MC/18/63

Safeguarding Policy, Procedures and Guidance - GDPR Amendments

Contact Name and Details	Tim Carter; Safeguarding Adviser; cartert@methodistchurch.org.uk
Resolutions	63/1. The Council receives the report. 63/2. The Council approves the amendments to the Safeguarding Policy in line with the General Data Protection Regulation (2018).

Summary of Content and Impact

Subject and Aims	Amendments to the current Safeguarding Policy, Procedures and Guidance to reflect changes required by the introduction of the General Data Protection Regulation (2018).
Main Points	• Amendments of references to data protection terminology and legislation in line with GDPR • Requirement for privacy notices to be provided to those who report safeguarding concerns/activities and those about whom information is processed • Standard Privacy notices to be used to cover safeguarding activities in line with GDPR provisions • Requirements as to when privacy notices must be supplied • Retention directions required by the Independent Inquiry into Child Sexual Abuse (IICSA) relating to case records of child safeguarding concerns • Clarification of retention periods for safeguarding material beyond completion of the IICSA as required by the GDPR • Requirement for monitoring and support group members to sign a confidentiality agreement prior to disclosure of personal and special category data
Background Context and Relevant Documents (with function)	**Relevant Documents:** GDPR Guidance available via the Information Commissioner's website TMCP Guidance relating to GDPR
Consultations	District Safeguarding Officers
Impact	• Additional administration for those responding to safeguarding concerns and managing activities where a privacy notice will be required • Potential increase in confidence and transparency for those seeking support in relation to safeguarding concerns or impacted by safeguarding processes • Potential reduction in non-compliance risk to the Church

Introduction

The General Data Protection Regulation (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK. It is part of the wider package of reform to data protection legislation and guidance, which includes the Data Protection Bill, currently passing through parliament. The GDPR sets out requirements for the management of personal data by organisations, which come into force on 25 May 2018.

The Methodist Church Safeguarding Policy, Procedures and Guidance were updated during 2017. Additional information was included within both procedures and guidance sections providing material about confidentiality, information sharing and data security. This was in line with statute and statutory guidance available at that time, including the Data Protection Act 1998, Information Sharing for Practitioners 2015 and Working Together to Safeguard Children 2015.

The arrival of GDPR has been well publicised, increasing awareness of individuals and organisations of rights and duties relating to information management. It is likely that the actions of the church within the safeguarding arena will come under increased scrutiny from those who are part of safeguarding processes. While many of the provisions in the new regulation are similar to those contained in the Data Protection Act 1998, new procedures and guidance are required to support compliance and awareness in a potentially sensitive and contentious environment.

It is noted that the Data Protection Bill is currently passing through Parliament. This will provide further clarity in relation to data protection within UK legislation. Significant amendments relating to the draft bill have been tabled in recent months, which include provision for safeguarding as a lawful basis for processing. However, it will be sometime before the Bill receives royal assent and relevant amendments to the Safeguarding Policy, Procedures & Guidance can be made to include this legislation. As a result, it is proposed that interim changes be made to this policy to address the requirements of the GDPR with the acknowledgement that further amendments will be required during the following connexional year.

The key changes to the procedures are outlined above (Main Points) and the proposed amendments are extracted from the full policy and detailed below.

*****RESOLUTIONS**

63/1. The Council receives the report.

63/2. The Council approves the updated procedures and guidance.

Safeguarding Policy, Procedure and Guidance – GDPR Amendments

The following sections have been extracted from the current policy with additions and amendments indicated in bold, italicised text. The numbering of sections in this paper corresponds to the original policy.

4.1 Responding well

There are many situations whereby a member of the Church may have concerns, or be made aware of concerns, regarding a child or adult. The person noticing or being informed of concerns must consult with the minister, safeguarding church or circuit safeguarding officer and DSO within one working day. The only exception to informing any of the above is if one of them is the subject of the concerns. If that is the case, then they will be excluded. At no time should the person who is the subject of the allegations be informed. Contact should only be made after discussion and agreement with the statutory authorities.

General Data Protection Regulation (GDPR) requires that privacy notices are supplied to those about whom information is received by the Church. This includes direct disclosures from the parties involved and third party reports about others (see 5.1.4).

Further action will be decided in discussion and agreement with the statutory agencies.

