Guideline Leaflet L13: Data Protection

If a church processes any personal data, for example on a computer, in a paper-based filing system or in cloud-based storage, it must follow the rules set out in the Data Protection Act 2018 and the UK GDPR. This leaflet explains what this means for churches. It should however only be taken as general guidance and should not be used as a substitute for obtaining legal advice.

At the end of the leaflet we have provided a checklist for churches to work through.

If churches have questions that fall outside the scope of this leaflet then we would advise that you contact the Information Commissioner's Office for their advice. (Details are on page 3)

Please note, specific arrangements apply to the retention of safeguarding records. A BUGB Safeguarding Record Keeping Guide is available at www.baptist.org.uk/gdprsafeguarding. In the light of the ongoing Independent Inquiry into Child Sexual Abuse, Baptist churches must not destroy safeguarding records, as they may be relevant to the Inquiry.

This Guideline Leaflet is regularly reviewed and updated. To ensure that you are using the most up to date version, please download the leaflet from the BUGB website at www.baptist.org.uk/resources

The date on which the leaflet was last updated can be found on the download page.

L13: Data Protection

These notes are offered as guidelines by the Legal and Operations Team to provide information for Baptist churches.

The legal services undertaken by the Legal & Operations Team of the Baptist Union of Great Britain are carried out and/or supervised by a Solicitor who is authorised and regulated by the Solicitors Regulation Authority. Regulatory Information is available here:

L17 Legal and Operations Team – Regulatory Information

These notes can never be a substitute for detailed professional advice if there are serious and specific problems, but we hope you will find them helpful.

If you want to ask questions about the leaflets and one of the Baptist Trust Companies are your property trustees, you should contact them. They will do their best to help.

If your church property is in the name of private individuals who act as trustees they may also be able to help.

INTRODUCTION AND CONTENTS

The subject of Data Protection is one which churches cannot afford to ignore. It can however be quite complicated, and this is a lengthy Guideline Leaflet. We have therefore sought to highlight at various points the major principles which churches need to be aware of and also include what we hope are relevant examples. **Please ensure that at least one person on your leadership team reads the entire leaflet.**

Please also see www.baptist.org.uk/gdpr

Further information and advice about compliance with the Data Protection Act 2018 and the UK GDPR can be obtained from: Information Commissioner's Office, Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF

The ICO provides a free telephone helpline: 0303 123 1113 (Monday to Friday 9-5) as well as a live-chat facility via their website. For more information about contacting the ICO please see https://ico.org.uk/global/contact-us

In November 2017 the ICO launched a new telephone service dedicated to small organisations and charities – to find out more see https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/

You can also sign up to receive a monthly newsletter by email which contains the latest developments in Data Protection here: https://ico.org.uk/about-the-ico/news-and-events/e-newsletter/

SECTION 1: DATA PROTECTION LEGISLATION

The need for legislation covering Data Protection arose because of the growing use of computers which can store a vast amount of personal information about individuals. Without safeguards these personal details could easily be accessed by individuals and other organisations.

The Data Protection Act 1998 was introduced to protect individuals against the unfair use of their personal information. The 1998 Act was replaced by the 2018 Data Protection Act (DPA) which incorporated the European General Data Protection Regulation (GDPR). When the UK left the European Union the GDPR remained part of UK Data Protection legislation in the form of the Retained General Data Protection Regulation (UK GDPR) but the UK government now has the independence to keep the data protection framework under review. There are a number of fundamental principles (the Data Protection Principles) which the original DPA established which are based upon the rights of the individual to respect for their private and family life, free from interference by the State (in turn based upon Article 8 of the European Convention on Human Rights). The principles are also incorporated in the 2018 Act.

These principles are based upon the right of an individual to know what data is being held about them and to check its accuracy; and the concept that someone's personal information should be used only for the specific purposes for which it is expressly held by an organisation and not disclosed to those who are not authorised to hold it.

If a church processes any *personal data* it must follow the rules set out in the DPA. Failure to do so could result in enforcement action being taken, by the regulator, the Information Commissioner's Office (ICO), against the church in question or against the trustees if the church is unincorporated.

There are serious implications for breaching Data Protection legislation which we have outlined below. Whilst the type of personal information held by most churches is unlikely to result in a serious data breach you do need to be aware of the possible consequences.

- The ICO has a range of enforcement tools at its disposal including the imposition of a financial penalty (a 'monetary penalty notice'). Under UK GDPR this could be up to the equivalent of £17.5 million for the most serious breaches.
- The ICO can alternatively issue an Enforcement Notice requiring an organisation to stop handling (or 'processing') personal data which would have serious implications for a church which depends on handling the personal data of a wide variety of different individuals, from the trustees to the members and volunteers.
- Where the ICO takes official enforcement action, this is always publicised on their website, which can lead to serious reputational damage for a church.
- The ICO has said on many occasions that the rules under data protection law (both under the DPA and the UK GDPR) apply in the same way to charities as they do to commercial entities.
- In addition, there are currently a number of criminal offences for which individuals working in a paid or unpaid capacity could receive convictions, in certain circumstances, where they recklessly (or intentionally) mishandle personal information.

SECTION 2: THE TECHNICAL TERMS (Definitions and Examples)

2.1 Personal data **means information relating to a living individual who can be identified from that data (or from that data plus other information in your possession). Personal information can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal) or a statement of intention about them. From 2018 this also included 'online identifiers' such as computer IP addresses.**

The definition of **personal data** in data protection law includes two types of personal information about living individuals. This can be information held in electronic format or certain kinds of paper records or manual filing system.

Personal data held in electronic records includes information about a living individual contained on or sent via a desktop/laptop/tablet computer e.g. within a file/folder or an email; portable hard drive, CD, DVD, USB stick; cloud storage; mobile phone e.g. text message, file or folder, voicemail; landline phone e.g. voicemail or fax machine.

Personal data in electronic format also includes images of living individuals (provided that the image is clear enough for particular individuals to be identified). Therefore, digital photos held on mobile phones and on any computer, laptop/tablet or in the cloud, will be personal data of the individuals concerned, as will moving images/video footage of living individuals held on mobile phones, digital video cameras, CCTV recording equipment or elsewhere.

Your church is responsible for ensuring that all such information held by, or processed by, church staff and volunteers on church-owned equipment or personal equipment used in connection with the individual's role within the church is done so in a way which complies with Data Protection legislation.

> In addition to the usual data held by churches - such as names and contact details of church members, parents of children and young people attending church activities etc. – churches with websites need to be aware of data they are collecting through the site.
>
> If a church provides a 'contact us' form on its website to allow members of the public to make an enquiry then all the information supplied by them is the personal data of the enquirer and will need to be held by the church in accordance with data protection legislation.
>
> If a church uses cookies on its website to monitor any browsing activity by a visitor to its website, the church will be collecting personal data of that individual.

Personal data held within structured manual filing systems: Under data protection law, where personal information about living individuals is held within a 'relevant filing system,' this kind of data will be subject to data protection rules e.g. where a church holds personal data about any of its data subjects in a filing cabinet in alphabetical (or any other kind of) order so that it is easy to locate the information about any particular individual fairly easily. This could include card index systems with names of contractors which the church uses or a filing cabinet of paper files containing personal details relating to church members and attendees for example.

