# New Data Protection Laws

# A UK General Data Protection Regulation (UK GDPR) Toolkit for Parishes in the Diocese of Southwark

## Version 1.3 January 2021

**Contents**

[Foreword from Bishop Christopher 3](#bookmark0)

[A note from the Diocesan Legal Team 3](#bookmark1)

[Thank you from colleagues at Trinity House 3](#bookmark1)

PART ONE [A brief introduction to the UK GDPR 4](#bookmark3)

[Underlying Principles 5](#bookmark5)

[The key changes 5](#bookmark6)

[Who will be affected? 5](#bookmark7)

[A gear shift in risk 6](#bookmark8)

[Examples of failures to comply with the new law 6](#bookmark9)

[Key Points for Parishes 6](#bookmark10)

[Next Steps 7](#bookmark13)

[PART TWO A detailed guide to the UK GDPR 8](#bookmark14)

[Why implement new legislation? 8](#bookmark16)

[Consent, Rights and Accountability 8](#bookmark17)

[What is the scope of the UK GDPR? 8](#bookmark18)

[What’s new? Legal rights of Data Subjects 9](#bookmark19)

[Accountability - What is it and how do I comply? 9](#bookmark20)

[What is a privacy notice? 10](#bookmark21)

[What are the data subject rights? 10](#bookmark22)

[Lawful basis for processing 11](#bookmark23)

[How do I show that I am processing personal data lawfully? 13](#bookmark24)

[When am I allowed to process ‘sensitive personal data’? 13](#bookmark25)

[What do I need to do if there is a data breach? 14](#bookmark26)

[What’s new? Notifying breaches 14](#bookmark27)

[Where to use consent 15](#bookmark28)

[Can existing consents be relied on? 15](#bookmark29)

[What’s new? Marketing consents 16](#bookmark30)

[The need to document your data processing 16](#bookmark31)

[Do I need to register or pay a fee to the ICO? 16](#bookmark32)

[Processing personal data about children 17](#bookmark33)

[Will I need to appoint a Data Protection Officer? 17](#bookmark34)

[Deciding who will be responsible for Data Protection in the Parish 17](#bookmark35)

[CCTV 17](#bookmark36)

[What’s new? CCTV 18](#bookmark37)

[Key data - What to keep and for how long 18](#bookmark38)

[What about contracts with suppliers and partners? 18](#bookmark39)

[What’s new? Contracts with data processors and joint controllers 18](#bookmark40)

[What is a Data Protection Impact Assessment (DPIA) and when is it needed?](#bookmark41) 19

[Appendix 1 – A summary of the legislation changes 20](#bookmark42)

[Appendix 2 – UK GDPR Action Plan Checklist 22](#bookmark43)

[Appendix 3 – Audit Questionnaire 24](#bookmark44)

[Appendix 4 – Consent Form 27](#bookmark45)

[Appendix 5 – Privacy Notice 28](#bookmark46)

[Appendix 6 – DPIA Assessment Checklist 32](#bookmark47)

# 

# Update: January 2021

## This document was created ahead of the introduction of the new GDPR legislation in 2018. Since 1 January 2021, the UK is now considered a third country outside the EEA however the legislation introduced in 2018 remains largely unchanged by the UK’s departure from the EU. The content of this document has been updated to reflect that the law covering GDPR in the UK is now referred to as UK GDPR, however the principles and aims of the law remain the same.

# Foreword from Bishop Christopher

Dear Brothers and Sisters in Christ,

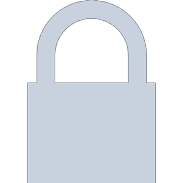
The General Data Protection Regulations (GDPR) which came into force on 25 May 2018 are important for all of us and must influence the way in which we handle personal information and data stored on individuals. So, I am pleased to say that the team at Trinity House have worked hard with our lawyers, Winckworth Sherwood, in order to make sure that we can provide you with the best possible advice and information on what you need to do as a parish and here it is. I am delighted to be able to commend this document to you.

In this guide you will find most of what you need to know to ensure that your parish and deanery is fully compliant with the needs of GDPR, but should you have any questions please do contact [data@southwark.anglican.org](mailto:data@southwark.anglican.org)

Thank you for all that you do to make our parishes such vibrant and welcoming places as we share the Good News of God in Christ with our communities.



# A note from the Diocesan Legal Team



## We have designed this GDPR Toolkit to take account of the National Church guidance, and to develop it further so that it is of greater relevance to parishes in the Diocese of Southwark. We therefore suggest that you apply this GDPR Toolkit in place of the National Church guidance. It is important that you follow this GDPR Toolkit carefully and use the checklist and forms contained within it to ensure the parish, and the church, is compliant with the law.

# Thank you from colleagues at Trinity House

## Over the past months we have worked with and supported parishes across our Diocese as they have implemented GDPR and have received helpful feedback from workshops, meetings, phone calls and emails. Following this feedback we have worked with our Diocesan Legal Team to produce this updated version of the toolkit which we hope will continue to support your implementation of GDPR.