4.1.1 Listening

If approached by anyone wishing to talk about a concern, follow the basic guidelines below:

- Consider whether the time and place are appropriate for you to listen with care and security. Do not defer listening, but seek the other person's agreement to find a suitable place to listen.
- Stay calm and listen to the information very carefully, showing you are taking seriously what you are being told. Do not pass judgement, minimise or express shock or disbelief at what you are being told.
- Listen with undivided attention and help the other person to feel relaxed. Do not put words into their mouth.
- Take into account the person's age and level of understanding. It may be appropriate to ask if they mind you taking notes while they talk or at the end so you can check with them that you have understood everything correctly – but only if it is appropriate.
- Do not make promises you cannot keep.
- Do not promise confidentiality but explain what you will do with the information
- Find out what the person hopes for.
- Reflect back key points of what has been said to confirm you have understood what has been communicated.
- ***Provide a privacy notice and explain in a clear and simple manner the information contained in it (see 5.1.4).***
- Either during (if appropriate) or after, make notes of what was said, including the date, time, venue and the names of people who were present. Sign the record.
- The district safeguarding officer should always be advised when a referral is made to Children's Services/the police.
- Provide the person with the means to contact you and be clear about how and when you will give feedback. Be prepared to continue to be there for the person. Be dependable.
- Do not contact the person about whom allegations have been made.
- Offer reassurance that disclosing is the right thing to do.

4.1.4 v. What are the actions of the district safeguarding officer on receipt of a concern?

- Consider the child's or adult's safety throughout.

- Check whether a referral to Children's Services or Adult Social Care (as appropriate) is necessary and if so, has been made.
- ***Check whether privacy notices have been provided to relevant parties and provide them if required and appropriate (see 5.1.4).***
- Consider if notification to Connexional Safeguarding Team is necessary (see next section).
- Contact the media office to discuss communications within the local church and circuit.
- Ensure management of the case is separate from anyone involved in pastoral support.
- Consider support needs to the victim/ survivor, family/close friends and the accused and their family.
- Ensure pastoral support is not provided by parties who are directly involved in the management of the case or are in supervision or oversight of anyone about whom there is a concern.
- Notify Methodist Insurance or ensure someone has done so.
- Liaise with the Connexional Officer for Legal and Constitutional Practice to agree if notification to the Charity Commission is necessary.
- Notify District Chair and Superintendent.
- Consider whether a Safeguarding Contract is necessary pending any court case.
- Consider whether colleagues from other churches or community organisations need to be informed following advice from Children's Service/Adult Social Care/ police (as appropriate).

4.5.8 Risk assessments

The Methodist Church initiates various forms of risk assessment in a response to safeguarding matters. These may be commissioned by the Connexion, completed by the district safeguarding officer or conducted at church or circuit level dependent on the circumstances. Proportionality is a fundamental principle in considering the nature or risk assessment that is appropriate in each case. Further details of relevant policies, procedures and guidance is included in the *Methodist Church Risk Assessment Policy and Procedures:* www.methodist.org.uk/safeguardingriskassessment

In any case where risk assessment is being considered, preparations should include the provision of a privacy notice to the subject of the assessment and any other party about whom information is received. Even where a privacy notice has already been provided, a new version should be supplied which addresses the specific issues relating to the risk assessment, particularly with regard to information sharing, clarification of the lawful basis for processing and consent (where applicable).

An interim Safeguarding Contract may be put in place while a police, Children's Services or Adult Social Care initial assessment or investigation are ongoing. This should also be considered when the Church becomes aware of external employment disciplinary procedure relating to a safeguarding matter that may impact on roles and activities undertaken by church members, staff, ministers or volunteers. However, detailed risk assessments which include in-depth inquiries and interviews with related parties should not be initiated until the statutory or external employment processes are concluded. This is to ensure that actions undertaken in the course of the risk assessment do not contaminate evidence or impact on such proceedings or assessments.

4.6.2 Responding well (Domestic Abuse)

(See quick guide flowcharts in 4.6.4 below)
All forms of domestic abuse are intrinsically damaging and the importance of the safety and protection of those involved must be paramount. Those responding to reports of domestic abuse should ensure that they identify whether any of the following circumstances apply:

- children are living in the household
- children are regular visitors to the household
- the victim is an adult who lacks capacity

- the victim is dependent upon their partner for care

Procedures relating to children and adults in the previous section should be followed in all cases.

