has published advice about [access to personal records](#) and [protecting personal data](#) and has also published a report on [unprotected personal care records](#).
- 5.4. What follows are key points about managing safeguarding records:
  - 5.4.1. Safeguarding records should only be seen by those who need to have proper access to them.
  - 5.4.2. There should be a written protocol about who has access to the records and how records are accessed in an emergency or in planned or unplanned absences of the record holder.
  - 5.4.3. Paper files should be contained in a lockable fire proof cabinet.
  - 5.4.4. Electronic files should be password protected and backed up regularly. A secure server is preferable. Systems should be virus protected. Data must never be stored on pen drives or other removable media unless encrypted.
  - 5.4.5. Great care should be taken when scanning paper records so that they retain their authenticity. This is especially the case when records are required in criminal or civil cases.
  - 5.4.6. Make passwords hard to guess (6-12 characters in length, at least one capital letter and at least one symbol). Do not use a word that appears in a dictionary as this is easily broken.



- 5.4.7. Sending information via e-mail is quick and easy but is open to the risk that someone other than the intended recipient can intercept it. Assume that it could be read by anyone. This will help to ensure that you take appropriate care both in the content of the email and any attachments. Take care to check the address you are sending it to.
- 5.4.8. Personal data in relation to safeguarding is likely to be classified as 'sensitive personal data' under the Data Protection Act because it is likely to relate to an individual's sexual life or the commission or alleged commission of an offence. Greater care is required when handling sensitive personal data and you should seek professional advice (e.g. from your Diocesan Registrar) if you are ever unsure of how to manage such data.
- 5.4.9. Emails containing safeguarding personal information should ideally be in an approved encrypted format. Most organisations are moving to this level of security. Some may consider using the free Criminal Justice System secure email system <https://www.cjism.net/>.
- 5.4.10. If full email encryption is not available, email file attachments should be always protected by an approved encryption (password protected) method<sup>6</sup>.
- 5.4.11. No letter containing confidential information and identifying details should be sent other than by 'Special Delivery' (which tracks documents online together with signed proof of delivery) Always use the double envelope safeguard. The relevant information should be contained within an inner envelope marked confidential but no classification details shown on the outer envelope.
- 5.4.12. Professional advice (IT and Legal) should always be obtained in relation to digitisation of old records.
- 5.4.13. Safeguarding record retention in the Methodist Church. [Guidance of Best Practice in Retaining Records](#) (page 5) states they should be kept for 75 years.
- 5.4.14. Safeguarding record retention in the Church of England. [The Care of Diocesan Records](#) (paragraph 9.7) states that personnel records in relation to lay employees whose responsibilities bring them into contact with children should be kept indefinitely after their employment ceases. Pursuant to the House of Bishops' guidance entitled 'Personal Files Relating to Clergy'<sup>7</sup> records and copies of records in relation to safeguarding allegations and concerns with regard to clergy should be retained for 50 years from the cleric's death, (page 20).
- 5.4.15. Working within local Multi Agency Public Protection Arrangements (MAPPA) or within the Local Safeguarding Boards arrangements (Children or Adults) may require agencies to follow locally agreed protocols.

---

<sup>6</sup> Sometimes computer firewalls reject fully encrypted emails or password protected emails as 'hostile'. If an encrypted email is sent it should be followed up by a telephone call or an 'open' email informing the recipient that they have been sent an encrypted / password protected email so that they can check their inbox and /or contact their system administrator if an encrypted email is not received.

<sup>7</sup>[https://www.churchofengland.org/media/660031/clergy%20file%20guidance%20notes%20\(april%202013%20edition\).pdf](https://www.churchofengland.org/media/660031/clergy%20file%20guidance%20notes%20(april%202013%20edition).pdf)

## APPENDIX 1

### Suggested Model Templates for Safeguarding Records

The following two model template examples can be used as a one-off reporting template, for the safeguarding adviser's running record, or in a local church where, for example, a person who represents a safeguarding risk attends a local church. (It is designed for electronic use and if printing for use on paper, expand the boxes first.)

These templates are not intended as mandatory examples as it is recognised that a number of Districts / Dioceses already have more complex systems. They are models of good practice which can be used or amended as required.

#### Example 1

##### Name of Diocese / District / Parish / Circuit

<b>Case Subject:</b>	Name: Date of Birth: Address: Telephone: Mobile: Email
<b>Case type (Delete as appropriate)</b>	<b>Child/Young Person, Adult who is Vulnerable, Domestic Violence or Abuse, Other Casework</b>
<b>Case Start date:</b>	
<b>Contact person: (the person who first raised the issue)</b>	Name: Church/Agency: Address: Telephone: Mobile: Email:
<b>Issue: (e.g. Nature of concern / risk/ behaviour)</b>	
<b>Other contact 1 (e.g. Parent / Carer / church worker /other)</b>	Name: Relationship to Case subject Church/Agency: Address: Telephone: Mobile: Email:
<b>Other contact 2 (e.g. Parent / Carer / church worker /other)</b>	Name: Relationship to Case subject Church/Agency: Address: Telephone: Mobile: Email:
<b>Other contact 3 (e.g. Parent / Carer / church worker /other)</b>	Name: Relationship to Case subject Church/Agency: Address: Telephone: Mobile: Email:

<b>Detail initial and following dates in chronological order / what was said / actions agreed and by whom</b>	<b>Author &amp; Role</b>
Date	

**Example 2**

[Name of District/Diocese]

**Confidential Incident / Concern Report Form**

Ref No.

<b>Name and contact details of child / young person / adults experiencing, or at risk of abuse or neglect / at risk:</b>	
<b>Name and contact details of parent / guardian / carer of above named:</b>	
<b>Name and contact details of worker / member / attendee causing concern:</b>	
<b>Name and contact details of parent / guardian / carer of above named:</b>	
<b>Position and church of person causing concern:</b>	
<b>Nature of concern: (the allegation / behaviour / risk that is causing concern):</b>	
<b>(Names of principle parties are essential. If you have not done so make a factual written record of your observations and any conversations - sign and date it)</b>	
<b>Who have you spoken to about your concerns?</b>	
<b>Child / young person / adults experiencing, or at risk of abuse or neglect / at risk:</b>	<b>Yes / No</b>
<b>Senior staff / line manager Position: Name:</b>	<b>Yes / No</b>
<b>Contact details of senior staff / line manager:</b>	
<b>Social Services</b>	<b>Yes / No</b>
<b>Police</b>	<b>Yes / No</b>
<b>Probation</b>	<b>Yes / No</b>
<b>Name / Position / Contact details of persons contacted:</b>	
<b>Initial Report compiled by: Signature: Date and time:</b>	
<b>Initial action / feedback at Circuit / Parish / District / Diocese level:</b>	
<b>Name / contact details of person taking action:</b>	
<b>Position / Role Date and time:</b>	

