Guideline Leaflet L13: Data Protection

If a church holds personal data either on a computer or in a paper-based filing system it must follow the rules set out in the Data Protection Act 1998, and from 25th May 2018, the new General Data Protection Regulation 2016. 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 6)

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.

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.

1. INTRODUCTION TO DATA PROTECTION LEGISLATION

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.**

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 (DPA) seeks to protect an individual against the unfair use of their personal information. From 25th May 2018 the new General Data Protection Regulation (GDPR) will supersede the DPA. There are a number of fundamental principles (the Data Protection Principles) which the DPA establishes 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 of the DPA also form part of the new GDPR.

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 holds *personal data* either on a computer or in a paper-based filing system it must follow the rules set out in the DPA and, from the 25th May 2018, the GDPR. 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.

- Under the current law the ICO has a range of enforcement tools at its disposal including the imposition of a financial penalty (a 'monetary penalty notice') of up to £500,000 for the most serious breaches.
- Under the GDPR, the financial penalty for the most serious breaches will rise to €20 million (or 4% of annual turnover, whichever is the higher) for all organisations, including churches and other charities.
- 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 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.

2. THE TECHNICAL TERMS

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.**

The new GDPR widens the definition of personal data to include 'online identifiers' such as computer IP addresses.

> 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.

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.

This 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;
- 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 or laptop/tablet will be personal data of the individuals concerned, as will moving images of living individuals held on mobile phones, digital video cameras or CCTV recording equipment.

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.

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 Sensitive Personal Data is personal data which consists of information concerning the data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, membership of a Trade Union, physical or mental health condition, sexual life (and sexual orientation under the GDPR) commission or alleged commission of any offence, a record of any proceedings for any offence committed or alleged, or a record of any sentence or proceedings. *In addition, when the GDPR comes into force in May 2018, genetic data and biometric data (e.g. fingerprint data or data obtained through facial-recognition technology) will 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. Where churches carry out Disclosure and Barring Service (DBS) checks on employees or volunteers, they may also process sensitive personal data in the form of criminal convictions data. 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 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 data 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')

2.5 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.

2.6 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.

Currently, data processors have no direct obligations under data protection law but this is changing under GDPR so that data controllers and data processors will be 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 (from May 2018) 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.

Most 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**.

3. DATA CONTROLLERS AND THE INFORMATION COMMISSIONER'S OFFICE (ICO)

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 are currently required to 'notify' the ICO of their processing. This means maintaining an annual registration with the ICO and paying the registration fee (currently £35 for charities), unless an exemption from notification applies.

There is currently an exemption from notification for certain not-for-profit organisations (which can include churches). However, this is very narrowly construed and is of very limited remit. It is likely that most Baptist churches should register with the ICO. [Details in Annex 1]

The process can be done online via the ICO website – https://ico.org.uk/for-organisations/register/

Under GDPR there will no longer be a requirement to notify the ICO in the same way. However it will remain a legal requirement for data controllers to register with the ICO and pay a data protection fee. It is anticipated that exemptions will still apply which will mean some churches will not need to register or pay a fee.** These fees will be used to fund the ICO's data protection work.

The ICO have now (February 2018) published their draft proposals for this which still need to be approved by government. They can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/guide-to-the-data-protection-fee/

To summarise these proposals as they affect churches…

- Whilst there are three payment tiers all Charities (unless they are subject to an exemption**) will only need to pay the lowest fee – 'Tier 1'. This is anticipated to be £40 per year (or £35 if you pay by Direct Debit).
- Churches which are already registered with the ICO will be contacted before their registration expires to explain what they need to do.
- Churches which have not registered, and which do not meet the criteria for exemption will need to register and start paying the fee.
- The ICO will impose fines for organisations which should pay a fee and do not do so.

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.

Where there is no exemption applicable, it is a criminal offence for an organisation to fail to register or to fail to keep its registration details up-to-date. Where a church converts from an unincorporated association to a CIO it should therefore update its registration with the ICO accordingly.