- The following actions should be taken where domestic abuse is suspected:
- If you suspect someone is experiencing domestic abuse but they have not said anything to you, do not be afraid to ask but ask gentle, non-direct questions, such as "How are things at home?"
- Reassure the person that it is not their fault.
- Consider their safety and yours as well as colleagues and if possible prepare a plan of action to protect anyone disclosing abuse (and yourselves).
- Do not investigate.
- Do not confront the alleged perpetrator.
- Keep confidentiality; all conversations should be treated as confidential within the bounds of safeguarding. Seek consent to share information if you wish to discuss it with someone else unless a child or vulnerable adult is at risk.
- Remember to focus on the safety of the victim (and children, if any are involved).
- Provide information on resources/services available to them.
- Do not advise on a course of action but encourage them to explore options.
- Record the information and retain it securely.
- ***Take advice from a church, circuit or district safeguarding officer prior to sending a privacy notice to anyone other than the party reporting the issues to ensure that the safety of the survivor, any children or other parties will not be compromised.***

4.7.2.1 Arranging a Safeguarding Contract

- When a local church becomes aware of a person who is considered to be a risk, a representative of the local church should be in contact with the relevant statutory agencies and may include probation and the police.

- A small group of about five people should be set up (the monitoring and support group). This should include the minister and any people who have agreed to offer pastoral support for the offender and accompany them in worship and other church activities. It is helpful if at least one member is from outside the local church, as this helps to promote objectivity. It should also include someone with expertise and experience in this field and someone to represent the wider church community.

- A risk assessment must then be carried out**.** This should include reviewing the nature of the concerns and risk posed and looking at the church building and range of activities carried out. The police or probation service should be consulted for advice where they are actively managing the subject as part of the risk assessment. If the church was originally aware of the subject, an independent risk assessment may have already been undertaken if not done, it needs to be done, see SO690 (eg because of a blemished DBS check or previous notification to the Connexional Safeguarding Team and decisions of a safeguarding panel). Where the concern is new and shared by the statutory agencies with the church, basic safety checks should be undertaken and inform the safeguarding contract (eg what access to rooms in church buildings when other activities are taking place etc) whilst a more comprehensive risk assessment is planned and discussions had with the Connexional Safeguarding Team and DSO about who will undertake this.

- ***Preparations for the risk assessment should include the provision of a privacy notice to the subject of the assessment and any other parties invited to contribute to it. Even where a privacy notice has already been provided, a new version should be supplied which addresses the specific issues relating to the risk assessment, particularly with regard to information sharing, the legal basis for processing and consent (where applicable). Further information is available in the Methodist Church Risk Assessment Policy:***

(link to be added)

- A monitoring and support group can be set up prior to a prison release**,** or following one, where the offender is no longer supervised by probation and where there have been no convictions but serious concerns exist. Advice should be sought from the DSO and District Safeguarding Group.

- Once a group is set up, a meeting should be held with the subject and a written contract drawn up.

4.7.2.4 The Monitoring and Support Group

- ***All members of the group should be requested to sign a confidentiality agreement, which specifies how they will act in relation to information provided to them in the course of their engagement with the monitoring and support group. This will occur prior to provision of personal data and special category material about the party subject to the Safeguarding Contract. A standard confidentiality agreement can be obtained via the Methodist Church website (link to be added).***
- ***An initial briefing meeting should take place with the members of the monitoring and support group to ensure all parties are aware of data protection requirements, relevant standing orders, procedures and policies. In most cases, the district safeguarding officer is the appropriate person to provide this briefing and provide the members with an opportunity to raise questions about their role.***
- Training and support should be provided for the group**.**
- The group should meet regularly and keep a record of its meetings.
- A report should be sent to the DSO and Connexional Safeguarding Team annually or when circumstances change.
- Review appropriateness of the safeguarding contract conditions and consider whether a new risk assessment would be appropriate and discuss with the connexional safeguarding team every 3 years.
- The group should meet the subject to review the arrangements and address any concerns. If boundaries are not being kept, or if the contact is not being kept in other ways, it is important to address the problem (in situations where boundaries are not being kept, it may be necessary to prohibit the subject from coming onto church premises).
- Where police or the probation service are actively managing individuals and it is clear that there are significant issues around compliance, consideration should be made to making the relevant officer aware of the situation.
- Over time, the regularity of the meetings may be reduced if all parts of the contract are being fulfilled. The subject should never be left completely without support and monitoring. The minimum provision would be an annual, recorded discussion between the minister, local safeguarding officer and DSO or appointed DSG member and the subject.
- When officers and ministers change in the church, it will be important to ensure continuity of awareness and provision of pastoral support for the subject.
- If the subject is moving to worship in another Circuit or at another Local Church see Standing Orders 692(1)-(3)
  A safeguarding contract may only be revoked or amended following recommendations from a Safeguarding Committee in accordance with Standing Order 690A(3).

