THE TRUSTEES FOR METHODIST CHURCH PURPOSES

GUIDANCE NOTE

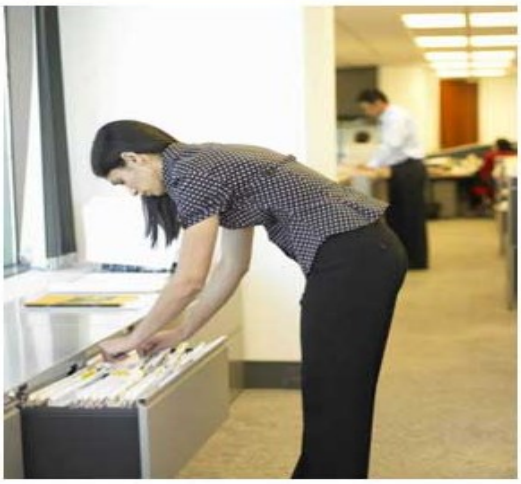
PLEASE NOTE*:* The information contained within this Guidance Note has not been updated since GDPR and the Data Protection Act 2018 became law. For guidance on the new requirements under GDPR and the Data Protection Act 2018, please see the GDPR Guidance Note:

(https://www.tmcp.org.uk/about/data-protection/resources/guidenotes/gdpr).

During the period that TMCP updates the Guidance Notes in relation to Subject Access Requests ('SAR') to reflect the changes introduced by GDPR and the Data Protection Act 2018, we still consider the information contained within this Guidance Note to be applicable. Whilst there are only subtle difference between this guidance and the new law, for your information, the main changes are in relation to Data Subject Access Requests and are:

- A Subject Access Request no longer needs to be made in writing and may be made verbally;
- Ordinarily, a fee can no longer be charged to provide the information and
- The statutory time period has been reduced from 40 days to 30 in which to respond to the SAR.

The Background of Data Protection



The first Data Protection Act was passed in 1984 and established the basic principles.

The current Act is the 1998 Data Protection Act, which complies with a European directive to facilitate the transfer of information within the European Union.

The main difference between the original and the current legislation is that manually held records are now included. The original Act only applied to data processed by automatic means (generally meaning by computerised methods).

Version 3 - April 2014

In 2012 TMCP became the Data Controller for connexional Methodist bodies, as well as for churches, circuits and districts. As a result of that, TMCP expanded the purposes for which all of the above bodies (as Data Processors) can hold data.

Below is a list of the purposes that are included in the TMCP Notification.

Details of the full and comprehensive list are available to view on the Register of Data Controllers' on the Information Commissioner's website. Simply type in TMCP's Registration Number **Z5439898**:

http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

WHAT DOES TMCP'S NOTIFICATION COVER? (1)

TMCP's Notification is designed to cover all the data you are likely to hold for example that a person is on the members roll, a church council member, a lay worker or that they covenant their giving.

However, the Data Protection policy is an ongoing review and therefore if you find that you hold information that is not covered by the Notification, then please let us know and we will endeavour to review our Notification accordingly. Not all of the Notification Purposes will apply to local churches. The Notification is intended to cover the work of local, circuit, district and connexional bodies, hence why pension administration is included for example.

Notification Purposes

1. Staff Administration
2. Administration of Membership Records
3. Fundraising
4. Realising the Objectives of a Charitable Organisation or Voluntary Body
5. Crime Prevention and Prosecution of Offenders
6. Assessment and Collection of Taxes and Other Revenue
7. Accounts and Records
8. Advertising, Marketing and Public Relations
9. Benefits, Grants and Loans Administration
10. Education
11. Legal Services
12. Pastoral Care
13. Pensions Administration
14. Processing For Not For Profit Organisations
15. Property Management

NEW EUROPEAN DATA PROTECTION REGULATION (2)

Proposals for a new European Data Protection Regulation was introduced by the European Commission in early 2012. The draft regulation was approved by the EU Parliament in March 2014 and is now due to go before the Council of Ministers (probably in June 2014).

The main objective of the new proposals is to modernise the current Data Protection laws across Europe and bring them into the digital era we now find ourselves in.

However, the UK's Information Commissioner believes that the new proposals are too onerous and prescriptive. If the new Regulation is implemented, the result will undoubtedly mean tougher penalties for non-compliance.