** 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, or providing or administering activities for individuals who are members of the body or association or have regular contact with it
- you only hold information about individuals whose data you need to process for this exempt purpose
- the personal data you process is restricted to personal information that is necessary for this exempt purpose

Further information and advice about compliance with the Data Protection Act 1998 and the 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 our 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/

4. THE EIGHT DATA PROTECTION PRINCIPLES

There are eight **Data Protection Principles** laid down in the Act which set out the rules for dealing with personal data. These are listed below and apply to all churches which handle and process personal data either on a computer or in a paper-based filing system. It also applies irrespective of whether the church needs to register with the ICO.

The Act requires the data controller to ensure that all personal data is dealt with in accordance with the 'Eight Principles' set out in the Data Protection Act. These Eight Principles in summary form (and paraphrased) are as follows:

***Personal data* must be fairly and lawfully processed**

***Personal data* must be processed for limited purposes**

***Personal data* must be adequate, relevant and not excessive**

***Personal data* must be accurate and up to date**

***Personal data* must not be kept for any longer than is necessary**

***Personal data* must be processed in line with the data subjects' rights**

***Personal data* must be processed securely**

***Personal data* must not be transferred to other countries without adequate protection**

These Principles are expressed in a slightly different format in the new GDPR but they will apply in much the same way. It is important to note that a much greater amount of detail is provided in relation to data subjects' rights than at present in the DPA and these rights are extended.

5. PROCESSING PERSONAL DATA IN A FAIR AND LEGAL WAY

The first data protection principle says that personal data must be fairly and lawfully processed – and that you must have legitimate grounds for processing it. **This is critical for churches to understand and get right.** We will start by looking at what it means to process data fairly and then look at the grounds churches can use to process personal data.

5.1 Fair Processing and Privacy Notices

Fairly is an extremely important element of the first Data Protection Principle and will continue to be a crucial part of data protection compliance under the GDPR.

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.

There is currently a requirement under the DPA to tell data subjects about this processing at the time that the church first collects their personal data, or as soon as possible thereafter. The rationale for this is that all data subjects have rights under the DPA and they cannot exercise their rights in relation to their personal data if they do not know what personal data is being collected about them and how the church intends to use it.

Data protection 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 policy' on its website explaining how the information collected through the website

will be used by the church.

Under the GDPR, it will be a legal requirement to include much more detail in privacy notices. The following is not an exhaustive list but it provides examples of the kinds of information which will need to be provided to individuals under the new law.

- The identity of the church (or Trustees) as data controller and appropriate contact details. If the church has appointed a Data Protection officer (and most churches will not need to do this) 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 fair processing information 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.

Annex 3 contains examples of forms which could be used to collect personal information in a number of scenarios

5.2 Legitimate grounds for processing personal data

As the legal grounds for processing personal information will need to be mentioned in privacy notices from May 2018 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, particularly when the GDPR comes into effect. 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).

There are a number of other legal conditions which could legitimise the processing by churches in certain cases

and those shown below may apply in particular circumstances.

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.

  There is, in addition, a legal exemption under the Data Protection Act 1998 which can be applied meaning that the church would not necessarily have to notify the data subject concerned that the disclosure was being made (e.g. if notifying the data subject would prejudice the purpose of the disclosure such as by 'tipping off' a suspected criminal).

- 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 Legitimate grounds for processing SENSITIVE personal data

In addition to the conditions set out above there are separate conditions to be met when dealing with sensitive personal data. (For an explanation of what is meant by sensitive personal data please see page 4).

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.'

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

EXAMPLE: The minister keeps information on his computer (or in a card index system) about church members and their pastoral needs. Sometimes these notes includes 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 8 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 it is likely that the 'legitimate interests' ground will be the most applicable processing ground.

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 'sensitive personal data'. This means that there needs to be an additional legal ground for this processing (see page 9).

The likely ground will be the 'charities ground' (Condition D) but this is subject to stringent 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)

We can therefore see that, in many cases, the processing carried out by the church may not be based upon the data subject's consent, but may properly be legitimised by 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 examples in Annex 3.

5.4 Data Protection Impact Assessments

When a church is intending to carry out any data processing of highly sensitive personal 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 Code of Practice Conducting privacy 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 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.

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. The Information Commissioner has published a series of articles on the ICO website. Below is a link to their recent article entitled, "Consent is not the silver bullet," which explains this point further.

https://iconewsblog.org.uk/2017/08/16/consent-is-not-the-silver-bullet-for-gdpr-compliance/

Consent is one of a number of legal bases for processing a data subject's personal data. 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 – and this will depend on (i) the type of personal data processed (i.e. whether it is 'ordinary' personal data or sensitive personal data) and (ii) the particular purposes for which the items of personal data listed in (i) are to be processed (i.e. it is context dependent). Where there is uncertainty over this, legal advice should be sought.