SECTION 5

Procedures for information sharing and confidentiality

Careful attention should be paid to the storage, use and sharing of data held by the church relating to other people. This is critical to ensure that those who engage with safeguarding processes have

confidence in the legitimacy and appropriateness of actions taken. The management of information is governed by law, statutory and government guidance including:

The General Data Protection Regulation (2018)
Information Sharing for Practitioners (2015)
Working Together to Safeguard Children (2015)
(The Data Protection Bill - currently going through Parliament)

Further guidance in relation to information sharing can be found in Section 7.3.2 Information Sharing Guidance.

5. 1 The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) outlines the rights of individuals regarding information that is held and used by organisations. Many of the provisions which were previously within the Data Protection Act 1998 are also present within GDPR but the requirements for transparency have been increased, along with the sanctions for failing to comply. It is important that everyone within the church understands their responsibilities under GDPR and complies with its requirements.

The introduction of GDPR provides an opportunity for all those engaging in activities, which relate to safeguarding to review how they use information about others and commit to the highest standards of data protection practice. This is in line with the Safeguarding Policy commitments contained in Section 2 and should form a natural part of safeguarding activity.

Further information is available from the following sources:
www.tmcp.org.uk
www.ico.org.uk

5.1.1 Key Terms

There are several key terms relating to data protection and the GDPR, which need to be understood in order for those supporting safeguarding within the Methodist Church to comply with their legal responsibilities.

Personal Data is any information relating to an identified or identifiable natural person, the 'Data Subject '. This could include details such as names, dates of birth and addresses provided for a church activity to support safeguarding participants or contained within information provided about a safeguarding concern. On occasions, anonymised information about a specific situation is communicated between parties. This will still be personal data if it is possible to identify the individual through the circumstances.

Special Categories of Personal Data
- *political opinions*
- *religious or philosophical beliefs*
- *trade union membership*
- *the processing of genetic data*
- *biometric identity data*
- *health information*
- *sex life*
- *sexual orientation*

In the majority of cases, safeguarding concerns will include special category personal data.

***Criminal Offence Data** is designated under a separate category with additional requirements relating to its processing. This is information relating to criminal allegations, proceedings or convictions.*

***The Controller** is the legal entity that is responsible for ensuring compliance with data protection requirements.*

- *For churches, circuits and districts, this is the Trustees for Methodist Church Purposes*
- *For the Connexional Team, this is the Methodist Council*

They will also be the relevant Controller for safeguarding, complaints and discipline matters.

***The Processor** is any person who processes data on behalf of the Controller. This will include those who record and share personal and special category data within safeguarding contexts. GDPR confirms the responsibility of processors in complying with the provisions of GDPR. For this reason, all parties who are likely to process data within a safeguarding context are advised to gain familiarity with key concepts and definitions and raise any queries or requests for clarification with safeguarding officers.*

***A Data Subject** is an individual about whom particular personal data is held by an organisation.*

***A Privacy Notice** is a notice informing individuals about why their personal data is being collected, how it will be used, their right of complaint and access to that information.*

***Data Mapping** is the process by which organisations assess the categories of information they process and record, how this information is used and for how long it is necessary to be retained. Retention information will be made available via the Methodist Church website to confirm for how long data should be held (link to be added).*

5.1.2. How must data be processed?

- *Fairly*
- *Transparently*
- *For a specified, explicit and legitimate purpose*
- *Adequate and limited to what is necessary*
- *Accurately and where necessary kept up to date*
- *For no longer than necessary for the specific purpose*
- *Securely*

Undertaking the following activities will help to ensure compliance with the principles of data processing under the GDPR:

- *Taking time to understand policies and procedures provided by the Methodist Church which address data protection*
- *Be prepared to explain an individual's rights under GDPR if they raise questions during safeguarding processes*
- *Providing privacy notices that clearly explain the lawful basis for processing and provide details of the data subject's rights*
- *Ensuring that data subjects have an opportunity to advise data processors of any inaccuracies and being proactive in making corrections within required timescales*

- *Following information provided in this Safeguarding Policy, Procedures and Guidance document about storing, retention and sharing of data, particularly with reference to security*
- *Reviewing practice to ensure that the retention of information is actively managed and time frames for retaining material are followed*

