



# SAFEGUARDING RECORD KEEPING

**BUGB guide to record keeping for local Baptist churches**

**The Baptist Union of Great Britain**

## **CONTENTS**

INTRODUCTION	3
WHAT IS A SAFEGUARDING RECORD?	4
COMPLYING WITH THE REQUIREMENTS OF THE INDEPENDENT INQUIRY INTO CHILD SEXUAL ABUSE	5
PRINCIPLES OF CREATING A GOOD SAFEGUARDING RECORD	6
RECORDING SAFEGUARDING CONCERNS / ALLEGATIONS	7
RETENTION OF SAFEGUARDING RECORDS	8
STORAGE, ACCESS, SHARING AND DISPOSAL OF RECORDS	9-10
APPENDIX A – SAFEGUARDING INCIDENT FORM	11-13
APPENDIX B – FREQUENTLY ASKED QUESTIONS	14

## 1) INTRODUCTION

Good record keeping is a vital part of safeguarding best practice. This guide sets out to help advise local Baptist churches about all aspects of the record keeping process, from the initial records made to the appropriate storage and retention of such records. It applies to safeguarding records relating to both children and adults at risk.

Records should use clear, straightforward language and be concise and accurate so that they are easily understood by a reader who is not familiar with the situation. They should clearly differentiate between facts and opinion. It is important that safeguarding records are stored safely and securely, and are not kept for longer than is necessary.

Under the Data Protection Act 2018, organisations are required to meet certain requirements and principles in relation to what information is recorded, how this information is shared and with whom, and the arrangements for the storage of the records. It should be noted that this guide is provided for guidance only and does not constitute legal advice.

For further information about data protection, please see the Baptist Union's *Guideline Leaflet L13: Data Protection*, which can be found on the website or by clicking [here](#). The Information Commissioner's Office (ICO) website is also a useful source of information, which can be accessed by clicking [here](#).



## 2) WHAT IS A SAFEGUARDING RECORD?

For the purpose of this guide, safeguarding records include:

<b>Allegations/ concerns</b>	Any information that relates to allegations of abuse by church workers (paid or voluntary); disclosures of abuse perpetrated by individuals outside of the church; historic abuse allegations; concerns about risk of potential harm to a child or adult; support given to a child, adult or families following a safeguarding incident: <i>e.g safeguarding-related enquiries, support and advice offered and received, allegations/concerns (including details of how these are handled, followed up, decisions reached, actions taken, referral information, pastoral support provided and eventual outcome)</i>
<b>Risk Assessments</b>	Any information that relates to risk assessments and managing risk in church settings: <i>e.g health and safety risk assessments of activities, risk assessments of known/alleged offenders</i>
<b>Safeguarding Contracts</b>	Any contracts made with known / alleged offenders in order for them to participate in church life
<b>Subject Access Requests</b>	A Subject Access Request is a written, signed request from an individual to see information held on them, which should be provided within 40 days (changing to a month under GDPR) unless an exemption applies
<b>Employment</b>	Any information that relates to the recruitment, support and training of ministers and church workers (paid or voluntary) in line with safer recruitment best practice: <i>e.g. appointment files (councils, committees and other bodies), personnel files (current and leavers), job descriptions, applications, references, staffing reviews, training completed, employment tribunal cases, termination documents</i>
<b>Disclosure and Barring Service (DBS) checks</b>	DBS checks undertaken (date of the check; name of the applicant; position applied for; type of certificate requested and its reference number; actions taken), DBS referrals, DBS risk assessments following a blemished disclosure
<b>Disciplinary action</b>	Any information relating to disciplinary action concerning a minister or church worker (paid or voluntary): <i>e.g. minister discipline files, supervision files, legal aid. It should include all documentation concerning allegations, investigations and risk assessments, regardless of the findings</i>
<b>Leadership and governance</b>	Any information that relates to safeguarding leadership and governance, including the development of local safeguarding policy and procedures: <i>e.g. agendas and minutes of safeguarding meetings, action points, policy development, training records, etc</i>
<b>Quality Assurance</b>	Audits and outcomes, annual returns, etc
<b>Events and activities</b>	Any information relating to events / activities held for children or adults at risk: <i>e.g registers, emergency contact numbers, relevant medical information, consent from parent/carer (for attendance, photography and any communications with children, such as text, phone or email), incident/accident forms, insurance documentation, hiring agreements for groups using the church premises for activities with children or adults at risk</i>

### 3) COMPLYING WITH THE REQUIREMENTS OF THE INDEPENDENT INQUIRY INTO CHILD SEXUAL ABUSE

In March 2015, the UK Government announced the establishment of an Inquiry into child sexual abuse by state and non-state organisations.