It is therefore important for data processors to ensure now that '**explicit**' consent is given by the data subject when data is collected and this would certainly include the collection of data by new appointments for inclusion in the church/circuit directory. Consent given implicitly, will be abolished if the new Regulation become law.

Principle 7 on page 10 deals with information security which also covers electronic devices in which data can be stored on or sent from. Procedures relating to this topic are likely to become more burdensome and arduous if the current proposals become law.

We will ensure that you receive any updates regarding the European Data Protection Regulations, via the website as soon as possible and the possible implications these may have on the church as a whole, but also as you as data processors.

WHAT IS PERSONAL DATA

(3)

1.1. The Data Protection Act 1998 defines *personal data* as:-

"Data which relates to a living individual and who can be identified:

From those data or

from those data and other information which is in possession of, or is likely to come into the possession of, the Data Controller.

This includes any expression of opinion about that individual and any indication of the intentions of the Data Controller or any other person in respect of the individual".

1.2. Data may also be classified as *Sensitive Personal Data* for which explicit written consent is required from the data subject to hold and process such data:

Race or ethnic origin

Religious or other beliefs of a similar nature

Physical or mental condition

Member of Trade Union

Political opinions

Sexual life

Commission or alleged commission of any offence

Proceedings of any offence committed or alleged to have been committed.

Please be aware that data relating to children belongs to the child and not the parents. In Scotland a child is deemed to have sufficient maturity from the age of 12, but no such clarification exists in England or Wales. **(See section 7 for further information – Rights of the Data Subject)**

If you are unsure of whether the data you are holding is classified as personal data for the purposes of the Act, a step by step guide is available from the Information Commissioner's Office:

http://www.ico.gov.uk/upload/documents/library/data_protection/dtailed_specialist_guides/160408_v1.0_determining_what_is_personal_data_-_quick_reference_guide.pdf

WHAT RECORDS ARE COVERED

(4)

This is Personal Data which is contained in records that are held either electronically or written manual records. Electronic records are easier to identify as it would cover any data that is held digitally. Some examples of these are:

- Computer
- DVD
- CCTV
- Microfiche

Think
Protect Personal Data

However, manual records are more complicated as the data must be held in a 'relevant filing system".

What is a 'Relevant Filing System'?

The Data Protection Act defines a 'Relevant Filing System' as:

"*Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.'*

In practice this means that the records have to be in a 'structured' order and therefore records relating to individuals are filed either alphabetically or by category.

The Information Commissioner suggests that a 'temp test' is applied to ascertain whether your manual records are held in a 'relevant filing system'. So would a temporary administrative assistant be able to extract specific information relating to a specific individual without prior knowledge of your type of work or the documents you hold?

If the information can be found quickly by the 'temp' then it will be considered that the records are held in a 'relevant filing system'.

However, if your records are not structured in such a way and it would involve sifting through all your records in order to obtain the data required, then it will not be considered that your records are held in a 'relevant filing system'.

With electronic data, you generally have the ability to do a computerised search. If it would take such a process to find data in your manual records, then generally it cannot said to be 'structured'.

DATA PROTECTION ACT 1998

THE EIGHT PRINCIPLES

(5)

The key to complying with the Data Protection Act is to follow and adhere to the 8 principles, which are laid down by Schedule 1 of the Act. The ethos of the Principles is to ensure that you do not hold any 'secret files' unless you are entitled to do so. Each of these principles puts obligations on the Data Controller to make conscious decisions on how personal information is collected, held and used.

(1) Data must be processed fairly and lawfully

This means that you must have legitimate grounds for collecting and using the data and must not use the data in ways that would have an unjustified adverse effect on the individual or for any illegal purposes.

It is good practice to have a 'Privacy Notice' which provides individuals with information as to why you are collecting their data and how you intend to use it, such as inclusion in the church or circuit directories. The Information Commissioner has provided a Code of Practice and more information on this can be found in Section 6.

You must always be open with the individual about the data you hold about them and how you obtained, use and retain the data. They must also be made aware of how to opt out of having their data processed.

(2) Personal Data shall be obtained for only one or more *specified* and *lawful* purpose

This principle again, reiterates the need for openness as you would not be complying with the Act if you processed data for any purpose which is not compatible for that in which it was obtained. In practice, if the purposes are different from the original purpose then consent of the individual should be sought.