Under the new 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 GDPR makes it quite clear that consent must be very easy to withdraw at any time without detriment to the data subject. The 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.

There will be circumstances in which churches will be able to rely upon the 'legitimate interests' ground for the processing of non-sensitive personal data of their data subjects. 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 even though the application of this ground is not reliant upon the individual's consent, where a church relies upon the 'legitimate interests' ground for processing an individual's personal data, data protection law provides that individual 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.

7. PUTTING THE DATA PROTECTION PRINCIPLES INTO PRACTICE

We will use the scenario outlined on page 10 to illustrate the way that the Data Protection Principles apply to churches.

Principle 1: **Processing must be fair and lawful and carried out with appropriate legal grounds**

The individual who is being provided with support for their spiritual needs would need to be aware of what personal data is being collected about him/her and why/how it will be used (with the extra detail required under the new GDPR from May 2018). The individual needs to be provided with the fair processing information. There is no one 'set' way of doing this and the church will need to adopt a policy on how this is to be carried out. If a 'new members pack' is provided to people when they become church members, such information could be provided to them then. See also section 5.1 on Privacy Notices. The ICO has published guidance on its website on this topic – see

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Principle 2: **Processing must be for limited purposes**

The church must only use the information in relation to the individual's spiritual needs 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 individual felt that she wanted to share her experiences of the support from the church with the wider community in order to promote the good work of the church she may give her consent for the information to be shared in this way.

Principle 3: **Processing must be adequate, relevant and not excessive**

When the 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 adequate, relevant and not excessive. In other words, the minister must ensure that they record only that information about the individual which is actually needed in order to provide the support.

Principles 4 and 5: Personal data must be up-to-date and not held longer than is necessary

Data protection law 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.

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, except for safeguarding-related information.

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.

<u>Principle 6:</u> Processing in accordance with individuals' rights

All data subjects currently have a number of rights under the Data Protection Act 1998. These will be extended in some respects under the GDPR.

The rights which will be most relevant to churches include:

- the right of access to a copy of their personal data (the right of subject access) – see Section 8
- the right to correct any mistakes in their personal information;
- the right to restrict or prevent their personal data being processed for direct marketing purposes (see section 9 on direct marketing) and in certain other limited circumstances;
- the right to erasure – subject to certain conditions e.g. if the processing of an individual's personal data is based upon their consent and after having withdrawn their consent for the processing, the church continues to hold the individual's personal data;
- the right to take proceedings through the civil courts against the data controller entity (either the charity trustees or the CIO, whichever is the legal entity) for compensation where they have suffered serious damage or distress as a result of the processing of their personal information;
- the right to complain to the ICO if the data subject believes that the church has not handled their personal data in accordance with data protection law.

<u>Principle 7</u>: Processing be must carried out securely

The principle states that "*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*."

Churches must therefore 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 means that churches will need to consider the following as appropriate:

- storing paper based information in secure, lockable cupboards;
- 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 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. This can make the difference between a church having to report a data breach and not having to do so – see Data Breach Reporting below.

Below is a link to a guide published by the ICO which provides suggestions in relation to how organisations can improve their IT security. Although aimed at small businesses, it provides useful guidance for all organisations:

https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

An important element of the 'organisational' element of Principle 7 is that all staff (including volunteers) who handle personal data are trained 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. **The ICO expects this to be held at regular intervals.** See Annex 4 for some suggestions about training

<u>Data Breach Reporting</u>

Under current data protection law, it is not mandatory that any breach of data protection law is reported. However, the ICO would expect all serious breaches to be reported. The ICO has produced helpful guidance on this topic in order to assist data controllers such as churches with the decision as to whether they currently need to report a data breach and how to deal with breaches once they have been identified.

It is important to bear in mind that under the GDPR there is a greater responsibility to report data security breaches to the ICO within 72 hours.

You have to notify the ICO of a breach which is likely to result in a risk to the rights and freedoms of individuals and, if unaddressed, such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Organisations (including churches) can be fined if they fail to do so.