Baptist churches fall within the scope of the Inquiry and in terms of their record keeping have a responsibility “to ensure that everything of potential relevance to the Inquiry is retained”, as outlined below:

***‘Under Section 21 of the Inquiries Act 2005 the Inquiry has the power to order the production of documents. Failure to comply with such an order without reasonable excuse is an offence punishable by imprisonment (Section 35 of the Inquiries Act 2005).***

***It is also an offence for a person, during the course of an Inquiry, to destroy, alter or tamper with evidence that maybe relevant to an Inquiry, or deliberately to do an act with the intention of suppressing evidence or preventing it being disclosed to the Inquiry’.***

It is clear from the above that Baptist churches must retain any records which may be relevant to the Inquiry. Relevant material includes all of the wide-ranging safeguarding records listed above in section 2. For further information about the Inquiry, please go to: [www.iicsa.org.uk](http://www.iicsa.org.uk)



## 4) PRINCIPLES OF CREATING 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, professional standards, codes of practice and guidance.

### Transparency

Where information about a safeguarding concern is classed as personal data (any information relating to an identified or identifiable natural person), it is likely to be available to those about whom it is written, unless an exemption applies.

### Accessibility

Written records are a vital tool and should be accessible to those who have a need to know this information. For example, the Designated Person for Safeguarding must ensure that an authorised individual from within the church is able to access the safeguarding records should they be unavailable.

### Accuracy

Personal data must be accurate, and where necessary, kept up to date.

### Security

Records should be stored securely and measures must be taken to avoid loss, theft, damage and inappropriate access or onward disclosure (see section 7 for further details).

## 5) RECORDING SAFEGUARDING CONCERNS / ALLEGATIONS

It is important to record safeguarding concerns and allegations as accurately as possible, and to pass it on to the Designated Person for Safeguarding at your church within 24 hours. A template Safeguarding Incident Form can be found on pages 11-13 (Appendix A) or downloaded from the safeguarding section of the BUGB website.

<b>Timing</b>	A written record of the concern / allegation should be made as soon as possible afterwards, but always within 24 hours
<b>Who is it about?</b>	Include the names of all key people involved, including any actual / potential witnesses
<b>What happened?</b>	Use exact quotes of the person's own words where possible, in quotation marks. Include the views / perspective of the child or adult at risk. Record any action taken by church workers.
<b>How did it happen?</b>	For example, if someone is alleged to have assaulted a child, did they use an implement, or was it a kick or a hit?
<b>Where did it take place?</b>	Include the location / venue name and full address
<b>When did it take place?</b>	Include both the time and date
<b>Why did it happen?</b>	Record any explanations offered to you by the people involved. Do not include personal opinions.
<b>What should happen next?</b>	What action will follow? For example, what are you going to do next, what is X going to do next? Make sure reminders are set for any action necessary.
<b>What did happen next?</b>	Did X do what they were planning on doing? Put checks in place to make sure that this is followed up.



## 6) RETENTION OF SAFEGUARDING RECORDS

The following guidelines give indications of good practice in terms of the retention of specific types of safeguarding information.