For example, a church member provides their personal details for inclusion in the church directory. They then take up a post within the circuit meeting. It would not be appropriate for the individual's data to be automatically included in the circuit directory without their consent.

(3) Personal Data shall be adequate, relevant and not excessive

This principle is more commonly referred to as 'Information Standards' which means that the data should be:

- Adequate, relevant and not excessive;
- Accurate and kept up to date and
- Not kept for longer than absolutely necessary.

Where sensitive personal data is relevant, such with Minister's pastoral records, it is important that the data you hold regarding an individual is periodically checked to ensure of the accuracy of the data as the individual's circumstances may change regularly.

Opinions are also covered by this principle. Therefore the data record must contain information as to whose opinion it is, the circumstances it is based on and any evidence to support the outcome of the opinion. The Act does not give the individual the right to have the opinion changed or deleted simply because they do not agree with it, but they would have reasonable grounds to object if the opinion was based on inadequate or incorrect information.

You may be interested to know that the Information Commissioner receives complaints about 'inadequate' data processing regarding the quality of CCTV images. So, where a church has a CCTV system for security purposes and retains copies of the footage for a period of time, you would not be complying with this principle if you could not identify the individuals, as the purpose for installing the system cannot be fulfilled.

The Information Commission has published a Code of Practice regarding the usage of CCTV, which is available from their website.

(4) Personal Data shall be accurate and kept up to date

This has largely been dealt with in the section above. However, the law does recognise that it is not always practically possible to check all the personal data you hold and therefore you must take all reasonable steps to comply with this principle. Nevertheless, the more important the data, such as sensitive personal data, the more effort should be made to ensure its accuracy.

With regards to opinions, quite often one person's opinion on a situation can be very different to another person's opinion. If this situation occurs, you should mark the data appropriately to indicate whose opinions the data relates to and if appropriate, why that particular opinion has been formed.

It is also permissible, providing the individual is aware, to hold the data for statistical, historical or other research reasons. A prime example of this would be to hold data relating to the addresses of members in order to determine exactly where your church's congregation comes from and how it may have changed in recent years. Details of statistical data could be added to the church's Privacy Notice.

(5) Personal Data shall not be kept for longer than is necessary

The Act does not specify any minimum or maximum periods of time that data should be kept for. However, you should bear in mind that the longer you keep personal data the more likely it is to go out of date and become inaccurate. It is good practice to periodically review your files and delete any data that is no longer needed or relevant.

Church bodies may wish to think about a formal 'Retention Policy' for the various types of personal data they hold.

There is a clear link between the third, fourth and fifth principle, which means that if you hold personal data for longer than necessary then by definition the data will be excessive and may also be irrelevant and inaccurate.

There are times when you must keep some personal data, for providing references for example. It is quite possible that a former employee or volunteer may require a reference after their work has ceased with you. It would not be appropriate for you to still hold their emergency contact details after they leave, but a review of their position would be needed in order to provide the reference. How long this information should be kept for would be a matter for your Retention Policy.

Where a crime has been committed or reported to the police, all data should be preserved. It may no longer be relevant to you, but will be required by the investigating authorities. This will also apply to CCTV coverage, again demonstrating the requirement for accurate pictures. You will be told by the authorities when you can securely dispose of the data.

It is also possible that you hold personal data for more than one purpose, which is allowed if the individual is aware and consented. For example, one individual may have data held about them as they are a managing trustee (a member of the Church Council) and appear in the church directory, this data includes their date of birth. The church may also have a policy to send each of its members a birthday card. It would be appropriate to continue to hold that individual's data for the purposes of sending them a birthday card after they ceased to be a managing trustee of the church.

(6) Personal Data should be processed in accordance with individual rights

This section is self-explanatory but is dictated directly by the Act. The Act says that individual's rights are as follows:

a. A right to access their personal data
b. A right to object to the processing if it is or is likely to cause distress or damage
c. A right to prevent the processing for direct marketing
d. A right to object to decisions being taken by automated means
e. A right to, in certain circumstances, have inaccurate information:
    - Rectified
    - Blocked
    - Erased
    - Destroyed
f. A right to claim compensation for damages caused by a breach of the Act.

(7) Information Security

This Section is especially relevant for all Methodist Safeguarding Officers and should be read in conjunction with the Methodist Safeguarding Policy.