2.2 Data subject refers to the living individual whose personal data you hold. In a typical church situation this would include trustees, ministers, church members, members of the congregation, children in the Sunday School or Youth Group, and those attending Alpha courses etc. whose names and personal details are recorded.

However, the definition also extends to all those living individuals whose personal information is held – even if this is only a name and email address or name and phone number. Therefore, complainants and casual enquirers who have no previous relationship with the church would be included within the definition if the church holds their name and any other details about them, as would those whose contact details are held because they relate to an individual who provides a service to the church (such as an electrician, for example).

2.3 Special Category Data is personal data which the UK GDPR says is more sensitive and so needs more protection. This was previously known as 'Sensitive Personal Data' and is information concerning the data subject's race or ethnic origin, politics, religion, trade union membership, health, sex life or sexual orientation. *In addition, genetic data and biometric data (e.g. fingerprint data or data obtained through facial-recognition technology) now also fall into this category although it is highly unlikely that churches will hold any such data!*

Much of the information which churches are likely to process will be sensitive personal data as it is likely to concern the data subject's religious beliefs. Information relating to the physical or mental health of church members, employees, volunteers and other individuals may also be held by a church.

2.4 Criminal Offence Data is personal data relating to criminal convictions and offences. Under the UK GDPR this is a separate category of data. Churches may, for example, be told about convictions which relate to the safeguarding of children and adults at risk, including the preparation of a Safeguarding Contract with a church member.

2.5 Data Processing refers to the operations carried out on personal data. The usual processing operations are: Collecting - Editing - Storing/holding - Disclosing - Sharing - Archiving - Viewing (e.g. personal data on an electronic device or in paper records) - Recording - Listening to (e.g. a voicemail message left

by a church member) - Erasing/deleting. During the 'life cycle' of personal data, several different processing operations can be carried out in relation to that data – from its initial collection to its eventual erasure and removal from church electronic or paper records.

If the church – or people working for the church in a paid or unpaid capacity - holds personal information electronically or in organised paper records, you will be processing it.

In a typical church situation, there could be several individuals who process personal data on behalf of the church. This may include:

- Minister – processing members' personal data for pastoral reasons
- Church treasurer – holding bank details of individuals to whom expenses are paid
- Church administrator – maintaining the church's contact list or Directory
- Youth Club leader – holding emergency contact details of parents
- Safeguarding administrator – holding references and other information about those who are working with children and adults at risk in the church.

Please note that this list is not exhaustive!

A volunteer within the church agrees to collate the contact information provided by parents of children attending a Holiday Club. Whether this information is stored electronically or held in paper form in a folder you are processing personal information.

A member of the public signs up via your website to receive information about the local Foodbank. Their contact details are sent directly to the Foodbank who contact them about volunteering opportunities. Even though the church is only passing the details on to the Foodbank, this activity will mean that it is 'processing' the personal data of the member of the public, even if only for a very short period of time.

A church member takes photographs at a church-organised event and emails them to the Minister and Church Secretary in case they want to use them as publicity for a future event. If these photographs contain recognisable images of people then you are processing personal information.

Where individuals are processing personal data for church purposes and in accordance with their paid or unpaid role within the church they will be processing in their role as 'staff' of the church as a 'data controller' (church) i.e. the processing will be deemed to be by the data controller. (See next section for the definition of 'data controller')

2.6 Data controller refers to the person (i.e. legal person) who determines the purpose and the manner by which personal data is to be processed. This is the name of the legal entity which holds the personal data. **In the case of an unincorporated Baptist church, the data controller will be the charity trustees* (usually the minister, deacons and elders or Leadership Team).** In the case of churches which are registered with the Charity Commission as either Charitable Incorporated Organisations (CIOs), or as Companies Limited by Guarantee (CLG) - then **the data controller will be the CIO or the CLG.**

It is important to note that the definition of data controller also includes all staff and volunteers who work for the church. Therefore, when staff and volunteers process personal data **in their role within the church** they will be processing as the data controller entity.

It is important that such staff (including volunteers) have been adequately trained in data protection and are processing the data in accordance with their duties. If they act outside of the remit of their roles this could lead to the church being liable to the ICO for a data breach. If a staff member or volunteer were to process this data for their own personal use they run the risk of committing one of the criminal offences under the DPA and the church/charity trustees being liable to the ICO for a data breach.

A volunteer within the church holds contact details provided by parents of children attending a Holiday Club. When parents provided this information, they were told it would be used to contact them in an emergency and also to inform them of future church activities which their children might like to attend. If this volunteer then uses the information she holds to contact parents about a child-minding service she is setting up then she is in breach of Data Protection legislation.

* For a definition of who are regarded as the church's Charity Trustees please see page 2 of our leaflet C15:

Help I'm a Charity Trustee. This can be found at www.baptist.org.uk/resources/C15

2.7 Data processor refers to the legal person who processes the personal data on behalf of the data controller and under their instructions. This 'person' will be a third party e.g. an individual (such as a sole trader or self-employed person) or another organisation which is asked by the church to carry out some kind of processing on their behalf. The key point is that for the third party to be deemed a data processor (rather than a separate data controller) they must be processing the personal data for the church's purposes and not their own business purposes. The staff who work for the data processor entity also fall within the definition.

> **EXAMPLE:** A church enters into an agreement with an IT supplier to provide a new church IT system which will securely store the personal data of its members, volunteers, trustees and employees. As part of this agreement, the IT supplier is to maintain the IT system. This would mean that staff of the data processor entity (the IT supplier) would need to have access to the IT system and in so doing, could have access to the personal data of the aforementioned data subjects.

Under the UK GDPR, data controllers and data processors are jointly and severally liable for breaches and so each would be legally liable to the extent to which they are responsible in any data breach.

In the example above if the IT supplier's systems were compromised due to poor security and the church personal data were accessed unlawfully by third parties (e.g. hackers) it would be both the church (data controller) and the IT supplier (data processor) that would face potential enforcement action by the ICO for the breach and/or claims for compensation by individuals who had suffered harm or distress as a result of this data breach.

Many churches will not have third parties processing personal data on their behalf (although it is worth all churches considering whether or not this is the case for them) - but those which do so should have a written contract in place. If your church does use a data processor (or thinks that it might do) **it is VERY IMPORTANT that you read the section 'Data Processor Contracts' in Annex 2 at the end of this document**.

SECTION 3: REGISTRATION WITH THE INFORMATION COMMISSIONER'S OFFICE (ICO) (and exemptions)

Under the DPA, it is the data controller entity which has direct obligations to comply with data protection law. In order to comply with the DPA, data controllers need to pay an annual fee to the ICO **unless they qualify for an exemption. (See below)**

As of 2018 the fee for all charities (including churches) is £40 – or £35 if you pay by Direct Debit. These fees are used to fund the ICO's data protection work. Unless your church qualifies for an exemption, which is narrowly construed, you should pay this fee on an annual basis as it is a criminal offence not to do so. The easiest way to do this is online via the ICO website - https://ico.org.uk/for-organisations/data-protection-fee/.

You should bear in mind that even if you believe that your church does not actually need to register with the ICO, the organisation will still be subject to general data protection law and the guidance in this document should be followed.