Category	Type of Record	Retention Period
<b>Allegations/concerns/ risk assessments/ safeguarding contracts</b>	Records of safeguarding incidents, allegations or concerns	75 years after last contact with the individual concerned
	Records that relate to safeguarding concerns/allegations about church workers (paid or voluntary)	75 years after employment / role ceases
	Risk assessments / safeguarding contracts concerning known or alleged offenders	75 years after last contact with the individual concerned
<b>Events / activities specifically for children and young people / adults at risk (where no safeguarding incidents or concerns raised)</b>	Registers / records of events or activities*	At least 3 years after the event
	Parent / carer consent forms*	At least 3 years after the form has been completed
	First Aid / accident forms*	At least 3 years after the form has been completed
	Health and safety risk assessment*	At least 3 years after the risk assessment has been completed.
<b>Employment</b>	Minister personnel records where there are safeguarding allegations / investigations, regardless of the findings	75 years from the date of the minister's death
	Personnel records relating to church workers whose role involves contact with children and adults at risk	75 years after employment / role ceases
<b>Disclosure and Barring Service (DBS) checks</b>	Record of a Disclosure and Barring Service (DBS) check being undertaken for a church worker (paid or voluntary)	75 years after employment / role ceases (Please see BUGB Guide to DBS Checks for more information on what to keep)
	Record of a minister's DBS check history	75 years from the date of the minister's death
<b>Discipline</b>	Record of a church worker's (paid or voluntary) disciplinary procedure relating to safeguarding allegations / offences	75 years after employment / role ceases
	Record of a minister's disciplinary procedure relating to safeguarding allegations / offences	75 years from date of the minister's death

\*Please check with your church insurer, who may require you to keep these records for a longer period.



## 7) STORAGE, ACCESS, SHARING AND DISPOSAL OF RECORDS

Here are some key points to help you when thinking about managing safeguarding records:

### Storage

- Church workers should be made aware that their basic details are being stored and for what purpose.
- Parents and carers, as well as the children / adults at risk concerned, should be aware that records for activities / events will be made and securely stored.
- All paper records should be stored in the church office, in a lockable, fire proof cabinet. If your church does not have its own building, then we would recommend that you store your safeguarding records electronically on a cloud-based system with appropriate security arrangements in place.
- You may wish to scan paper records once no further action is needed (for example, where an incident has occurred, any necessary investigation has been completed). Great care should be taken when scanning paper records to ensure they retain their authenticity. If you are scanning records, make sure that you do not shred your paper copy before confirming that your documents are correctly scanned and saved.
- Electronic records should be password protected and backed up regularly. A secure server (e.g. a cloud based server) is preferable. Systems should be virus protected. Data must never be stored on personal computers, USB drives or other removable media unless it is securely encrypted.
- Passwords should be hard to guess and always stored separately.

### Access

- Safeguarding records should only be available to those who need to have access to them, such as the Designated Person for Safeguarding, minister, group leader, DBS verifier.
- There should be a written protocol about who has access to the records, including how records are accessed in an emergency or in the absence of the record holder.

### Sharing records

Before you share a record, make sure you've thought through the following:

- Do I have the right to share this information?
- Does the person receiving the information have a real need to know?
- Are there any conditions on sharing this information? For example, only for the named individual.
- How can I protect this information on transit?
  - a. Sending information via e-mail carries the risk that someone other than the intended recipient can intercept it. Take appropriate care both in the content of the email and any attachments. Double-check the address you are sending it to. Only copy people in on a need to know basis.
  - b. Great care is required when handling safeguarding information. Emails containing safeguarding-related personal data should ideally be in an approved encrypted format. If this is not possible, always password protect any attachments. Seek professional advice if you are ever unsure of how to manage such data.

- c. Letters containing confidential information and identifying details should be sent by Special Delivery. Use two envelopes, placing the relevant information in an inner envelope marked confidential, with no classification details on the outer envelope.
- How will I record the fact I've shared this information?
  - a. We suggest a simple form (example shown below).

## Disposal

### **At the end of an investigation:**

When you have reached the point where you are planning the long term storage of safeguarding records remember the following:

- Within your church, there is no need to keep multiple copies of safeguarding records. One full set should be kept securely, either on paper or in electronic version. The Designated Person for Safeguarding should keep control of these files.
- If several people in your church have been involved in dealing with a safeguarding concern, make sure that only one copy of any electronic correspondence is kept, and that other copies have been securely deleted (double-delete)
- Plan ahead so that records can still be accessed by those who need to deal with them in the long term.
- Be aware that the police and other statutory authorities will keep their own records of any incident you report. However, you cannot rely on their records for future reference as they will not share records with you.