Data breaches therefore 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.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

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

Principle 8: ensuring that personal data is not transferred to a country or territory outside of the European Economic Area (EEA) unless that country or territory provides an 'adequate' level of protection for the processing of individuals' personal data

The countries within the EEA (which includes the countries of the European Union plus Norway, Liechtenstein and Iceland) have their own versions of the UK's Data Protection Act 1998, as they are all based on a European Directive which was passed in 1995, and so any transfer of someone's personal data to any of these countries (e.g. by email or by post, for example) will be deemed 'adequate.' In addition to this, there are a number of other countries (on the nick-named 'white list' of countries which have been deemed to offer an adequate level of protection for EU data subjects' privacy rights (including Canada, New Zealand and Switzerland for example)– see link below:

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Where a church wishes to transfer the personal data of a church member outside of the EEA and the country of destination is not on the 'white list', it would be a breach of data protection law to transfer that data unless in accordance with the rules on 'international data transfers.' Such transfers can be made but it does require an extra level of compliance to be adhered to.

There are a number of 'exceptions' to the above rule and one of these is based upon the data subject's consent so that, in certain circumstances, where the church wishes to send information about, for example, a member in the UK to church members working abroad, the church could ask for the UK member to consent to this transfer. It is recommended that legal advice be taken as there are a number of additional factors which need to be taken into account in this scenario.

The other circumstance in which Principle 8 might affect churches is where a church wishes to use the services of a cloud provider to store personal data of its data subjects.

In this case it will be essential for the church to carry out due diligence on the cloud provider before signing any contract. This should include making enquiries as to the geographical location of the cloud provider's computer servers or data centre. If they are located in a country outside of the EEA then the solution should not be adopted by the church unless the cloud provider can demonstrate compliance with UK data protection law. It is recommended that churches take legal advice where this is an issue. In addition, cloud providers are usually regarded as data processors for the personal data of the data controller which they store, with attendant compliance implications for the service contract with that provider.

8. SUBJECT ACCESS REQUESTS

The Data Protection Act gives all data subjects the right of access to their personal data. An individual is also entitled to be informed by the data controller whether their personal data is held, and if that is the case, to require the data controller to give a description of the personal data, the purposes for which they are being held and who will see that data. A data controller is not obliged to supply this information unless a request is received in writing (which includes email). Currently such a request must be answered within 40 calendar days and payment of a fee of up to £10 may be requested before the information needs to be provided.

From May 2018 (when the GDPR come into force) the £10 fee will no longer apply and the statutory period for dealing with subject access requests is to be reduced to one month. This means that you have just one month from the date on which you receive the request until you have to provide the person submitting the request with the information you believe they are entitled to see,

Whilst is it is rare that churches will receive such requests it certainly can't be ruled out as a possibility. 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 BU Data Protection Officer is willing to advise any BUGB member church which receives a Subject Access request. There is also a very useful guidance document on the ICO website, the Subject Access Code of Practice which can also be accessed from the link below. However, legal advice should be sought in all cases where there is uncertainty regarding the information to be provided to the requester

https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf

It is important to bear in mind that the subject access right entitles the data subject to copies of only their own personal data. 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 Y (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.

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 print off 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 legal 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.

9. 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 Annex 3

10. A FEW LAST THINGS TO CONSIDER

Publishing information on the Church Website

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. 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.

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) would be the sensitive personal data of the individuals concerned.

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. 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. See Annex 3

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, in general terms, the GDPR requires all data controller organisations (and data processors) to maintain more detailed records than at present.

Data Protection Policy

All churches should have an internal 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 which can be found 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. The ICO has further guidance on this topic on their website which can also be accessed from the link below:

https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

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 log in relation to subject access requests is advisable.