A specific exemption applies to 'not-for-profit' organisations which includes churches. This exemption applies if you meet **all** of the following conditions:

- you are only processing data for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit (i.e. your church), or providing or administering activities for individuals who are members of the body or association (your church) or have regular contact with it
- you only hold information about individuals whose data you need to process for this exempt purpose (i.e. church members and those in regular contact with it)
- the personal data you process is restricted to personal information that is necessary for this exempt purpose only

By way of example, if your church is holding details about paid staff or people hiring your building, or you collect details of parents of parents who are not otherwise connected with the church, then you are not likely to be

exempt from registration.

SECTION 4: DATA PROTECTION PRINCIPLES

Under the 1998 DPA there were eight **Data Protection Principles** which set out the rules for dealing with personal data. These were reduced to seven under the GDPR and under UK GDPR they apply to all churches (and other organisations) which handle and process personal data either on a computer or in a paper-based filing system. They also apply irrespective of whether the church needs to register with the ICO.

These seven principles (summarised below) should lie at the heart of your approach to processing personal data.

Lawfulness, fairness and transparency

This means that you will need to

- identify the lawful basis (or bases) for collecting and using personal information
- ensure that you don't process the data in a way that is detrimental, unexpected or misleading to the individuals concerned
- be clear, open and honest with people about how you will use their personal information

Section 5 expands on what this means for churches.

Purpose Limitation

This means that you will need to be clear about what your purposes for processing personal information are.

Data Minimisation

This means that you need to make sure that the personal information you are processing is:

- adequate (sufficient to meet your stated purpose)
- relevant (has a clear and rational link to that purpose)
- limited to what is necessary (you don't hold more information than you need)

Accuracy

This means that you will need to:

- do what you can to ensure the information you hold is not incorrect or misleading
- take reasonable steps to correct or remove incorrect data as soon as possible

Storage Limitation

This means that you should not keep personal information for longer than you need to.
You will need to think about (and be able to justify) how long you keep personal information.

Integrity and confidentiality (security)

You must ensure that you have appropriate security measures in place to protect the personal information you hold.

Accountability

This principle requires you to take responsibility for what you do with personal information and how you comply with the other principles. You therefore need to have appropriate measures and records in place to demonstrate your compliance.

SECTION 5: THE PRINCIPLE OF LAWFULNESS, FAIRNESS AND TRANSPARENCY

This first principle means that you should

- Identify the 'lawful basis' (or bases) under which you are processing personal information (lawfulness)
- Handle people's personal information in ways that they would reasonably expect (fairness)
- Be clear, open and honest with people about who you are, and how and why you use their personal data (transparency)

This is critical for churches to understand and get right. We will start by looking at what it means to be fair and transparent - and then look at the grounds churches can use to process personal data.

5.1 Fair Processing and Privacy Notices

A key part of being 'fair' is not processing an individual's personal data in a way that they would not expect and involves telling the data subject

(i) what items of personal data are being collected about them (particularly if it is not clear or if information about them might be obtained later from third parties)

(ii) how and why their personal data is being processed by the church and

(iii) with whom their personal data might later be shared e.g. if the data needs to be shared with, say, another church or indeed a different organisation later on in order to provide pastoral support for that individual.

Data Protection legislation requires data controllers to inform individuals about the collection and use of their personal data at the time the information is collected from them. The rationale for this is that all data subjects have rights under the DPA and they cannot exercise their rights in relation to personal data if they do not know what personal data is being collected about them and how the church intends to use it. The law does not specify exactly how this notification should be done but in practice it is usually achieved by means of a 'privacy notice' or 'privacy statement.'

The statement can be made orally although the church would need to ensure that it has a robust means of evidencing that this information has in fact been provided to the data subject. It could also be done by means of a paragraph in the church notice-sheet.

Where a church collects the personal data of any data subject through its website, the fair processing requirement could be met by having a 'privacy notice' on its website explaining how the information collected through the website will be used by the church.

The UK GDPR sets out what information should be provided to the individuals whose data is being processed. The following is not an exhaustive list but it does cover the information which churches will usually need to provide. The complete list can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/.

- The identity of the church (or Trustees) as data controller and appropriate contact details. If the church has appointed a Data Protection officer (or main contact person) then their name and contact details should also be included.
- The purpose or purposes for which the data are intended to be processed
- The legal grounds for the processing (see next section)
- The period of time for which the personal data will be held by the church (or criteria used to determine this) and any other information that is necessary to enable the processing to be fair to the data subject e.g. the identities of others with whom the church might share the individual's personal data, how it will be stored securely
- Notification to the individual that they have the right to complain to the ICO if they are not happy with how their personal data have been processed
- Notification to the individual of other rights in relation to their data, including, but not limited to, the right to ask for copies of their personal data (by making a subject access request), to ask for their data to be rectified if it is incorrect, and to have their data erased if it is being processed without a lawful basis.
- Where the personal data is being processed with the individual's consent, the latter must be told that they have the right to withdraw their consent at any time without detriment to them;
- The individual must be informed if their personal data needs to be processed for a contractual or statutory reason and what the consequences are of failing to provide the information.

As explained earlier, churches will collect the personal data of quite a wide variety of data subjects, not just members, trustees or staff (paid and unpaid). There is a legal requirement to provide privacy notices to all of these individuals in the most appropriate format.

It is important that when providing a privacy notice to a particular individual, that it is relevant to that particular individual and covers all of the uses which are likely to be relevant for the church and the individual concerned e.g. a privacy notice provided to an employee will contain different wording to that provided to the parents of children attending a Holiday Club. This is because the kinds of information collected by the church in relation to the employee will not be exactly the same as the information collected in relation to the Holiday Club and the purposes for the processing will be different in each case.

We have a leaflet about **Privacy Statements** with examples of wording to use when collecting personal information in a number of scenarios and a sample 'Contact and Consent' form on our website at https://www.baptist.org.uk/Groups/304642/Data_protection_documents.aspx

5.2 Lawful bases (or legitimate grounds) for processing personal data

As the legal grounds for processing personal information need to be mentioned in privacy notices it is important that churches are clear which grounds they are using to process such data. These will not be the same in every case. Personal information is collected about employees so that they can enter into an employment contract with the employee. Collecting contact details of the parents of children attending a holiday club are different and may require the consent of those parents particularly if this means they will be sent details of future events.

The Data Protection Act says that at least one of 6 conditions must be met for personal data to be processed fairly. **The two conditions which will normally be most relevant to churches are likely to be**:

A. The consent of the data subject. This is **not** the most 'important' or 'safest' ground for processing, contrary to popular belief as this term has a very specific meaning in data protection law. The incorrect use of consent as a legal ground for processing can have unintended and difficult implications for the church and we will look at this in more detail in Section 6.

B. The processing is necessary for the legitimate interests of the data controller (providing that the processing is not unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject).

Collecting and holding the contact details of church members and others in regular contact with it is in the **legitimate interest** of the church because the church needs this information to enable it to keep in touch with such people and provide pastoral support as appropriate. **You do not therefore need to obtain the consent of church members and regular attenders to hold their personal information**. Consent may be needed in other contexts and to enable to you to publish information and this is covered in section 6.