5.1.3 What are the rights of a data subject?

a) Right to be Informed
This is addressed by the provision of privacy notices (see 5.1.4) and information supplied by the Methodist Church via various sources.

b) Consent
There is a requirement where consent applies that it is true consent and that there is a right to withdraw that consent. Consent must be explicitly provided and not assumed. Many safeguarding data processing actions are required by legislation, statutory or government guidance and therefore the issue of consent may not be applicable.

c) Right of Access
This is addressed by the Subject Access Request Process through which information held about an individual may be obtained (see 5.1.5).

d) Right of Redaction
Inaccurate or incomplete data should be rectified within one month. This period can be extended to two months if the material is complicated. Third parties with which the information has been shared must be advised of the corrections.

This is done routinely within risk assessment processes where a draft copy of the assessment is supplied to the subject to allow them to identify inaccuracies and provide feedback before it is submitted to the Safeguarding Panel. Where inaccurate information has been rectified, a note should be retained to confirm that action has been undertaken, who made the amendment to the record and the date on which this was done.

If a factual inaccuracy is notified, then it is important to clarify whether it is in fact erroneous information or an evidenced judgement from a risk assessor or other party with which that person is in disagreement. It may be helpful to discuss this in more detail with the individual reporting the error, if this becomes contentious.

e) Right to Erasure or Right to be Forgotten
This is not an absolute right and may be requested in the following circumstances:
- ***the data is no longer necessary for the purpose for which it was collected***
- ***consent is withdrawn***
- ***there is no legitimate interest for the continuing processing***
- ***the data was unlawfully processed***
- ***the data related to online services aimed at children***
- ***if it causes unwarranted damage or distress***

A few exceptions exist to this right, such as that processing is necessary in order to comply with statutory requirements or is required to defend a legal claim. Bearing in mind current requirements to retain information, advice should be taken from Conference Office and/or the data controller before deleting a record which is otherwise required to be retained.

f) Right to Restrict Processing
Individuals can restrict processing activities where:

- *the accuracy of the data is questioned*
- *there has been an objection to the processing and it is being considered whether there are legitimate grounds to override the objection*
- *processing is unlawful and the individual has requested restriction as opposed to erasure*
- *the data is no longer required but the individual requires it for legal purposes*

Where it is believed that this right may be applicable relating to safeguarding information, guidance should be obtained from the relevant data controller and Conference Office, before any restrictions are put in place.

g) Right to Data Portability
This provides the ability for individuals to transfer their data from one organisation to another. Further advice should be taken from the data controller in relation to this right where applicable.

h) Right to Object
If an objection is raised by an individual to the data processing, it must be stopped immediately unless:

- *it can be demonstrated that there are legitimate grounds for processing which override the rights and freedoms of the individual*
- *is required to establish, exercise or defend a legal claim*
- *conducting research for the performance of a public interest task*

Further advice should be taken from the data controller in relation to this right where the right to object is raised as a matter of urgency.

i) Automated Decision Making or Profiling
It gives individuals the right to have an automated decision undertaken by a human. This is unlikely to relate to safeguarding within the Methodist Church.

5.1.4 Privacy Notices
Privacy notices are central to effective data protection practice within safeguarding and they should be supplied using standard documents for specific activities such as the reporting of a safeguarding concern, ongoing safeguarding case management and prior to undertaking a risk assessment. Standard documents are available via the Methodist Church website and should be used on all occasions as the basis for information provided to individuals. This is to ensure that all information required by GDPR is supplied.

Children must also be provided with information about how their data is used in the same way as adults but there is an expectation that any information provided will be appropriate to the child's age and capacity to understand.

For further details of specific information that must be included in a privacy notice see section 7.3.7 Required contents for privacy notices.

5.1.4.1 When should information be supplied?

a) If information has been provided by a person to whom it relates, a privacy notice should be supplied at the time.

However, it is acknowledged that safeguarding concerns are raised at times and situations where it may not be possible to provide a notice immediately. Disclosures are often made on the basis of perceived trust in an individual and do not relate to their role or familiarity with data protection. It may also be that the party providing the information is too distressed to receive this information

and discuss the contents at the point of initial disclosure. In such circumstances, a church, circuit or district safeguarding officer should be contacted at the earliest opportunity (within 24 hours) to provide support and assist with the provision of the required information. It will be helpful for any party in this position to acknowledge the situation with the party who is providing information and confirm when a privacy notice will be supplied.

b) If information has been supplied to the church by a third party which relates to another individual, the person to whom the information relates should receive a privacy notice within a reasonable period of the data being received within one month.

