APPENDIX 4 – PROCEDURES FOR THE MANAGEMENT OF SAFEGUARDING INFORMATION

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:

General Data Protection Regulation (2018)

ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

Working Together to Safeguard Children (2018)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729914/Working_Together_to_Safeguard_Children-2018.pdf

Information Sharing for Practitioners (2018)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/721581/Information_sharing_advice_practitioners_safeguarding_services.pdf

Care and Support guidance issued under the Care Act 2014 *bit.ly/2bOUaho*

Adult Safeguarding: Sharing information – SCIE Jan 2015 *bit.ly/1cIHFBB*

Data Protection Act (2018)

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

1. The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) and Data Protection Act (2018) outline 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 and new Data Protection Act but the requirements for transparency have been increased, along with the sanctions for failing to comply. Everyone within the church should understand their responsibilities under GDPR and comply with its requirements.

The introduction of GDPR and the Data Protection Act (2018) provide 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 part of all safeguarding activity.

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

2. Key terms relating to data protection

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 so that they 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 relating to safeguarding. If the information is anonymous, it 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
- genetic data
- biometric identity data
- health information
- sex life
- sexual orientation

In most 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 Methodist Council. They will also be the relevant Controller for safeguarding and 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 to comply 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 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 needs to be retained. Retention schedules are available on the TMCP and Methodist Church websites confirming the length of time data should be held.

2.1 How must data be processed?

- fairly
- transparently
- for a specified, explicit and legitimate purpose
- adequate and limited to what is necessary
- accurately and 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:

- take 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
- provide privacy notices that clearly explain the lawful basis for processing and provide details of the data subject's rights
- ensure that data subjects have an opportunity to advise data processors of any inaccuracies and be proactive in making corrections within required timescales
- follow information provided in this Safeguarding Policy, Procedures and Guidance document about storage, retention and sharing of data, particularly with reference to security
- review practice to ensure that the retention of information is actively managed and time frames for retaining material are followed.

2.2 What are the rights of a data subject?

1. Right to be Informed

This is addressed by the provision of privacy notices (see 5.1.4) and information supplied by the Methodist Church from various sources.

2. Consent

Any consent must be true consent with 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, in which case consent is not needed.

3. 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).

4. Right of Redaction

Inaccurate or incomplete data should be corrected 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 corrected, a note should be retained to confirm that action has been taken, 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 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.

5. 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 continued 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 processing is in order to comply with statutory requirements or 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.

6. 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.

7. Right to Data Portability

This allows individuals to transfer their data from one organisation to another. Further advice should be taken from the data controller in relation to this right.

8. 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; or
- is required to establish, exercise or defend a legal claim; or
- conducting research for the performance of a public interest task.

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

9. Automated Decision Making or Profiling

This gives individuals the right to have a decision undertaken by a human, rather than an automated system. It is unlikely to relate to safeguarding within the Methodist Church.

3. 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 reporting a safeguarding concern, ongoing safeguarding case management and before 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. Sample privacy notices may be found on the Methodist Church website.

Children must also be provided with information about how their data is used in the same way as adults but it should 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 Appendix 4.

3.1 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, safeguarding concerns may be raised at times and in situations where to provide an immediate notice is impossible. 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. The person may be too distressed to receive this information and discuss the contents at the point of initial disclosure. In such circumstances, a church, circuit or DSO 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 anyone in this position to tell the person 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.

The privacy notice should have been supplied at the first point at which contact was made or before the data is disclosed to another party. 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. It will be helpful to make the point that the Methodist Church places great emphasis on ensuring that all parties are made aware of their rights and that details are provided as required by GDPR. The use of privacy notices will become familiar practice but may initially be unfamiliar and *cause* concern. Many people will be glad of this transparency, though 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. Under GDPR, the provision of a privacy notice is now mandatory.

Even where processing is being undertaken without consent for safeguarding purposes, the Data Protection Act 2018, Schedule 1, Part 2 (see 5.1.5), still requires a privacy notice to be supplied at an appropriate time.

4. The Lawful Bases for Processing Personal Data

The basis for processing personal and special category data must be included in a privacy notice. 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 may apply 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.

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 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:

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 subject or another person where they are incapable of giving consent.

d) It 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 that processing relates solely to the members or to people who have regular contact with it in connection with its aims. Personal data is not disclosed outside that body without consent.

e) Processing related to data which is made public by the subject.

f) It is necessary in relation to legal claims or court requirements.

g) It is necessary in the public interest on the basis of a law which is proportionate to the aim pursued.

h) It is necessary in relation to preventive or occupational health or the provision of health and social care.

i) It is necessary for public health, cross-border threats to health etc.

j) It is necessary for archiving in the public interest (scientific or historic).

5. Specific Provisions in the Data Protection Act 2018 relating to Safeguarding

While the General Data Protection Regulation provides for routine processing of data for church activities, the Data Protection Act 2018 makes specific provision for the release of information relevant to safeguarding situations.

1. The supply of information to investigations or inquiries conducted by statutory agencies such as police, adult or children's services.