There are a number of other lawful bases which churches could use in particular circumstances. For example, personal data can be processed if the processing is -

- Necessary for a contract with data subject; this is likely to apply where there is a contract between the church and a data subject and the personal data needs to be processed in order for the contract to take effect e.g. where the church employs someone, such as an administrator.

  The collection of an Administrator's contact details, national insurance number, bank and tax details will all be necessary in order to employ them. Without this information it would not be possible for the church to enter into the employment contract with the Administrator. It would therefore not be appropriate or legally correct to ask the Administrator to provide his or her consent for the processing of this kind of personal data.

- Necessary for a legal obligation (other than contract); this may apply where a court order to disclose personal data relating to a data subject is served on a Baptist Church or where there is an Act of Parliament (outside of the Data Protection legislation) which requires the church to disclose or share personal data e.g. where a safeguarding disclosure must be made to the local authority. These are examples of mandatory disclosures where there is a legal obligation to disclose personal data of a data subject.

- Necessary to protect the vital interests of the data subject; this really only applies in 'life or death' situations e.g. if the data subject's personal data needed to be shared with a third party in order to save the individual's life or protect them from serious harm.

5.3 Processing Special Category data

In addition to the conditions set out above there are separate conditions to be met when dealing with Special

Category data. (For an explanation of what is meant by Special Category data please see page 5).

The most relevant grounds for churches are likely to be

C. that the **explicit** consent of the data subject should be obtained OR

D. that the processing is carried out as part of the **legitimate activities of a non-profit body** or association which exists for religious purposes and where the processing:

- is carried out with the appropriate safeguards for the rights and freedoms of data subjects
- relates only to individuals who are members of the body or who have regular contact with it in connection with its purposes; **and**
- does not involve disclosure of the sensitive personal data to a third party without the consent of the data subject.'

EXAMPLE: The minister keeps information on his computer (or in a card index system) about church members and their pastoral needs. Sometimes these notes include an opinion about a person's spiritual needs or details about their physical or mental health or their sexual orientation.

This will be personal data and therefore either Condition A or Condition B on page 10 must be met. If the Minister needs to keep a record in order to provide support for that person as part of his or her role as minister in the church, then 'legitimate interests' ground will be the most applicable legal basis for processing.

The information collected is about the individual's spiritual needs, health and sexual orientation and so this information would also fall into the category of 'special category data'. This means that there needs to be an additional legal ground for this processing.

The likely ground will be the 'charities ground' (Condition D) but this is subject to a number of conditions:

- that appropriate safeguards are in place (for example, the record is kept securely i.e. in a password protected file or in a locked cupboard and cannot be accessed by anyone other than those who strictly need to access it); and
- that the data subject is a church member or someone who has regular contact with the church and not merely someone who occasionally puts in an appearance; and
- the information is not disclosed to a third party i.e. someone who works for a separate data controller entity, without the consent of the data subject.

If even one of the above conditions cannot be met then the church will need to obtain the explicit consent of individuals whose pastoral records are being held. (Condition C)

If the Minister wishes to share any of this sensitive personal data with (for example) their Regional Minister they would need the explicit consent of the individual concerned to share this information as the Regional Minister person is a 'third party' and part of another data controller entity (their Association)

Other conditions which may be relevant are that the processing of sensitive personal data is

- Necessary to fulfil an employment law obligation: this will be relevant in relation to the sensitive personal data of employees of the church which are processed in connection with their employment e.g. to maintain records in relation to statutory sick pay;
- Necessary to protect the vital interests of the data subject or some other person (where their consent cannot be obtained) – applies in 'life or death' situations;
- Necessary for legal advice/proceedings e.g. this may apply where the church needs to obtain legal advice e.g. where the church faces possible or actual legal action by a member or employee and these individuals' sensitive personal data need to be shared with a solicitor or barrister in order to obtain legal advice;
- For ethnic monitoring/equal opportunities processing

In many cases, therefore, the processing carried out by the church may not be based upon the data subject's consent but can be done lawfully using one of the grounds listed above.

Irrespective of whether consent needs to be sought from the data subject for the processing of any of their personal data, it is a legal requirement that data subjects be provided with the fair processing information e.g. by means of privacy notice or statement as mentioned in section 5.1

A privacy notice or statement should not be confused with consent; they are not the same thing. Privacy notices notify individuals as to how their personal data will be processed. Consent is one of many grounds that can provide a legal basis for the processing. Sometimes, though, a consent statement can be inserted into a privacy notice (with appropriate wording and providing a space for the data subject to sign) if the most appropriate legal basis for the processing is indeed consent. See the sample 'Contact and Consent Form' on the 'Data Protection Documents' page on our website – www.baptist.org.uk/Groups/304642/Data_protection_documents.aspx

5.4 Processing Criminal Offence Data

Churches should not be processing any criminal offence data or information relating to criminal proceedings or offences or allegations of offences unless there is a clear lawful basis to process this data, such as where it fulfils one of the substantial public interest conditions in relation to the safeguarding of children and of individuals at risk or one of the additional conditions relating to criminal convictions set out in Parts 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018. In limited circumstances, churches may be involved in the following matters:

- Safeguarding investigations
- Safeguarding contracts
- Post-conviction risk assessments.

This processing should only ever be carried out on the advice of the Ministries Team of the Baptist Union of Great Britain, the Regional Association Safeguarding Contact or a statutory authority.

5.5 Data Protection Impact Assessments

When a church is intending to carry out any data processing of highly sensitive personal data (Special Category Data) which is likely to result in a high risk to an individual's rights or freedoms, a Data Protection Impact Assessment (DPIA) must be carried out prior to the processing. This may arise, for example, where a church may have a Safeguarding Contract in place or is processing information in relation to criminal allegations or convictions.

A DPIA may concern a single data processing operation but a single assessment may also address a set of similar processing operations that present similar high risks. The DPIA Guidelines define "a set of similar processing operations" as operations that are "similar in terms of nature, context, purpose, and risks". This means that there is no requirement to conduct individual DPIAs if other "similar" processing operations have already been assessed.

A DPIA should be continually reviewed and regularly re-assessed as a matter of good practice. A DPIA is not a one-time exercise and may need to be updated once the processing has begun. The Data Controller is responsible for conducting the DPIA which should be conducted in accordance with the ICO's guidance on how to do Data Protection Impact Assessments.

A DPIA may be in a structure and form that is most suitable for a church's operations but should:

- Include a description of the intended processing operations and the purposes of the processing
- Assess the necessity and proportionality of the processing
- Assess the risks to the rights and freedoms of data subjects
- Consider the measures to address the identified risks and thereby demonstrate compliance with the UK GDPR.

A record of the DPIA should be retained for the lifetime of the system or purpose (in relation to Safeguarding records please see the Safeguarding Record Keeping Document at www.baptist.org.uk/gdprsafeguarding). If it is determined that a DPIA does not need to be carried out, a record should also be kept of the reasons why a DPIA was not necessary.

If the risks to an individual's rights or freedoms cannot be mitigated or reduced by privacy-enhancing measures, such as encryption, whereby a high residual risk remains, the Data Controller should consult with the ICO.

SECTION 6: WHAT DOES CONSENT MEAN IN DATA PROTECTION LEGISLATION?