Technical and organisational measures should be taken to ensure that personal data is secure and cannot be lost, damaged, destroyed or processed unlawfully.

The level of your security depends on the nature of the data you are holding. For example, sensitive personal data, which could include your pastoral records, should have a higher level of security than the members roll and should be encrypted when being stored or sent electronically. The Information Commissioner is clear that serious breaches will result in a substantial fine.

The term "electronic devices" applies to laptops, notebooks, tablets, mobile phones, USB memory sticks, CD's and DVD's as well as your office/personal PC. Any of these devices may be your own personal equipment and therefore your data protection policy should be clear as to what data may be processed on these and that which may not.

Appropriate security measures should ensure that only authorised people can access, change, disclose or destroy data and that they are not able to act beyond the scope of their authority. You should also consider registering the devices with a remote "locate & wipe" facility to ensure confidentiality in the event of the device being stolen.

In November 2013, the information Commissioner prompted organisations to ensure that adequate training is given to temporary staff who regularly handle personal data as part of their duties.

(7) cont…..

You should also consider the security of your premises, who has access to those premises and the number of staff with access to the personal data, which will include paper files as well as computerised files.

For the larger organisations, it may be appropriate for you to consider a 'Breach-Management Plan'. The Information Commissioner recommends that the Plan should contain four basic elements:

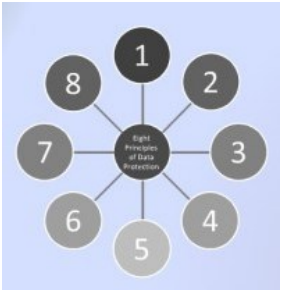
1. Containment and recovery.
2. Assessing the risks – are there any potential adverse consequences for Individuals.
3. Notification of breaches – this would concern the individuals, TMCP and the Information Commissioner. However, we suggest you contact TMCP in the first instance to discuss the severity of the breach and the next course of action.
4. Evaluation and response – an investigation as to the cause of the breach and the effectiveness of your response, both to the individual and the organisation.

(8) Sending Personal Data outside the European Economic Area

The Act specifically states that 'Personal data should not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data'.

You should be aware that the Channel Islands and the Isle of Man are not in the EEA. However, the Information Commission has published a list of all countries within the EEA or that have an adequate level of protection. The European Commission has ruled that Jersey, Guernsey and the Isle of Man do have adequate levels of protection.

You should always remember that documents such as the Church or Circuit Directories that are published on the internet can be accessed by anyone.



PRIVACY NOTICES (6)

A Privacy Notice is a statement which makes individuals aware of how their data is held and what it will be used for. It is best practice to have a Privacy Notice regardless of how little data you actually collect and process.

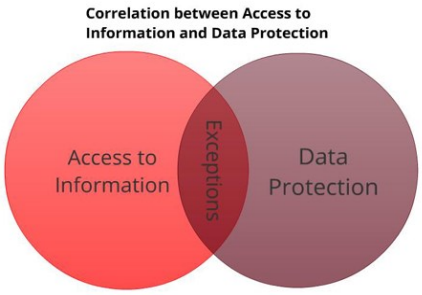
Your Privacy Notice should contain the following key elements:

- identify who will collect and process the data,
- confirm the purpose or purposes for which the data is processed,
- confirm who will have access to the data,
- how long the data will be kept for, and
- what you are doing to ensure the security of the data (see Principle 7)

On a basic level, but one which all churches will identify with, is the collection of personal information for inclusion in the church's Directory. The Privacy Notice should confirm that the data is collected and processed by an appropriate officer of the church council; the information will be used for inclusion in the church's Directory and if appropriate, will be circulated to all members of the church. It should also state other potential recipients of the Directory, such as the Circuit Meeting and whether or not it will be freely available to members of the public. This would certainly be the case if the Directory was to be published on the church's or circuit's website.

The Privacy Notice should be clear as to why the personal data is being collected. It should also try to indicate other instances of when the information will be used. This could be something as simple as sending a birthday card each year or where key holders details are released to other users of the church in emergencies.

Currently, and with the exception of sensitive personal data, it is sufficient to inform individuals of the contents of the Privacy Notice and as such how individual's data will be held and processed. However, you will note from section 2 of this booklet that should the new European Data Protection Regulations come in to force then consent given implicitly will be abolished. It is therefore good practice to start NOW obtaining explicit written consent from the data subjects when collecting their data.