### **After the storage time period has elapsed:**

- Confidential paper records should always be shredded.
- Electronic records should be permanently deleted (i.e double-deleted).

## Appendix A

### SAFEGUARDING INCIDENT FORM

*This form should be completed with the Designated Person for Safeguarding*

Name of church / organisation	
Contact details of church / organisation	

Name of Designated Person for Safeguarding (DPS)	
Contact details of Designated Person for Safeguarding	

Name of person who has safeguarding concern or to whom disclosure was given	
Contact details of person who has safeguarding concern or whom disclosure was given	

### INDIVIDUAL OF CONCERN CONTACT DETAILS

Name	
Date of birth	
Address	
Phone number / email address	

### ALLEGED / KNOWN PERPETRATOR CONTACT DETAILS

Name	
Date of birth	
Address	
Phone number / email address	

### THE INCIDENT

What happened? (Nature of concern / disclosure made - use the person's own words if known)

When did it happen? (date, time)

Where did it happen? (specific location)

Who was allegedly involved and in what way? (includes witnesses)

### ANY ACTION THAT HAS BEEN TAKEN

Have the carers or parents / guardians been informed? (Please tick)  
If so, when and by whom? If not, why have they not been informed?

Yes	No	
-----	----	--

Have the statutory authorities been informed?  
If so, please complete the below table:

Yes	No	
-----	----	--

*Example:*

Authority	Police				
Name	Bobby				
Position	Child abuse officer				
Email contact	<a href="mailto:bobby@police.com">bobby@police.com</a>				
Phone contact	077999				
Contacted by	Minister				
Date & time of contact	1.30pm 1/4/15				

Has the Local Association been informed?  
(Please do so if the statutory authorities are involved)  
If so, when and by whom?

Yes	No	
-----	----	--

Any other action taken:

### FUTURE ACTION TO BE TAKEN

What action needs to be taken?

Who is responsible for this?

### SIGNATURES

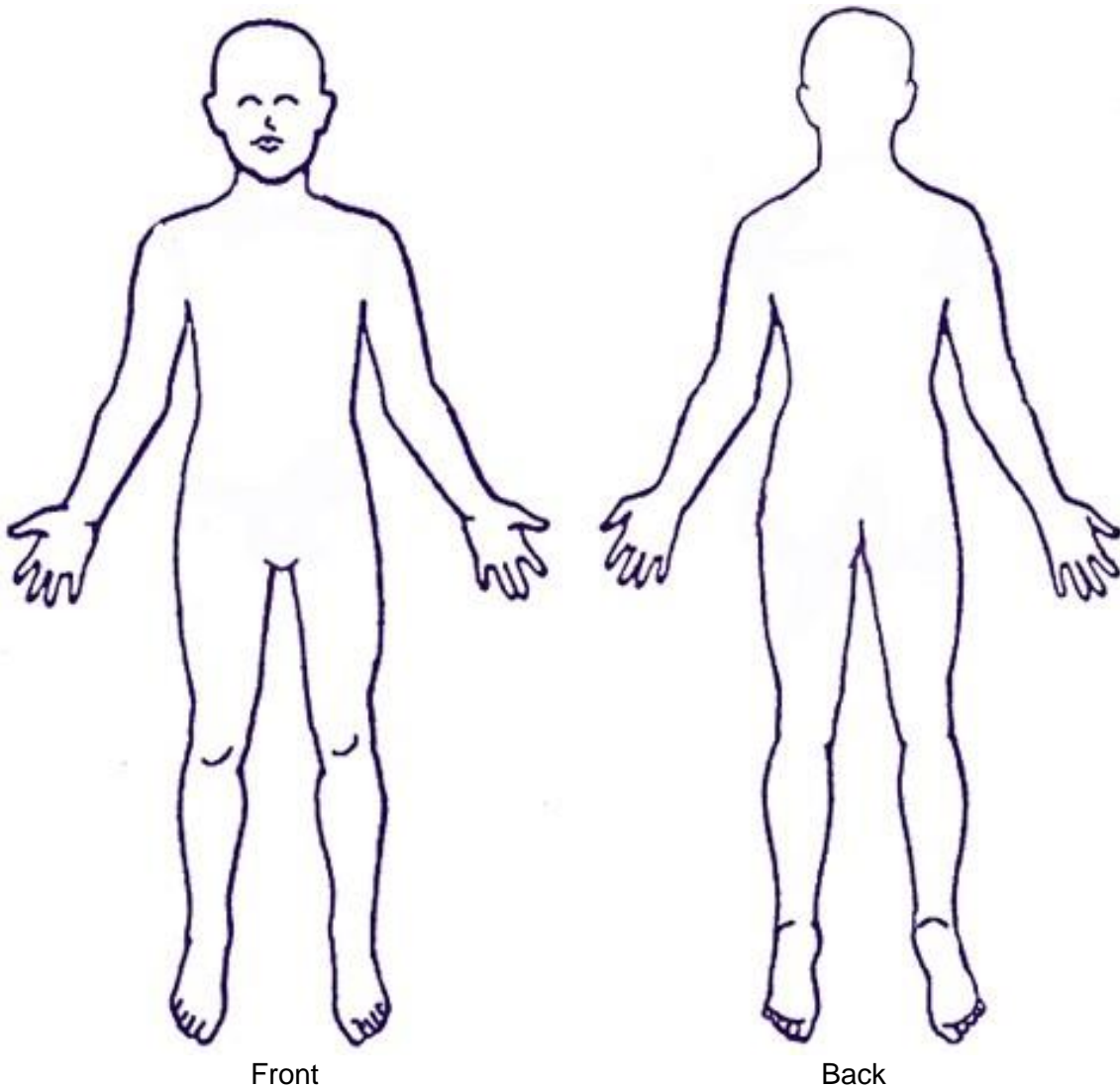
Signature of Designated Safeguarding Person		Signature of minister, or Church Safeguarding Team member	
Date & time		Date & time	