Care should be taken in applying consent as a processing ground because there can be unfortunate consequences for data controllers if this ground is misapplied. Contrary to popular belief, consent (in data protection law) does not represent the 'gold standard' of compliance, nor is it a 'safe bet' for the unsure data controller.

As explained in Section 5, consent is one of a number of lawful bases for processing a data subject's personal information. In terms of importance, they are all of equal weighting. The key to data protection compliance is in understanding which legal ground will apply to the processing of personal data in any particular situation. We have tried to advise in Section 5 what this means for churches.

Under the UK GDPR, consent is clearly defined as being quite explicit and fully informed, unambiguous, involving some kind of positive step on the part of a data subject (e.g. by ticking a box, returning a signed form or by clicking through a carefully and specifically worded consent statement on a website). It is clear that there is no room for implied consent. In addition, the UK GDPR makes it quite clear that consent must be very easy to withdraw at any time without detriment to the data subject. The UK GDPR states that consent will not be the appropriate ground where there is an 'imbalance of power' between the data controller and the data subject (such as in the employer/employee relationship) or where the data subject's personal data is needed in order to enter into a contract with the data subject.

In other words, the data subject must really have a free choice. Difficulties can arise if a church has asked an individual to provide his or her consent to the processing of their personal data and the individual then withdraws their consent for the processing. If, for example, the processing of a church administrator's personal data is based solely on their consent, this can lead to difficulties in continuing the employment relationship if the administrator then withdraws their consent for this processing.

In many areas of church life, churches will be able to rely upon the 'legitimate interests' ground for the processing of non-sensitive personal data of their members and others who are in regular contact with them. However, this will still require churches to provide those individuals with the fair processing information so that it is completely clear how their personal data will be used (see Section 5.1 on privacy statements above).

In addition, it is important to bear in mind that where a church relies upon the 'legitimate interests' ground for processing an individual's personal data, data protection law still provides individuals with a right to object to the processing of their personal data if he or she can show that the processing would cause them substantial and unwarranted damage or distress.

SECTION 7: PUTTING THE DATA PROTECTION PRINCIPLES INTO PRACTICE

Lawfulness, Fairness and Transparency

All individuals whose personal data is processed by the church need to be made aware of what personal data is being collected about him/her and why/how it will be used. As explained in Section 5.1 this is usually done by means of a Privacy Notice and churches will need to ensure this happens. If a 'new members pack' is provided to people when they become church members, such information could be provided to them then. There is further information about Privacy Notices on our website at
https://www.baptist.org.uk/Groups/304642/Data_protection_documents.aspx

The ICO also has guidance on its website on this topic at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Purpose Limitation

The church must only use the information it holds in the way that it has said that it will in its privacy notice to the individual. Use of this information by the church for any other purpose may represent a breach of data protection law unless the church has updated its privacy notice to the individual and is able to identify a legal basis (which might be consent or one of the other legal grounds) for the new use of the person's data. For instance, if the church wanted to use someone's story of how the church had helped them deal with issues in their life on the church website, individuals would need to give their specific consent for their personal information to be shared in this way.

Data Minimisation

Churches must ensure that they only hold information which is adequate, relevant and limited to what is

necessary. For example, if a minister records their opinions about the spiritual needs of the individual whom he or she is assisting, they must ensure that the information which is recorded is sufficient for them to be able to provide that support but not more than is actually needed. They should not record information which isn't relevant to their stated purpose of providing pastoral care and support for that individual.

Accuracy and Storage Limitation

Data protection legislation does not state how long personal data must be kept for. However, what is deemed 'necessary' will depend on the church's legitimate operational purposes, insurance requirements and any other statutory provisions e.g. there are legal requirements in relation to the keeping of employee records for tax purposes.

It is strongly recommended that all churches have in place a data retention policy or schedule which sets out the various periods of time for which different kinds of records containing personal data will be kept. It is important that data subjects are advised of the periods of time for which their own records will be kept or what the criteria are in relation to how long their data are retained.

We have a sample data retention schedule on our website for churches to use and adapt. This can be found at https://www.baptist.org.uk/Groups/304642/Data_protection_documents.aspx

It is also important that churches have measures or procedures in place to ensure that there is periodic updating of records. The ICO has stated that holding on to records 'just in case they come in handy later on' is not a legitimate reason for retaining individuals' personal data. Churches will need to consider how long they will need to hold on to records of individuals with whom they lose touch. Retaining pastoral and sensitive information about a former church member who last made contact 20 years ago is unlikely to be compliant with data protection law. This however doesn't prevent a church retaining the names of church members and details of when they came into membership, were baptized, left the church etc. for historical purposes - but they shouldn't hold any contact details or any other personal or sensitive information.

Records of the deceased will also need to be processed sensitively and securely. Even though personal information about someone who has died is no longer subject to data protection law, the common law duty of confidentiality will still apply for a period of time after someone has passed away. In addition, records relating to a deceased person may also contain information about living individuals (e.g. their family and friends). The personal information of the latter will therefore need to be processed in accordance with data protection law, with an exception being safeguarding-related information.

Once a data retention policy or schedule has been established it is important that all records are held in accordance with this policy and that church staff and volunteers and data subjects are aware of the policy. Records should be securely and permanently removed from church manual/paper records and any electronic system once the retention period has expired. Retaining records beyond the period of time set out in the retention policy not only risks the church being in breach of data protection law but also potentially raises risks for the church when data subjects exercise their right to obtain a copy of their personal data – see Section 8.

Integrity and Confidentiality (Security)

The principle states "You must ensure that you have appropriate security measures in place to protect the personal data you hold." It does not define 'appropriate security measures' and so it is left to data controllers to determine what this means in their context taking into account the nature of the personal data and the perceived risks to it. For more information on this see the guidance from the ICO:

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

Churches need to ensure that any personal data held is processed in a sufficiently secure manner (whether in paper or electronic form) to prevent unauthorised access (whether by unauthorised church staff or third parties). This could include any or all of the following:

- Storing paper-based information in secure lockable cupboards;
- Making appropriate use of password protections and encryption of particularly sensitive electronic documents;
- Restricting access to both paper and electronic personal data to those who are necessary for it to be processed;

- Ensuring that there are clear processes in dealing with telephone calls and that personal data should not be disclosed over the telephone unless the church recipient is confident of the identity of the caller and that they have legal grounds to disclose any personal data requested (the church may require callers to put requests in relation to personal data in writing for example).
- Ensuring that information is not leaked through eavesdropping in public places (whether through speech, written or electronic communication); and
- Ensuring sensitive personal data is transmitted securely in a way that cannot be intercepted by unintended recipients;
- in relation to data held electronically, computer systems should be securely configured, have adequate firewalls and malware protection and receive regular software updates;

The ICO strongly recommends that electronic devices which hold an organisation's personal data are encrypted e.g. desktop computers, laptops, tablet computers and USB sticks for example.

All staff (including volunteers) who handle personal data should have some training in Data Protection - ideally in a way that is appropriate to their role). A key feature which is often highlighted by the ICO in the aftermath of serious data breaches is the lack of staff training.

See Annex 3 for some suggestions about training for church staff and volunteers

Accountability

In essence this principle means that the church's charity trustees need to understand that they are responsible for ensuring the church complies with Data Protection legislation and can demonstrate that they are complying. Working through the checklist we have provided in Annex 1 and recording what actions have been taken will enable you to do this.