RIGHTS OF THE DATA SUBJECT

(7)

With a limited number of exceptions, Data Subjects have the right under section 7 of the Data Protection Act 1998 to be given details of any data that is processed and held specifically about them. This relates to:

- Electronic records, for example:
  - Emails
  - Database entries
- Manual records that are held in *'relevant filing system'*
  See section 4 for further information.

They have the right to be provided with a description of the data being held, the purposes for which the data is being processed, the source of the information and who the likely recipients of the data are.

The Data Subject is under no obligation to inform you as to why they are making the data access request.

Further information is detailed in section 5 relating to the 'Eight Principles' but as a general rule, the Data Subject has a right to ensure that:

1. their personal data is correct,
2. their personal data is relevant,
3. their personal data is processed fairly,
4. their personal data is not excessive,
5. their personal data is not kept longer than necessary.

Data Belonging to Children

As previously stated in section 3 Data which relates to children belongs to that child and not the parent or carer. In judging whether such data should be disclosed to anyone other than the child, you should have regards to the following:

1. What is the nature of the data? – routine or sensitive
2. What is the child's own view?
3. Are there any court orders in place?
4. Do you have a duty of confidence?
5. Are there any adverse effects to the child if the data is disclosed?
6. Is there any detriment to the child if the data is NOT disclosed?

WHAT YOU SHOULD DO IF YOU RECEIVE A DATA SUBJECT ACCESS REQUEST

(8)

A Data Subject has a right under section 7 of the Data Protection Act 1998 to request access to data held about them. For this to be enforceable the request must satisfy the following requirements:

1. Be in writing. An email is sufficient and consideration must be given to disability issues.
2. Must be from the Data Subject themselves or from a legal Agent, such as someone holding a Lasting Power of Attorney. Evidence of this must be provided.
3. Provide proof of ID, if the Data Subject is not well known to you.
4. Provide adequate information to allow you to locate the data they are requesting.
5. Provide a set fee of £10.

TMCP has a form, which is available to download from the Website or from the TMCP office. This form should be used where possible as it is designed to enable the Data Subject to provide all the relevant details that will be required in order to process their request efficiently and on time.

Once a request for data has been received, the Data Subject must receive a response within 40 calendar days.

A copy of this must be forwarded to TMCP as Data Controller. However, as Data Processor, it is you who holds the information and who must provide the data requested by the Data Subject.

Failure to comply with a Data Subject Access Request may result in the following actions:

- An Enforcement Notice being issued by the Information Commission (failure to comply with this is a criminal offence)
- A Monetary Penalty of up to £500,000
- Legal Action being taken by the Data Subject

Please note the indemnity which is authorised by Standing Order 019(4) to TMCP, as Data Controller. In the event of non-compliance by the Data Processors and a claim being made, the Data Processors may be personally liable to meet any claim or face any consequential criminal proceedings.

A copy of this is located in Appendix 1.

WHAT IF THE RECORD CONTAINS DATA RELATING TO ANOTHER INDIVIDUAL?

(9)

It has already been stated that a Data Subject has a right to access data that directly relates to them. They are not automatically entitled to data that relates to another living individual.

However, what do you do if you receive a Data Subject Access Request which involves data relating to another individual? Clearly there is a conflict between a right of access on the one hand and a right to privacy on the other.

Under such circumstances, you only have to disclose the data to the Data Subject if:

1. You have the consent of the third party; or
2. It is *reasonable in ALL the circumstances* to comply with the request without the consent of the third party.

There is no problem if point 1 above is satisfied and you have the consent of the third party, but point two can be more problematic.

You must consider whether the third party is identifiable from the data. In some cases, removing their name or job title will provide them with anonymity thus protecting their privacy. However, in a lot of instances this will not be the case as it will be obvious to the Data Subject who the third party is, even with their name removed.

There may be situations where it is not possible to get the third parties consent, it is too costly to try and obtain their consent or they have outright refused to give consent. Here you must decide whether it is 'reasonable in all the circumstances' to disclose the data without the consent of the third party. Factors that should be considered are:

- Is there a duty of confidentiality to the third party,
- What steps have you taken to *try* and obtain their consent (retain a record of action).
- Is the third party capable of giving consent;
- If consent has been refused, is this reasonable?