## BODY MAP

Name of Individual of Concern \_\_\_\_\_

Name of person completing this form \_\_\_\_\_

These diagrams are designed for the recording of any observable bodily injuries that may appear on the person. Where bruises, burns, cuts, or other injuries occur, shade and label them clearly on the diagram. **Remember it's not your job to investigate or to decide if an injury or mark is non-accidental. Listen, observe and pass it on.**



Signature \_\_\_\_\_

Date and time \_\_\_\_\_

## APPENDIX B - Frequently Asked Questions

**1) Who needs to know about the new requirements for gathering, processing and storing safeguarding information?**

Everyone in your church who is involved in handling information about children, young people and adults at risk.

**2) What are the rights of an alleged perpetrator in terms of making a subject access request?**

An alleged perpetrator has the right to make a subject access request, but you are acting legally if you do not supply them with data that would be likely to prejudice the apprehension or prosecution of an offender. In this instance, seek advice from your Association Safeguarding Contact straightaway.

**3) If our church puts a safeguarding contract in place do we need to send a copy to our Association Safeguarding Contact?**

Your Association Safeguarding Contact will need to see a copy of the contract, but will not store the contract afterwards, simply keeping a record of who the contract refers to, the church's name and the date it was put in place.

**4) As the DBS Verifier for our church, do I need to keep a record of DBS check certificate numbers?**

Please see the BUGB Guide to DBS Checks for detailed information on this.

**5) What if the church insurers ask us to keep safeguarding information for longer periods than this guide suggests?**

We would encourage you to comply with the greater of our guideline periods and your insurer's requirements.

**6) What should we do in the event of a breach of these data protection requirements in relation to safeguarding information?**

The 2018 Data Protection Act requires organisations to report all breaches of the data protection legislation. Reports should be sent to the Information Commissioner's Office ([www.ico.gov.uk](http://www.ico.gov.uk)).



**This policy has been produced for use in Baptist churches in England and Wales.  
Policy issue date: 14 May 2018**

Safeguarding Team, Baptist Union of Great Britain, Baptist House, PO Box 44, 129 Broadway, Didcot OX11 8RT  
Tel: 01235 517700 Email: [safeguarding@baptist.org.uk](mailto:safeguarding@baptist.org.uk) Website: [www.baptist.org.uk](http://www.baptist.org.uk)  
BUGB operates as a CIO with registered charity number 1181392