SECTION 8: SUBJECT ACCESS REQUESTS

Data Protection legislation gives individuals the right to obtain a copy of their personal data which organisations hold as well as other supplementary information. This helps individuals to understand how and why organisations are using their data and that they are doing so lawfully. Any individual can, therefore, ask your church about information you hold about them. They can ask you to confirm that you are holding personal information about them and ask you for a copy of what you hold. This is commonly referred to as a 'Subject Access Request' (SAR).

Whilst is it is rare that churches will receive such requests it should not be ruled out as a possibility. We are seeing more incidences of SARs being used where a data subject have a grievance against a church. Churches are, therefore, strongly advised to ensure that they have clear policies and procedures for dealing with all requests for information about their data subjects and that those who are likely to deal with such requests in the first instance (normally the Minister, Church Secretary or church office staff) are sufficiently trained in data protection to be able to deal with them or pass them on expediently to the relevant person.

The law around SARs changed under the GDPR (and has been retained in the UK GDPR) whereby:

- Requests can be made to anyone in the organisation by any means – including verbally or via social media. The request doesn't have to include any specific phrase or refer to particular legislation as long as it is clear that the individual is asking for their own personal data.
- You cannot normally charge a fee to provide this information. However, where the request is clearly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request. You can also charge a reasonable fee if an individual requests further copies of their data following a request. You must base the fee on the administrative costs of providing further copies.
- You have one calendar month in which to provide the requested information. The month starts from the day the request is received, even if the request is sent outside of normal working hours, so if you receive a request on 4 June you have until 4 July to provide the information

The BU Data Protection team is willing to advise any BUGB member church which receives a Subject Access Request but will not usually be able to complete these for you. Legal advice should be sought in all cases where there is uncertainty regarding the information to be provided to the requester.

A separate guidance note for churches on handling Subject Access Requests is available here.

There is also some information on the ICO website - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Individuals are only entitled to their own personal data and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, where any documents held by a church include personal data of anyone other than the data subject, this data is not disclosable unless the other individuals have provided consent for the disclosure of their information.

Quite often, data subjects' personal data will be very closely intertwined with that of other living individuals e.g. where a church member X expresses an opinion in an email about church member Y to individual Z who works for the church, the email will contain the personal data of all three individuals. The email will identify X and Z (their names and email addresses will be their personal data) and the opinion of X will be both the personal data of X and Y. If Y makes a subject access request for their personal data, X's opinion will usually be disclosable as it is the personal data of Y. However, steps would need to be taken to anonymise this information by removing (redacting) the name and email address of the other parties to the email.

The section *'What should we do if the data includes information about other people'* in the information provided by the ICO (see above link) is helpful.

It is also important to note that data subjects are not entitled to copies of documents, only their personal data contained within them. However, in practice, the usual, and simplest way for a church to comply with a subject access request will be to review documents and redact the personal data of third parties and any information which does not constitute the personal data of the requester (e.g. information which may relate to church policy or procedure rather than the data subject who has made the request).

There are a number of exemptions which can apply to subject access requests in particular circumstances, which would provide a church with a lawful basis for withholding certain personal data to individuals when they make a Subject Access Request. These include, but are not limited to, legal professional privilege (in relation to advice obtained from a solicitor or barrister) and the 'crime' exemption which can be applied where the provision of personal data to a data subject would be likely to prejudice a criminal investigation.

SECTION 9: DATA BREACH REPORTING

Under the UK GDPR, certain types of personal data breaches must be reported to the ICO within 72 hours of becoming aware of the breach, where feasible.

A 'personal data breach' is when personal information is lost or stolen, inadvertently sent to the wrong recipient, access by an unauthorised third party or unlawfully amended or destroyed.

If the breach is likely to result in a high risk of adversely affecting individual's rights and freedoms, then this must be reported to the ICO and the individuals affected should also be informed as soon as possible.

For more information about personal data breaches see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

To report a data breach to the ICO, follow this link: https://ico.org.uk/for-organisations/report-a-breach/

If you become aware of a data breach but do not feel you need to report this – i.e. you don't think this is likely to severely affect the rights and freedoms of the individuals concerned, you should still record the breach and why it was decided not to report this.

Data breaches need to be assessed on a case by case basis. For example, you would need to notify the ICO about a loss of the minister's laptop which contained all her pastoral notes (including sensitive personal information) which was not in password-protected documents. On the other hand, the unauthorised provision of the church directory to a third party might not need to be reported, depending on the circumstances.

SECTION 10: INTERNATIONAL TRANSFERS

Because the UK GDPR primarily applies to controllers and processors located in the UK, individuals risk losing the protection of the UK GDPR if their personal data is transferred outside of the UK.

On that basis, the UK GDPR restricts transfers of personal data outside the UK, or the protection of the UK GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

This will generally affect churches in one of two ways

a) The organisation which they use to hold or process data (e.g. DropBox, MailChimp, or MS Teams) is based outside the UK

b) Churches want to send information about people in their church to members living overseas.

The ICO have detailed guidance on this area which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

In summary form … once an organisation has recognised that it needs to transfer data out of the UK it needs to check:

- If the country concerned is covered under the 'adequacy regulations' issued by the Government of the United Kingdom– in other words, has the UK determined that this country has adequate protection in place? A list of such countries is on the ICO website. *From January 2021 such countries and territories include those within the European Economic Area (EEA) plus those covered by existing EU Commission 'adequacy decisions' (Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay) and Gibraltar.* If so, then it is fine to make the transfer.
- If the country is not covered by the UK adequacy regulations then organisations should see if the transfer is covered by one of the 'appropriate safeguards' in the UK GDPR. Details are on the ICO website (see above link) and include entering into a contract with the receiver incorporating standard data protection clauses recognised or issued in accordance with the UK data protection regime. These are known as 'standard contractual clauses' ('SCCs' or 'model clauses').

If all else fails then organisations can rely on a number of exemptions and, again, these are explained on the ICO website. The one which churches are most likely to use is if the individual (whose data is being transferred outside the UK) has given their explicit consent. The ICO website explains what information you need to provide to the individual concerned to enable them to give their consent.

SECTION 11: A FEW LAST THINGS TO CONSIDER

All documents referred to in this section
can be found at https://www.baptist.org.uk/Groups/304642/Data_protection_documents.aspx

There is also a link to this page from our main Data Protection webpage www.baptist.org.uk/gdpr

Publishing information on the Church Website and/or other social media sites

Publishing information via the internet is publishing it world-wide. In these circumstances it is most likely that consent will be the most applicable legal basis for this processing. Each person's explicit and informed consent should be sought before publishing their personal information on your website etc. This includes photographs and special care should be taken with photographs especially of children and young people. It is strongly recommended that churches obtain the consent of a parent or guardian with parental responsibility for the child in question before publishing information about children.

Streaming of Services

A church should seek consent from any individuals appearing on screen (where they can be identified) for their involvement in the filming and the processing of their personal data through video footage. Records of these consents should be kept, in line with the church data retention policy. This should be straightforward when there are limited numbers of people involved who are clear on the purpose for which their data will be used in the service.