11. 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 the eight principles of Data Protection.*
- *If you are unsure please read Sections 2.1 – 2.4 (pages 3-4) 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 2.5 (page 5)*

E: Does the church use Data Processors? (See section 2.6 for more information)
- *If the answer is **YES** then please ensure you read Annex 2 about Data Processor contracts and take appropriate action.*

F: Has the church already notified the ICO that they are a Data Controller?
- *If the answer is **YES** then you will be notified directly about new arrangements and fees*
- *If the answer is **NO** you should consider whether you are exempt from notification/registration (Read page 6 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) will need to be updated to be compliant with GDPR*
- *If the answer is **NO** then you will need to start to do this.*

Either way you should read Section 5.1 and look at the examples in Annex 3

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 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 at* www.baptist.org.uk/gdpr

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?*

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 4 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 (40 days for any request received before 25 May 2018)

M: Do you undertake any form of 'direct marketing' by email or text message? (See section 9)

- *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 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.*

P: Is the church undertaking any high-risk processing of sensitive personal data which might require a Data Protection Impact Assessment? (See section 5.4 for more information)

- *If the answer is **YES** please read Section 5.4 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 1 THE PROVISIONS CURRENTLY GIVING AN EXEMPTION FOR CHURCHES FROM THE NEED TO NOTIFY THE INFORMATION COMMISSIONERS OFFICE (Only valid until 25 May 2018)

Churches are currently exempted from notification if the processing

(a) is carried out by the church, that is under the direction of the Charity Trustees or others appointed by the Church Members' Meeting (*the Data Controller*)

(b) is for the purposes of establishing or maintaining membership of the church or for support of the church, or for administering activities for individuals who are either members of the church or have regular contact with it; **(this is the exempt purpose)**

(c) is of *personal data* in respect of which the *data subject* is:-

(i) a past, existing or prospective member of the church or its associated organisations;

(ii) any person who has regular contact with the church or its associated organisations in connection with the purposes: or

(iii) any person the processing of whose *personal data* is necessary for the exempt purposes

(d) is of *personal data* consisting of the name, address and other identifiers of the *data subject* or information as to:

(i) eligibility for membership of the church or its associated organisations;

(ii) other matters the processing of which is necessary for the exempt purposes;

(e) does not involve disclosure of the *personal data* to any third party other than:

(i) with the consent of the *data subject*; or

(ii) where it is necessary to make such disclosure for the exempt purposes: and

(f) does not involve keeping the *personal data* after the relationship between the *data controller* and the *data subject* ends, unless and for so long as it is necessary to do so for the exempt purposes.

FOR DETAILS OF THE EXEMPTIONS WHICH WILL APPLY FROM 25 MAY 2018 PLEASE SEE SECTION 3 ON PAGE 6

ANNEX 2 DATA PROCESSOR CONTRACTS

There is currently a requirement for a data controller to have a contract in writing with its data processors and this 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. However, under the GDPR, there will be a legal requirement to include a great many more clauses in order to ensure that the data processor entity carries out processing which is compliant with the new law. Legal advice should be taken in this regard as it is recommended that all contracts with third party data processor suppliers are reviewed before the 25th May 2018 as these will need to be compliant with the GDPR at that date.

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 SAMPLE PRIVACY NOTICES FOR COLLECTING INFORMATION

ANYTOWN BAPTIST CHURCH

Sample Privacy Notice to include on a form for collecting information from church members

Under Data Protection legislation the church Charity Trustees of Anytown Baptist Church are the Data Controller and can be contacted by ringing xxxxx xxxxxxxx or emailing trustees@anytownbaptist.org

We are collecting this information to enable the church to keep in touch with you and provide pastoral support as appropriate. Data Protection legislation allows us to process this information as we regard it as being in the church's legitimate interest.

Your name and contact details will be entered into our church database which is held on the church office computer which is password protected and accessed only by the Ministers, Church Secretary and Church Administrator. Your contact details will be removed from the database once you are no longer a member of the church – unless you ask to remain as one of our "church friends".

If you serve Anytown Baptist Church as a member of staff or in a key role then we will pass on your name and contact details to the Baptist Union of Great Britain and/or the Anywhere Baptist Association (of which we are members) to enable them to send you information relevant to your role. We will always ensure you are aware of what information is being shared with them and you will be able to decide which contact details are shared.

We would like to include your name and contact details in our Church Directory which will be distributed by email to all Church Members and in hard copy as appropriate. A copy will also be kept in the church office. We will not give copies of the Church Directory to anyone else. If you are happy for your details to be included please indicate where asked to do so below. You can ask for your details to be removed at any time.

To enable us to provide adequate pastoral support to you and your family, one of the Ministers may record information which may be regarded as sensitive. This information will be stored (in password protected documents) on the church computer but the password will only be known by the Ministers. This information will NOT be disclosed to anyone else without your consent.