If contact is being made with that individual, it is expected that the privacy notice will have been supplied at the first point at which contact is made or before the data is disclosed to another party, if not prior to this point. Where police, children or adult services are involved or likely to become involved, advice from the relevant statutory agency should be taken before disclosing any information to a party who is not already aware that the information has been passed to the church.

Where a privacy notice is supplied to a survivor of abuse or someone who is experiencing anxiety as a result of safeguarding processes, it may be appropriate to provide an explanation in person or via telephone to provide reassurance. This should be approached sensitively and explained with care, in addition to providing the privacy notice itself. It will be helpful to emphasise that the Methodist Church places great emphasis on ensuring that all parties are made aware of their rights and details of provided as required by GDPR. It is important to recognise that the use of privacy notices will become familiar practice but may initially be unfamiliar and treated with concern. Many people will be glad for the transparency that this action will demonstrate. Some may feel concerned that clarifying circumstances or making others aware of information they may not have been aware of previously may cause unnecessary anxiety. The requirements of GDPR mean that the provision of a privacy notice addressing necessary points is now mandatory.

5.1.4.2 The Lawful Bases for Processing Personal Data

The basis for processing personal and special category data must be included in a privacy notice. This will need to be added to the relevant template with reference to the particular circumstances of the situation. Processing on the basis of consent or legal obligation may be the most relevant to safeguarding activities.

Where processing only relates to personal data, one of the following bases must be included in the privacy notice:

a) Consent: the individual has given clear consent for the church to process their personal data for a specific purpose. This basis for processing may be applicable where an application is being made for enhanced DBS clearance in relation to regulated activity.
b) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations). This is likely to apply where a safeguarding concern is reported and parties within the church are required to interact with statutory authorities or take action to address safeguarding risks to children and people who may be vulnerable.
The Data Protection Bill currently going through parliament contains proposed amendments that would make specific legislative provision for the processing of personal data and special category data where it is necessary for the protection of children and adults at risk.
c) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
d) Vital interests: the processing is necessary to protect someone's life (generally life or death situations only).

e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests.

Where processing relates to special categories of personal data (see 5.1.1), the privacy notice must include the following:

- ***one of the six legal bases for processing personal data (above)***

- ***AND one of the conditions below***

The Data Protection Bill currently going through parliament contains proposed amendments that would make specific legislative provision for the processing of special category data where it is necessary for the protection of children and adults at risk.

a) Consent for one or more of the specified processes
b) Processing is required under obligations relating to employment, social security and social protection law
c) It is necessary to protect the vital interests of the data subject or another party where the party is incapable of giving consent
d) Processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition processing relates solely to the members or to parties who have regular contact with it in connection with its purposes. Personal data is not disclosed outside of that body without consent
e) Processing related to data which is made public by the subject
f) Processing is necessary in relation to legal claims or relating to court requirements
g) It is necessary in the public interest on the basis of a law which is proportionate to the aim pursued
h) Processing is necessary in relation to preventive or occupational health or provision of health and social care
i) It is necessary for public health such as safety of health care, cross-border threats to health etc.
j) Processing is necessary for archiving in the public interest (scientific or historic)

5.1.4 Subject Access Requests

Where an organisation holds data about an individual, under the GDPR, they have a right of access to that information. This can be obtained via a Subject Access Request. The person may apply via a Subject Access Request form available from the Trustees for Methodist Church Purposes website: www.tmcp.org.uk

This will be free of charge from May 2018. There is also a helpful guidance booklet, which can be provided along with the form. Any request relating to the access of information should be responded to promptly.

5.1.6 Retention of Safeguarding Information

The Independent Inquiry into Child Sexual Abuse (IICSA)

In March 2015, a government inquiry into child sexual abuse related to statutory and non statutory organisations was set up. The Chair of the inquiry wrote to church leaders outlining the authority held by the inquiry to request information from organisations under Section 21 of the

Inquiries Act 2005. The Chair confirmed that it was an offence to destroy, alter or tamper with evidence with the intention of suppressing evidence or preventing its disclosure to the inquiry. Consequently, the Chair directed that that information relevant to child sexual abuse in organisations should not be destroyed during the course of the inquiry. It has been confirmed that prolonged retention of records for this purpose will not be considered a breach of the current Data Protection Act. This is will also apply to GDPR.