Finally, you must take into consideration the possible effects that disclosure will have on a third party. Even where you have gone to great lengths, but unsuccessfully, to obtain the third party consent, you must refuse to disclose the data if this would cause adverse stress to the third party.

However, rude or embarrassing opinions will not satisfy this rule. The effect of disclosure must be detrimental to the third party.

WHEN TO REFUSE A DATA SUBJECT ACCESS REQUEST

(10)

This is probably the hardest issue within Data Protection and that is to recognise when you can or should withhold an individual's data.

The Data Protection Act does provide certain exceptions to when a Data Subject Access Request can be refused. Briefly, the main ones are:

1. National Security, Prevention or Detection of Crime or Apprehension or Prosecution of Offenders:

   Any pastoral records relating to known offenders for example, should not be disclosed to the Data Subject if you know or suspect that the individual has recommitted a crime which is being investigated by the police.

   Certain safeguarding issues may also fall under this exemption, especially when dealing with the vulnerable. If other governmental departments, such as Social Services, are involved with the Data Subject, then any Subject Access Request should refused until you are satisfied that there is no investigation being undertaken by that department and that disclosure will have no detrimental effect on the Data Subjects themselves or others.

   For example, could the release of an individual's personal data compromise the privacy or safety of a care worker?

2. Negotiations with the Data Subject:

   You may have a complaint or employment issue which is being carefully negotiated. You do not have to provide records relating to these negotiations until such time as an agreement has been reached. The exemption will not apply once an agreement has been reached.

3. Management Forecasting or Management Planning:

   An example of organisational restructure could fall into this category where redundancies are possible. It would not be appropriate to disclose an individual's data without compromising the procedure.

4. Confidential References:

   This only relates to references given by the Data Controller (in this case TMCP) and not by other organisations. However, it should be born in mind that TMCP is the Data Controller for the purposes of Notification and it is you as Data Processors who have control of the individual's data, and may find a case is raised with the Information Commission to compel the release of such references provided by you.

5. Legal Advice & Proceedings

This includes:-

1. Data relating to actual or prospective legal proceedings
2. Obtaining legal advice
3. Establishing, exercising or defending your legal rights

6. Data containing information relating to other individuals:

See section 9

Always remember, that there are other circumstances when data does not have to be released, such as the data being held in manual form which does not form part of a 'relevant filing system' and where the data record does not specifically relate to them. For example, an email between colleagues will not become personal data to another individual merely because they are named in that email.

INFORMATION FOR DATA SUBJECTS

(11)

Please read these notes before completing the Request for Personal Data Form at the back of this booklet.

Under the Data Protection Act 1998, you have a right to know what information is being held about you . However, you only have a right to your own data and therefore some records may not be disclosed to you because they contain data relating to other individuals. There may be other reasons why the records cannot be disclosed and further information on this issue is provided in section 8.

In order to assist the Methodist Church to comply with your request for data as efficiently as possible, you should consider the following points:-

1. Please complete the Request for Personal Data Form at the back of this booklet as thoroughly as possible. Your data may be held in more than one location and therefore in order to locate this data, we would require details of exactly what the data is and who is likely to be holding it. The Methodist Church is a large organisation and therefore the more information you provide us, the quicker and more efficiently we can respond to your request.

   It is not reasonable for you to request "all data held by the Methodist Church" relating to you. You must help us locate the precise data you are requesting.

2. The Data Protection Act covers both manual and electronic records which are held in a "relevant filing system". The definition of this is discussed in greater detail in section 4. However, you should bear in mind that the data must be filed in a structured way such as alphabetically or by category.

   Under the Act, Data Processors are not required to undertake a search of all records on the off-chance that they contain data about you. This is why it is vital that you provide as much detail as possible to help us identify the location of your data.

3. If you do not provide sufficient information to assist the Data Processor locate your data, then you will be informed as quickly as possible. However, please be aware that the statutory time period of 40 days will not include the days it takes to obtain sufficient information from you. If any further delay to your request for data is likely to be encountered, you will be informed of this as soon as possible which will provide an explanation of why and when you are likely to receive a response.

4. Other delays to your request for data will be because we have not received a £10 administrative fee or proof of identification from you. The 40 day statutory period will not include the days in which it takes to obtain these.

   Please ensure that one form of ID has an up to date photograph of yourself, such as a driving licence or passport. The other form of ID should display your current address, such as a utility bill.

