Christ Church Ware
Jesus led, Spirit empowered, Grace based.

Record keeping:

Based upon the recommendations contained within "safeguarding records: joint practice guidance for the Church of England and the Methodist Church- published 24th June 2015"

1. Introduction

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.

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.

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.

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

3. Information Sharing

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.

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.

The Parish Safeguarding Officer or incumbent must seek advice if you are in any doubt, without disclosing the identity of the person where possible. Legal advice from the Diocesan Safeguarding Advisor must be sought if there is any doubt as to whether or not you can share information.

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.

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.

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.

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.

When information is shared without the subject's consent or knowledge, it is recommended that the decision on sharing be discussed with the Dioceses Safeguarding Adviser's in consultation with a legal adviser if appropriate 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.

If a child or adult is in **immediate** danger and / or requires immediate attention, call the emergency services on 999.

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 Parish Safeguarding Officer and the Diocese Safeguarding Adviser.

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.

4. What should be recorded?

The following approach should help 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 Parish Safeguarding Officer 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 Parish Safeguarding Officer should ensure that parish records are able to be searched or indexed so that previous names and concerns can be easily retrieved.
- **Summary.** The Parish Safeguarding Officer 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.

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

The Church of England publishes a number of Document Management Guides. 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.

What follows are key points about managing safeguarding records:

- Safeguarding records should only be seen by those who need to have proper access to them.
- 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.
- Paper files should be contained in a lockable fire proof cabinet.
- 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.
- 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.
- Make passwords hard to guess (6-12 characters in length, at least one capital letter and at least one symbol).
- 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.
- 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.
- 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.cjsm.net/ .
- If full email encryption is not available, email file attachments should be always protected by an approved encryption (password protected) method.

- 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.
- Professional advice (IT and Legal) should always be obtained in relation to digitisation of old records.
- Safeguarding record retention in the Church of England.

Guidance on Records Retention

Basic record description	**Keep in Parish**	**Final Action**
Accident reporting sheets or book – if relating to adults	Date of incident + 20 years	Destroy
Accident reporting sheets or book – if relating to children	The date when a child became adult +20 years	Destroy
A clear CRB certificate or DBS copy	Within 6 months of the recruitment decision	Destroy
Risk Assessment recommendations and management plan in the event of an unclear or blemished disclosure	50 years after appointment/employment ceases	Destroy
Records of other safeguarding adult or child protection incidents ether within the parish or within a family/by an individual where the Parish was the reporting body or involved in care or monitoring plans. That is, any sex offender risk assessments and monitoring agreements.	50 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.	6 years after employment ceases	Destroy
Personnel records relating to lay employees not working with children and adults who may be vulnerable: including annual performance assessments, disciplinary matters, job descriptions, training and termination documentation.	50 years after the conclusion of the matter	Destroy
Parish agreement with diocese on obtaining CRB disclosures	Last action +5 years	Permanent [deposit]