In this case, the legitimate basis for processing is that it is in the substantive public interest for the prevention or detection of an unlawful act under the GDPR and Data Protection Act 2018,

Schedule 1, Part 2 (10). In all cases, a data protection form should be requested from the agency requesting the information which should be added to the safeguarding record. Concerns ***about*** the vulnerability of any party must be passed to the officer receiving information in writing.

2. Other safeguarding activities including recording information, making inquiries, risk assessment and the application of safeguarding measures.

The legitimate basis for these activities is that it is in the substantive public interest and necessary for the protection of someone of any age at risk from neglect, ***or*** physical or emotional harm, in accordance with the Data Protection Act 2018, Schedule 1, Part 2 (18). This includes specific individuals and groups ***[…]*** (e.g. children or adults at risk). If there is reasonable suspicion that the individuals need care and support,

are at risk from neglect, physical or emotional harm and unable to protect themselves, they are considered at risk for this legislation. Information can be shared without consent.

On occasion, concerns are raised that information sharing about safeguarding issues is a breach of the subject's human rights. Information Sharing for Practitioners (2018) provides the following guidance:

The provisions of the Human Rights Act and the common law duty of confidence must be balanced against the effect on children or individuals at risk, if information is not shared. Welfare of a vulnerable party is the most important thing and the need for disclosure should be assessed in every case on an ongoing basis.

It is possible that it is in the subject's overall interests, the public interest, or a legal obligation such as a court order may require disclosure. In the context of safeguarding a child or young person, where the child's welfare is paramount, it is possible that the common law duty of confidence can be overcome.

It can sometimes be helpful to share a copy of the government guidance to reassure those who may have concerns about the basis and legitimacy ***of*** information sharing.

6. 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, which ***is*** free of charge***.*** The person may apply to the data controller for a copy of the information held about them.

For routine data processing for all churches, circuits and districts, the Trustees for Methodist Church Purposes act as the Data Controller.

For data processing relating to safeguarding, complaints and discipline the Data Controller is the Methodist Church in Britain. Subject Access Requests relating to safeguarding, complaints and discipline should be sent to the Data Protection Officer at *dataprotection@methodistchurch.org.uk* or

Data Protection
Methodist Church House
25 Marylebone Road
London
NW1 5JR

All other subject access requests should be sent to:

Trustees for Methodist Church Purposes
Central Buildings
Oldham Street
Manchester
M1 MJQ

Further information is available from the TMCP website: *https://www.tmcp.org.uk*

7. Retention of Safeguarding Information

The Independent Inquiry into Child Sexual Abuse (IICSA)

In March 2015, a government inquiry into child sexual abuse ***in*** statutory and non-statutory organisations was set up. The Chair of the inquiry wrote to church leaders outlining its authority to request information 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 ***it*** 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. 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 includes the following documents:

- safeguarding casework files and records
- safeguarding referrals for advice, inquiries and support to other organisations and internally
- risk assessments
- documents relating 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
- records of safeguarding concerns about children and young people or about behaviour towards them
- policies and procedures relating to safeguarding children and young people

The following links contain documents that confirm this position: https://www.iicsa.org.uk/key-documents/78/view/letter-to-religious-leaders.pdf https://www.iicsa.org.uk/key-documents/115/view/2018-07-25-guidance-note-retentioninstructions-data-protection-requirements-version-2.pdf

Full Methodist Church retention schedules may be found here on the TMCP website.

8. Data storage

The following measures should be put in place if material containing special category or criminal data is retained:

- Access provision should be carefully planned

Only those that are required to see and use records should have access to them. A written protocol listing who has access should be drawn up with clear provision for emergency access. Data held on personally owned computers can be lost if unforeseen personal circumstances arise. This should never be the sole source of safeguarding records.

- Digital files should be subject to regular back-up.

If the data is stored on a stand-alone computer, the provisions for back-up should be away from this source to ensure that there is another copy if hardware is lost or corrupted beyond recovery. A secure server is the best option for back-up, where available but again access to safeguarding files should be limited to personnel listed in the access protocol.

- Pen drives or removable media must be encrypted if they are being used to store safeguarding records. However, the risks of loss of such items are higher than less mobile storage so great care should be taken in use.
- Software which identifies viruses, malware and phishing must be installed on systems storing safeguarding records. It must be regularly updated and the provision must include a regular scanning facility.
- Hard copy material must be stored in lockable cupboards or cabinets. Where available, these should be fire-proof.

- If material is scanned for digital retention, care should be taken to ensure that all parts of the document are contained in the scan, particularly the edges of documents. It is important to retain the integrity of the document; in case it is needed for proceedings at a later date.
- If plans are made for archiving safeguarding material with another institution, that organisation must be informed of the Methodist Church's requirements relating to retention of safeguarding records to ensure that records are not destroyed in error at a later date.
- Passwords must not include personal data which is easily identifiable e.g. a name, address, place or date of birth. Choosing three random words for a password can be easily remembered by visualisation of the items together and will create an appropriately secure password. This can be enhanced further by using a capital letter, number and symbol.