Data Protection is an issue TMCP on behalf of the Methodist Church takes seriously and endeavours to protect the rights of individuals at all times. Please contact us if you have any concerns or wish to discuss a particular issue in more detail.

The Trustees for Methodist Church Purposes
Central Buildings
Oldham Street
Manchester
M1 1JQ

Tel No 0161 235 6770

Methodist Church House
25 Marylebone Road
London
NW1 5JR

Tel No: 0207 486 5502

FREQUENTLY ASKED QUESTIONS (12)

1. **How do I know if I am a Data Processor?**

   If you obtain, manage, store and use data relating to an identifiable living individual on behalf of a local church, district, circuit etc. then you will be considered to be a Data Processor.

   In the event of a Data Subject Access Request being received, and the Data Subject has identified your church body as being likely to be holding data, we will contact the officers responsible for that body asking that you respond directly to the Data Subject within the time limits (40 calendar days) imposed by the Act.

2. **Are all manual files covered by the Act?**

   No, but if the data refers to an identifiable *living* individual and can *easily* be accessed by others, for example through a card index filing system, then the Act will apply.

3. **Can I refuse the Data Subject access to a reference if it mentions a third party?**

   No, you are required by law to provide as much information as possible. The identity of a third party should never be released without their consent. If the third party can be anonymised by removing their name and details then the data must be released.

4. **Is it OK to hold the contact details of people who are not members but use the church facilities?**

   Yes, but you should obtain the consent of these people first. Explain why you require the information, where it will be kept and exactly who will have access to it.

   Information relating to children should be kept secure with as few people as possible having access to this information.

5. **When do I need the consent of the Data Subject to process their data?**

   As from the 24th October 2001 the data Subject should be informed as to what information is held about them and for what purposes. Consent should be obtained as soon as the data is obtained, and this would include collecting data for the purpose of church or circuit directories. The Data Subject must be given the opportunity to withdraw this consent at any time.

   You could use a statement on the Data Collection sheet, which could be as follows:

   'The information you have provided will be held in accordance with our Privacy Notice. You must notify us in writing if you do not wish your data to be continued to be held by us'.

(12) cont..

6. **Some files contain allegations of improper conduct. Do I need to disclose these?**

In extreme cases information may be withheld if it can be shown that disclosure of the data would prejudice the prevention or detection of crime. This would also be the case in certain safeguarding issues where other organisations, such as social services, were involved.

Please contact TMCP for further guidance if this event should arise as soon as possible.

7. **Does the Data Protection Act prevent parents from taking photos at church events?**

No, providing the photographs are taken purely for personal use. Family and friends are permitted to take photographs and film such events providing they are for the 'family album' only. Please be aware however, that the use of internet based Social Media, such as Facebook, is not considered to be a personal "family album".

The Act would apply where the photographs are taken by church officials for publication, such as a newsletter or fundraising material. Under these circumstances, permission should be sought from the data subjects and/or their parents where appropriate.

8. **We are a shared Church. Are we covered under TMCP's Notification?**

Where there is a Methodist Council in existence then you will be covered by TMCP's Notification with the Information Commissioner.

9. **Do I need to mention the Data Protection Act when obtaining personal data from individuals?**

Yes. The person concerned should always be aware that the information provided will be stored as part of a relevant filing system and become part of their data entry.

APPENDIX 1

(13)

Standing Order 019 deals specifically with Data Protection and the requirements of the Managing Trustees to comply with the Data Protection Acts:

(1) All connexional, district, circuit, local *and other Methodist* bodies*, and all societies, institutions and other organizations subsidiary or ancillary to the Methodist Church* shall comply with the Data Protection Acts for the time being in force and with any regulations or orders made or having effect under *such legislation*.

(2) In particular, every such body shall be registered*, where required to do so,* with the relevant Commissioner *or other authority*, as specified in clause (3) below.

(3) *In England and Wales, and in Scotland, a*ny such body may be registered separately by giving the required notification directly to the *relevant authority (the Information Commissioner's Office)* and shall do so if the *notification* by the Trustees for Methodist Church Purposes ('the Board') is not sufficiently comprehensive for its purposes. Every such body which is thus registered directly with the Commissioner shall notify the Board in writing of that fact. Every such body which has not so notified the Board will be registered under the Board's *notification*.