Where a church is planning to hold a service in the church with a congregation and broadcast it at the same time to a wider audience (either live or later) then this may involve processing images of the persons attending the service who might be filmed and identifiable from the footage. It would be disproportionate to obtain consent from everyone in the congregation for their personal data to be used in this way. Please see Question 22 of our Data Protection 'Frequently Asked Questions' document for practical steps the church can take to manage data protection compliance in such a context.

Hybrid Working/Working from Home

Since the COVID-19 pandemic we have adjusted to new ways of working. This means that many of us are now working from home at times. Your church's data protection policy will still apply to those doing church work from home and who are processing individual's personal data. It is important to give consideration to the security of the data being processed from home by following the security practices recommend in Section 7 as well as thinking about the following:

- Are electronic devices where church-related personal information is held password or PIN protected? Family members should not be able to log on to the same account where church data is stored.
- Where possible, documents should be edited and saved onto church systems e.g. using online Microsoft Office tools, rather than saving documents to a personal device.
- Where a document is saved onto a personal device, create a specific folder for all church-related documents and review the folder on a regular basis e.g. empty your "recycling bin" in Windows to minimise the footprint of church documents on your device.

Using CCTV on the Church Premises

If your church uses CCTV then you are certainly required to be registered with the ICO. The ICO have helpful information about the use of CCTV and other types of video surveillance, found at Video surveillance | ICO.

Circulating Contact Details

Whilst there is no legal rule that states that churches must obtain the consent of individuals before their names and contact details are on any sort of published list, this is likely to be advisable particularly where the details are to be circulated by email or published in any way which would make it accessible to people outside the church. This is because this information (relating to church membership) is deemed to be Special Category data.

For example, the church could operate a system where everyone joining the church signs a form that says they are happy for the details they provide on the form to be used in the way you tell them they will be used. (We have a **sample contact and consent form** on our website.) If someone asks to have any or all of their contact details removed from such a list, then you will need to comply with their request as soon as possible.

Direct Marketing

In Data Protection law, 'Direct Marketing' means the communication of any advertising or marketing material to particular individuals. **This extends beyond offering goods and services and covers the promotion by a charity (including a church) of its aims and ideals, appeals for funds and campaigns.** Direct marketing commonly takes place via telephone, email, text message or post.

The ICO has specifically stated that the direct marketing rules apply to charities (including churches) in the same way that they do in relation to other organisations. It is beyond the scope of this guidance note to explain the rules in relation to direct marketing in detail as these can be complex. In general terms, however, the sending of direct marketing materials to individuals must be carried out in accordance with the Data Protection Act and this requires legal grounds.

In relation to postal marketing the most appropriate bases will be (i) consent or (ii) the legitimate interests ground.

Electronic forms of marketing, including by email or text message, are more tightly regulated and in general terms, require the explicit prior consent of the individual to whom the message is to be sent.

Further information on direct marketing can be obtained on the ICO's website – see the link below:
https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

If, when collecting contact details of the parents of children attending a holiday club, you intend to also use them to email (or send by text) details of other church-run activities which their children might be interested in attending – you need to make this clear on the form and ask the parents to indicate their consent to be contacted in that way. See example in our document (on the website) about **Privacy Statements**

Record-keeping

It is beyond the scope of this leaflet to provide more detailed information on exactly what needs to be kept by each individual church. However, we have produced a suggested **Data Retention Schedule** for churches to adapt for their own use and this is on our website. Some of the time periods given relate to legal requirements and other are 'good practice' and we have indicated this in the document. Data Protection guidance is that

personal information should not be kept for any longer than you need it. Individual churches will need to decide what that means in their own context.

Data Protection Policy

All churches should have their own Data Protection policy which sets out in some detail how the church, as a data controller, complies with Data Protection law. It should contain guidance on how requests for personal data are dealt with; including Subject Access Requests and requests from third parties such as the police and safeguarding authorities (data sharing). The ICO's statutory Data Sharing Code of Practice should also be adhered to when sharing any personal data with third parties.

We have produced a sample Data Protection Policy for churches to adapt for their own use which can be found on our website at www.baptist.org.uk/gdpr. The policy should contain guidance on data breach reporting procedure, data retention and security (in relation to both paper and electronic records) and should contain clear guidance on the use by staff (both paid and unpaid) of their own electronic devices both at home and on church premises. Data Protection law does not prevent churches from allowing staff to use personal devices to process the personal data of the church but there are significant compliance implications in doing so and there should be clear guidelines for staff in this regard.

It is currently good practice for all data controllers to keep records of disclosures e.g. where personal data is shared with third parties, and to keep a record of the legal basis for the disclosure and whether any legal exemption is applied. A similar record in relation to Subject Access Requests is required.

ANNEX 1: CHECKLIST AND ACTION POINTS FOR CHURCHES

A: Has one of the church leaders (Trustees) read through this leaflet?
- *If the answer is **NO** – please ensure that someone does!*

B: Does the church hold personal data in electronic and/or paper form?
- *If the answer is **YES** then the church needs to ensure that they hold this data in line with Data Protection legislation.*
- *If you are unsure, please read Sections 2.1 – 2.5 (pages 4-6) and discuss with all Trustees*
- *If you are absolutely sure that the answer is **NO** then Data Protection legislation doesn't apply*

C: Have you identified what personal data is held or processed by church staff and volunteers in connection with their role, who is holding/processing this and where it is held?
- *We would suggest that the Trustees take time to undertake this exercise to ensure that all are clear as to the extent of their responsibility in this area.*

D: Are you clear who the Data Controller is in relation to your church?
- *If the answer is **NO** then read section 2.6 (page 6)*

E: Does the church use Data Processors? (See section 2.7 for more information)
- *If the answer is **YES** then please ensure you read Annex 2 about Data Processor contracts and take appropriate action.*

F: Is the church registered with the ICO as a Data Controller?
- *If the answer is **NO** you should consider whether you are exempt from registration (Read page 7 carefully).*
- *If you are not exempt (or are unsure whether or not you are) then you should register with the ICO via their website* https://ico.org.uk/for-organisations/register/
  This page also includes a self-assessment checklist to help you decide if you need to register.

G: When collecting personal data from individuals do you provide them with information of what you are collecting and what you will be doing with it?
- *If the answer is **YES** then this information (Privacy Statement) may need to be updated to be compliant with UK GDPR*
- *If the answer is **NO** then you will need to start to do this.*

Either way you should read Section 5.1

H: Are you clear what grounds you are using to process the data you hold?
- *We would suggest that you take the list you produced to enable you to answer Question C and answer this question for all the different types of information you hold. As explained in sections 5.2 and 5.3 the most likely grounds would be 'Consent' or 'Legitimate Interest'. It is highly likely that you will use different grounds for different types of information held or processed. This is an important exercise to undertake.*

Having undertaken the work you need to do to answer Questions G and H – you should now make sure you are using the right form of Privacy Statement wherever and whenever you collect personal information.

If you are relying on 'consent' as your grounds for processing data you must read Section 6 and work out how this applies to your situation.

I: Has the church adopted a Data Protection Policy?
- *If the answer is **YES** then you should now review this in the light of the changes in legislation and our suggested policy which can be found using the link to the Data Protection Documents page at* www.baptist.org.uk/gdpr
- *If the answer is **NO** then you should look to produce one using our suggested policy which can be found as indicated above*

J: How secure is the personal information you hold?