You have the right to ask to see any information we hold about you (including the pastoral support information) by submitting a 'Subject Access Request' to the Church Secretary. You also have the right to ask for information which you believe to be incorrect to be rectified.

If you are concerned about the way your information is being handled please contact us using the above details. If you are still unhappy you have the right to complain to the Information Commissioners Office.

ANYTOWN BAPTIST CHURCH

Sample Privacy Notice to include on a form for collecting information about children attending a Holiday Club

Under Data Protection legislation the church Charity Trustees of Anytown Baptist Church are the Data Controller and can be contacted by ringing xxxxx xxxxxxxx or emailing trustees@anytownbaptist.org

We are collecting this information to enable the church to run the Holiday Club safely and ensure we can contact you (or other nominated adult) in case of an emergency. Data Protection legislation allows us to process this information as we regard it as being in the church's legitimate interest. If you are unable to supply the information requested then we will be unable to accept your child at our Holiday Club.

The information you supply will be held in paper form in a folder which will be kept in a securely locked cupboard in the church office. Only the Ministers and the Holiday Club leaders will have access to this information.

The information will be kept for three years from when the form was completed unless a safeguarding incident or concern is raised in which case it will be held for 75 years. If you have ticked the box asking us to keep you informed about future activities, we think your child might be interested in attending we will retain your details for the sole purpose of notifying you of such events. We will NOT pass on this information to anyone else. You have the right to ask to be removed from this circulation list at any time.

If you are concerned about the way your information is being handled please contact us using the above details. If you are still unhappy you have the right to complain to the Information Commissioners Office.

ANYTOWN BAPTIST CHURCH

Sample Privacy Notice to include on a form requesting details from a new (or potential) employee

Under Data Protection legislation the church Charity Trustees of Anytown Baptist Church are the Data Controller and can be contacted by ringing xxxxx xxxxxxxx or emailing trustees@anytownbaptist.org

We are collecting this information to enable us to enter into a contract of employment with you. If you are unable to provide this information then we will be unable to enter into that contract.

The information you supply in this form will be

- Held on the church office computer which is password protected and accessed only by the Ministers, Church Secretary and Church Administrator.
- Destroyed six months after you leave our employment

We will be undertaking performance appraisals as part of your employment and copies of the reports from these (along with all documents supplied as part of your application) will be kept in a password protected section of our church computer which can only be accessed by the Senior Minister as your Line Manager. If appropriate, information from these documents may be shared with other charity Trustees but will NOT be shared with anyone else without your consent.

You have the right to ask to see any information we hold about you by submitting a 'Subject Access Request' to the Church Secretary. You also have the right to ask for information which you believe to be incorrect to be rectified.

If you are concerned about the way your information is being handled please contact us using the above details. If you are still unhappy you have the right to complain to the Information Commissioners Office.

ANNEX 4

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 eight 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)

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

---

ANNEX 5 SAMPLE DATA PROTECTION POLICY FOR CHURCHES

This can be found via www.baptist.org.uk/gdpr

Association Trust Company	Contact
Baptist Union Corporation Ltd **East Midland Baptist Trust Company Ltd** **North Western Baptist Association** **South West Baptist Trust Corporation** **Yorkshire Baptist Association**	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 BMS International Mission Centre 24 Weoley Park Road Selly Oak Birmingham B29 6QX Telephone: 0121 472 4986
London Baptist Property Board	London Baptist Association 235 Shaftesbury Avenue London WC2H 8EP Telephone: 020 7692 5592
West of England Baptist Association	West of England Baptist Association The Old Forge Broom Hill Stapleton Bristol BS16 1DN 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 deal with churches that are in trust with the East Midland Baptist Trust Company Limited, the North Western Baptist Association, South West Baptist Trust Corporation and Yorkshire Baptist Association (Incorporated).

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:
The Baptist Union Corporation Ltd, Baptist House, PO Box 44, 129 Broadway, Didcot, Oxfordshire OX11 8RT England

A Company Limited by Guarantee. Registered in England No 32743. Registered Charity No 249635

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: buc.corp@baptist.org.uk
Website: www.baptist.org.uk
Registered Charity Number: 1125912

Date of Issue: May 2018