Relevant safeguarding material will include the following documents:

- ***Safeguarding casework files and records***
- ***Safeguarding referrals for advice, inquiries and support to other organisations and internally***
- ***Risk assessments***
- ***Documents created in relation to Safeguarding Panels***
- ***Safeguarding Contracts***
- ***Quality assurance information e.g. safeguarding audits, data returns etc.***
- ***Files relating to education establishments, recruitment and safeguarding***
- ***HR Staff files***
- ***Complaints and discipline material***
- ***Files on appointments to councils, committees and other bodies***
- ***Files and papers relating to Subject Access Requests***
- ***Safeguarding leadership and governance at a church, circuit, district and connexional level***
- ***DBS checks***
- ***Any records held of safeguarding concerns about children and young people or about behaviour towards them***
- ***Policies and procedures relating to safeguarding children and young people***

Retention beyond the Independent Inquiry into Child Sexual Abuse (IICSA)

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. The subject of the concern 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 a range of 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***

5.1.7 Data Security & Breaches

Careful consideration should be given to data security when storing, using and sharing information. Methods used to secure data should be reviewed on a regular basis.

Further guidance is available at Section 7.3.2 Storing, Using and Sharing information Securely.
The General Data Protection Regulation identifies that a data breach is the unlawful or accidental

- ***destruction,***
- ***loss***
- ***alteration or***
- ***unauthorised disclosure***

of any personal data.

What sort of issues could cause a data breach of safeguarding data?

- ***A password on a computer becomes compromised and as a result a third party gets access to safeguarding records***
- ***An email including personal data is sent to the wrong person via the auto complete address feature in an email***
- ***A tablet or laptop is lost or stolen***
- ***A computer crashes, or a virus infects data and records are no longer accessible as they have become corrupted***

What action should be taken if a breach of data protection takes place?

- ***Establish the extent of the breach and the impact that is likely on others including emotional distress and physical/material damage.***
- ***Contact should be made with a line manager or person in oversight.***
- ***The Connexional Safeguarding Team should be advised where there is a significant breach in relation to safeguarding material.***
- ***Consideration should be made of what measures will be needed to contain and manage the situation e.g. taking specialist advice, reporting to Police (if appropriate).***
- ***Details of the nature of the breach and the action taken should be recorded in all circumstances.***
- ***If it is likely that the breach will result in a significant impact on the data subject, it will need to be reported to the Information Commissioner within 72 hours by the data controller. Where information is not fully available, limited details can be reported in the first instance.***
- ***Contact the data controller and data protection officer for further details and guidance as to what is required, including whether the subject of information should be informed.***

What type of data protection breaches must be reported to the Information Commissioner?

High risk situations are likely to require a report to the ICO. These are where there is the potential for people suffering significant detrimental effect such as discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage or where this has already happened.

7.3 ~~Information sharing guidance~~

Guidance for the management of safeguarding information

(change of section title only)

7.3.2 ~~Data protection guidance and principles for sharing of information~~

Information Sharing Guidance

~~Specific data protection guidance for safeguarding matters will need to be produced following work currently being done. For guidance on data protection matters please see the Trustees for Methodist Church Purposes. https://www.tmcp.org.uk/about/data-protection/~~

(other content in this section remains unchanged)

7.3.7 Required contents for privacy notices

The following information must be supplied in a privacy notice to an individual providing personal or special category data that relates to them:

- ***Identity and contact details for the data controller & the data protection officer (see 5.1.1.)***
- ***Purpose and legal basis for processing***
- ***The legitimate interest of the church in processing the information (where applicable)***
- ***Any recipients or categories of recipients of the data***
- ***Retention period or criteria to determine retention period***
- ***The existence of the subject's rights about data***
- ***The right to withdraw consent where applicable***
- ***The right to lodge a complaint with a supervisory authority***
- ***Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data***
- ***Any automated decision making process or profiling which may be used and its consequences***
- ***Any intended transfer of information to other countries and relevant safeguards which will apply***

Information that must be supplied in a privacy notice to a person about whom the church has received details from another party:

The items below should be supplied <u>in addition</u> to those listed above:

- ***The categories of information supplied to the church about that person***
- ***The source the personal data and whether this was from material accessible***

There is no need to supply information about whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data where information has already been supplied by a third party.