9. 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. Data relating to safeguarding cases should always be handled with the utmost care. It is likely to include the most sensitive forms of data and any breach of data security is likely to have a serious impact on the parties involved. Safeguarding officers within the Church are committed to building trust with those whom they deal by ensuring that data security measures are in place to protect information. This includes following guidance about the secure transmission of information and protecting data that is retained e.g. the storage of hard copy material in locked cupboards or cabinets. All parties holding safeguarding data electronically must ensure that their computers have virus, malware and anti-phishing software, which is regularly updated.

The General Data Protection Regulation identifies a data breach ***as*** the unlawful or accidental

- destruction
- loss
- alteration or
- unauthorised disclosure of any personal data.

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

- A password on a computer becomes compromised so 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.

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 a line manager or person in oversight.
- Advise the Connexional Safeguarding Team.
- Consider what measures will be needed to contain and manage the situation e.g. taking specialist advice, reporting to Police. Action should be taken as soon as possible.
- Record details of the nature of the breach and the action taken.
- If it is likely that the breach will result in a significant impact on the data subject, data controller to report it to the Information Commissioner within 72 hours. Where full information is not 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 the 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.

9.1 Step-by-step guide to sharing information

Taking into consideration the above documents and the guidance provided in section 7.3 *Information sharing guidance*, the following procedure should be adopted when receiving a request for personal data or making such a request.

i) **Validate the person requesting information**
Before supplying any information to a third party, check their identity and that they are in a role or position, which is entitled to make such a request and ***to*** receive the information. If you have prior personal or organisational knowledge of the person concerned you will not need additional validation. However, it can be tempting to be helpful and respond directly, particularly to calls which suggest they may come from a statutory agency or another church member***,*** or are said to need urgent action.

The following actions may be taken to validate the person requesting the information:

- requesting confirmation of the request via an organisational email
- calling the person back via a main switchboard number to ensure that the number is linked to that organisation
- speaking to a manager or other key individual who may be able to verify that person's role or involvement
- doing an internet search to identify information about an organisation or individual
- checking with someone else you know who might be able to verify the person's role and identity.

If making a request for information, offer to provide evidence of your validity to the holder of the information by any of the methods above***.***

ii) **Validate the nature of the request**

Think carefully about whether there is a legitimate reason to disclose the information that you are thinking of sending and only disclose what is relevant and proportionate in the circumstances, *which* could include:

- current risk to a child
- current risk to a vulnerable adult
- request to provide information in relation to a statutory investigation (Police, Children's Services or Adult Social Care etc.)
- court order
- subject access request under the General Data Protection Regulation.

If there is any doubt about whether there is a legitimate reason for providing information, ask the DSO. If you are making a request for information, say why you believe there is legitimate reason for the other party to disclose it, identify any risk posed by not doing so***,*** and say how ***it*** will be used***.*** If the third party is not aware of safeguarding processes in the Methodist Church, it is often helpful to explain the procedures.

iii) **Consider whether it is appropriate to gain consent**

People often feel concerned about asking or telling someone that information about them is going to be disclosed to another party, particularly when it may not give a positive impression. Be prepared to identify at

the outset information may be shared if there is believed to be a safeguarding risk. This often leads to greater acceptance***,*** as the person sharing the information is perceived as acting in an open and honest way.

Explain:

- why the information is being shared
- what will be shared
- how it will be shared
- with whom it will be shared.

It may not be appropriate to gain consent or make the person aware that information is being shared if it will:

- prejudice the prevention or detection of a crime
- risk the health or safety of a vulnerable adult or child.

Where consent for information sharing has been refused by an adult believed to be at risk of harm, consider the following questions:

1. Does the person have capacity to provide the consent?
2. Could they be under duress or in fear of harm if they consent?
3. Are children at risk through the adult's refusal of consent?

If lacking capacity to provide consent, under duress or in fear or where there are children at risk, it may be necessary to share information without consent.

iv) **Consider the most secure way to provide the information**

While no method of sending personal information is completely ***in***fallible, due regard should be given to the security ***of*** personal data.

If using standard mail:

- Use recorded delivery, registered delivery or a courier.
- Do not write "Private and confidential" on the outside of the envelope, as this may draw attention to the contents.
- Avoid window envelopes that may allow the contents or name to be viewed from the outside.
- Ensure that the envelope is addressed to an individual.
- Confirm that the address is current and appropriate.
- If it is a residential address and a multi-occupancy premises, confirm that the mail is delivered to a secure place such as an individual mailbox, rather than being left in an open hallway.

If using electronic mail, the following options may be used:

- an encryption system
- a password-protected attachment with the password sent via *separate means (i.e. not by a further email to the same email address)*
- an email with anonymous content with a key sent separately
- check that you have the correct and current email address. Ask the recipient ***to*** confirm receipt, and follow up if this is not received

v) **Make a record**

When sharing personal information, you should make a record of the following information:

- what was shared
- with whom
- when