In other jurisdictions, any such body must register separately with the appropriate authority as required by the relevant legislation.

Further detail about the applicability of the Data Protection legislation is provided in a booklet available from the Trustees for Methodist Church Purposes.

(4) The Synod, Circuit Meeting, Church Council or other responsible authority of each body registered under the Board's notification shall indemnify the Board, as Data Controller, against the consequences of any breach of the Data Protection legislation, regulations or orders committed by any officer (ministerial or lay), meeting or committee of that body or by any other person or persons holding data relating to its affairs.

CHECKLIST FOR DATA PROCESSORS FOLLOWING A DATA SUBJECT ACCESS REQUEST (14)

When a Data 'Subject Access Request' ('SAR') is received, time is of the essence in order to reply within the statutory time limit of 40 days. In order to assist you, please refer to the following checklist:

- ☐ Has the SAR been received in writing or by email?
- ☐ Are you happy with the Data Subject's identity?
- ☐ Has the Data Subject provided sufficient information for you to identify the data requested?
- ☐ Has the £10 fee been received? (You may have to check with TMCP to see if it has been forwarded directly).
- ☐ Make a note of the date. If the above points have been complied with, you now have 40 calendar days to respond.
- ☐ Acknowledge receipt of the SAR and indicate when a response is likely to be given. Are there any reasons for a delay to the response?
- ☐ Notify TMCP and other Data Processors likely to be holding data immediately.
- ☐ Is the data held in a 'relevant filing system'?
- ☐ Does the data contain information relating to other individuals? See section 7
- ☐ Is there any reason why their data should not be disclosed? See section 8
- ☐ Is the data legible?
- ☐ Can you respond within the 40 day statutory time limit?

If you are unable to positively tick off all the above questions, then please talk to us at TMCP to seek advice.

REQUEST FOR PERSONAL DATA UNDER THE DATA PROTECTION ACT 1998

(15)

Please complete sections 1-4 of this form to help us identify all the relevant personal data to which you wish to gain access.

There is a £10 fee applicable to your request to cover administrative costs. Cheques should be made payable to the 'Trustees for Methodist Church Purposes' and be returned with this form.

SECTION 1

Your personal details:

SURNAME: _____

FIRST NAMES: _____

FORMER SURNAME: _____

ADDRESS: _____

_____

_____

POSTCODE: _____

TELEPHONE No: _____

MOBILE No: _____

Please give us details of your previous address if you have not resided at your current address for two years or more:

ADDRESS: _____

_____

_____

POSTCODE: _____

(15) cont….

SECTION 2

Details of Data

Please describe in as much detail as possible, the information you are requesting and all the church bodies you think may be holding your data, together with offices you held in those bodies and other reasons why you think data is being held.

Please use a separate sheet if necessary:

SECTION 3

Additional Information Required

It is vitally important to us that your personal data is protected and held in accordance with the Data Protection Act 1998. To ensure we disclose the information requested to you only please provide two proofs of identity (one of which must contain a photograph of yourself):

1. _____
2. _____

(Copies will be accepted, but we do reserve the right to request sight of the originals)

SECTION 4

Declaration of Data Subject

I confirm that I am seeking access to personal information about myself.

Signed: _____

Date: _____

Please return the form to:

Data Protection Officer
The Trustees for Methodist Church Purposes
Central Buildings
Oldham Street
MANCHESTER
M1 1JQ

□ £10 fee enclosed
□ 2 forms of ID enclosed

For Official Use Only

Date Form Received:	
40 Calendar Days Expires:	
ID Received:	
Fee Attached:	
Request Referred To:	
Date:	
Response to Data Subject Sent:	

DISCLAIMER:-

Whilst every effort is made to ensure the accuracy of this information, the Trustees for Methodist Church Purposes do not represent, warrant, undertake or guarantee that the information in this publication will lead to any particular outcome or result, or to the completeness, reliability and accuracy of the information set out.

The Trustees for Methodist Church Purposes reserves the right to revise this publication and to make changes to it from time to time without obligation to notify any person or organisation of such revision or change.

All the information in this publication is produced in good faith and for general information purposes only. The information is not legal advice and should not be treated as such.

Further information is available from :-

Information Commissioner, Wycliffe House, Water Lane,
Wilmslow, Cheshire SK9 5AF - Tel No: 0303 123 1113 (local rate)