- *Is paper-based information held in secure lockable cupboards which can only be accessed by those who need to process the information in line with their role in the church?*
- *Are all electronic devices where church-related personal information is held password or PIN protected?*
- *Are documents containing sensitive personal information encrypted?*
- *Have appropriate steps been taken to protect personal data being processed by individuals doing church work from home?*

K: Are all staff and volunteers who process personal information fully aware of their data protection responsibilities?

- *If the answer is **NO** then consider how best to enable this to happen. Depending on their role and the type of data they are processing this can range from a checklist they need to follow to a formal training session. See Annex 3 for some suggestions about training.*

L: Do you have procedures in place for dealing with any 'Subject Access Requests'?

- If the answer is NO then we suggest you put some in place which could be as simple as
  Step 1: Any requests received must be passed immediately to the Church Secretary (or the Minister in their absence)
  Step 2: Use the checklist on the ICO website to determine what you need to do
  https://ico.org.uk/for-organisations/subject-access-request-checklist/
  Step 3: Read the ICO Code of Practice on Subject Access Requests (link on page 15) and contact the BUGB Data Protection Officer (or take legal advice) if there is an uncertainty about what you need to do or what you can provide.
  Step 4: Make sure you provide the information to the person submitting the request within a month

M: Do you undertake any form of 'direct marketing' by email or text message? (See section 11)

- *If the answer is **YES** then ensure that you have the express prior consent of those to whom this is sent.*

N: Do you include any sort of personal information (including photographs) on your website?

- *If the answer is **YES** then ensure that you have the express prior consent of all individuals concerned*

O: Do you record or live-stream church services or other events?

- *If the answer is **YES** then ensure that you have taken steps to limit the personal data collected during filming and have the express prior consent of all individuals whose personal data will be captured on video.*

P: Do you have a printed or electronic Church Directory or Contact List?

- *If the answer is **YES** then it would be best practice to obtain express consent from those individuals included in it.*

Q: Is the church undertaking any high-risk processing of sensitive personal data which might require a Data Protection Impact Assessment? (See section 5.5 for more information)

- *If the answer is **YES** please read Section 5.5 and consider whether you need to undertake this assessment.*
- *If the answer is **NO** then please be aware that this may need to be carried out in the future if the relevant circumstances arise.*

ANNEX 2: DATA PROCESSOR CONTRACTS

The DPA 1998 introduced the requirement for a data controller to have a contract in writing with its data processors that needs to include specific clauses in relation to the security of the processing and in relation to the requirement to act only on the controller's instructions. Under the UK GDPR, a great many more clauses are required in order to ensure that the data processor entity carries out processing which is compliant with the law.

Where a church enters into an arrangement with a third-party data controller, the requirement for the mandatory data processor clauses to be included in any service contract does not apply. However, in practice it can sometimes be difficult to ascertain whether the third party is to perform a service in the capacity as the church's data processor or separate data controller.

Where there is uncertainty on this point, it is important to look at the facts: what is the third party actually going to be doing in relation to the church's personal data? It is important to bear in mind that it is not possible to 'contract out' of the requirements of data protection law and despite what any legal contract states between the parties, the data protection roles (i.e. data controller/data processor status) will depend on what the parties are actually doing with the personal data in question and, in particular, the level of control over substantive decisions in relation to the data.

The ICO has a useful guide available on their website which provides guidance in establishing whether an organisation is a data controller or data processor – see:
https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

ANNEX 3: Data Protection Training for Churches

Who for?

- Trustees
- Staff
- All who process personal information as part of their role in the church

When?

- As part of an induction programme for Trustees and Staff
- Whenever someone takes on a role which involves them handling personal information.
- Refresher training as part of other training events and/or at a Church Meeting

How?

Possibilities include:

- Document for individuals to read themselves - which includes the main points of this Guideline Leaflet as it relates to your church. It could include a list of questions at the end of the document to test whether the person has picked up the main points.
- Document (as above) which the Church's Data Protection Trustee (or other person) goes through with people on a 1-1 or small group basis.
- Large group training with PowerPoint and handouts. (See information below about the one we have produced)

What to include

The following topics will be suitable for most churches. Page numbers relate to the relevant pages in this leaflet:

- ✓ Introduction to Data Protection legislation and why it is important for your church to abide by it. (pages 2-3)
- ✓ Explanation of the types of personal information held and/or processed by the church. (pages 3-5)
- ✓ Ensuring that the correct information is provided to individuals when their data is collected (pages 7-8 and Annex 3)
- ✓ Explanation of the different grounds for processing personal information. (pages 8-11)
- ✓ What the seven Data Protection Principles mean in practice for your church. (pages 12-14)
- ✓ Explanation of the church's procedures for handling Subject Access Requests (page 15)
- ✓ Looking at any direct marketing which the church is involved in (pages 15-16)
- ✓ Consider staff and volunteer working from home arrangements and how personal data may be used outside the church context (page 18)

Please note that we now have a **'Introduction to Data Protection'** training pack on our website. This is intended to be used in a Church Meeting or other suitable gathering and can be found at https://www.baptist.org.uk/Groups/304642/Data_protection_documents.aspx

---

Association Trust Company	Contact
Baptist Union Corporation Ltd **East Midland Baptist Trust Company Ltd**	Baptist Union Corporation Ltd Baptist House PO Box 44 129 Broadway Didcot Oxfordshire OX11 8RT Telephone: 01235 517700
Heart of England Baptist Association	Heart of England Baptist Association 480 Chester Road Sutton Coldfield B73 5BP Office Mobile: 0730 505 1770
London Baptist Property Board	London Baptist Association Unit C2 15 Dock Street London E1 8JN Telephone: 020 7692 5592
Yorkshire Baptist Association	17-19 York Place Leeds LS1 2EZ Telephone: 0113 278 4954
West of England Baptist Trust Company Ltd	West of England Baptist Trust Company Ltd Little Stoke Baptist Church Kingsway Little Stoke Bristol BS34 6JW Telephone: 0117 965 8828

This is one of a series of *Guidelines* that are offered as a resource for Baptist ministers and churches. They have been prepared by the Legal and Operations Team and are, of necessity, intended only to give very general advice in relation to the topics covered. These guidelines should not be relied upon as a substitute for obtaining specific and more detailed advice in relation to a particular matter.

The staff in the Legal and Operations Team at Baptist House (or your regional Trust Company) will be very pleased to answer your queries and help in any way possible. It helps us to respond as efficiently as possible to the many churches in trust with us if you write to us and set out your enquiry as simply as possible.

The Legal and Operations Team also support churches that are in trust with the East Midland Baptist Trust Company Limited.

If your holding trustees are one of the other Baptist Trust Corporations you must contact your own Trust Corporation for further advice. A list of contact details is provided above. If you have private trustees they too should be consulted as appropriate.

Contact Address and Registered Office:

Support Services Team, Baptist Union of Great Britain, Baptist House, PO Box 44,
129 Broadway, Didcot OX11 8RT
Tel: 01235 517700 Fax: 01235 517715 Email: legal.ops@baptist.org.uk
Website: www.baptist.org.uk Registered CIO with Charity Number: 1181392

Date Reviewed July 2022 Date of Issue July 2022