## As always, please do contact us if you have further comments, suggestions or questions: [data@southwark.anglican.org](mailto:data@southwark.anglican.org)

# PART ONE

# A brief introduction to the UK General Data Protection Regulation (UK GDPR)

## The Data Protection Act 2018 (DPA 2018) has the effect of applying the GDPR to the UK. Together, the DPA 2018 and GDPR replace and update the Data Protection Act 1998 (DPA 1998) and give individuals more rights and protection regarding how their personal data is used by organisation. Parishes must comply with the requirements, just like any other organisation.

## Key terms explained:

## **Personal data**is information about a living individual which is capable of identifying that individual. E.g., names, email addresses, photos.

## **Processing**is anything done with/to personal data, including storing it.

## The **data subject**is the person about whom personal data is processed.

## The **data controller**is the person or organisation who determines the how and what of data processing. In a parish this is usually the PCC and Incumbent.

## A **data protection officer**is unlikely to be needed in parishes.

## **Direct marketing** is defined as the communication of advertising or marketing material which is directed to particular individuals.

## From 1st January 2021, the ‘UK GDPR’ has replaced the GDPR as the UK’s data protection law. The UK GDPR (which is currently substantially similar to the EU’s GDPR) is brought into force by the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

## The Information Commissioner’s Office (ICO) is the organisation responsible for the implementation of UK GDPR with new powers to fine organisations that do not comply.

## This Toolkit contains a **checklist** which covers the actions outlined within it to help you monitor progress. It may be helpful to start by carrying out a **data audit** - you may be surprised at just how much personal data is stored and processed around the parish. A template questionnaire to help you do this can be found in Appendix 3.

## One of the big changes in the law is you may need to obtain **consent** from the data subject for certain processing of their data. This will apply to members of the church community if they are sent advertising or fundraising information by email or postal address which is defined as **direct marketing** by the new regulations.

## Taking part in certain activities or performing roles will require personal data to be processed that does not require the data subject’s consent. For example, the processing of data to comply with Southwark Diocese “A Safer Church” guidance is done under the legitimate interests’ basis of processing personal data.

## We provide a sample **Privacy Notice** in this UK GDPR Toolkit in Appendix 5. We suggest that you read through the template, use it to review your current data processing and adapt it to produce your own Privacy Notice. This should be made available to members of the church with whom you communicate regularly.

## You can use the Consent Form in Appendix 4 to capture consent required for any direct marketing communications to your members.

## Finally, remember that this is a principles-based legislation so you will need to describe how you are complying with those principles within your Parish.

# Underlying Principles

## The UK GDPR has a number of underlying principles. These include that personal data:

### Must be processed **lawfully, fairly and transparently**.

### Is only used for a **specific processing purpose** that the data subject has been made aware of and no other, without further consent.

### Should be **“adequate, relevant and limited”** i.e. only the minimum amount of data should be kept for specific processing.

### Must be **accurate** and where necessary **kept up to date**.

### Should **not be stored for longer than is necessary**, and that **storage is safe and secure**.

### Should be processed in a manner that ensures **appropriate security and protection**.

# 

# The key changes

### Changes to **how consent can be obtained** from data subjects for the use of their data. For example, data subjects have to explicitly ‘opt in’ to allowing their data to be shared, and it must be made clear for what purpose their data is being used.

### **Data subjects have new rights**, such as **data portability** and the **right to be forgotten**.

### **Data must only be used for the purpose it was gathered** for and should be deleted when it is no longer needed for that purpose.

### **Sanctions over sharing data outside the European Economic Area (EEA) will be strengthened.** This requires organisations to ensure adequacy decisions or appropriate privacy safeguards are in place with organisations holding data outside the EEA.

### All **new and existing staff** and other key data users **must have suitable training** and awareness as well as additional sources of guidance and support when required.

### Conducting **Data Protection Impact Assessments** (DPIAs) in order to design data privacy into any new systems and processes will often be mandatory. For example, if new technology is deployed, where there is processing on a large scale of ‘special category’ personal data (formerly sensitive personal data), or if profiling is performed which will have an impact on individuals.

### Some organisations (but highly unlikely to apply to parishes) will need to appoint a **Data Protection Officer**.

### **Data breaches must be reported** where this is required, to the Information Commissioner’s Office **within 72 hours** of the breach.

### A new **principle of “accountability”** puts the burden on PCCs and Incumbents for compliance, requiring them to produce and maintain documents that demonstrate what actions have been taken to achieve compliance.

# Who will be affected?

## The quick answer is every organisation in the UK that handles personal data. These new data protection rules will apply both to the personal data of individuals living in the UK and also to the export of personal data to countries outside the UK.

## The UK GDPR applies to data controllers (people who specify how and why personal data is processed) and data processors (those who carry out the processing). Controllers must ensure that their processors comply with the legislation and the processors must also keep records of their processing activities. The new law means that both parties face a more stringent level of liability than they do under the existing law.

# A gear shift in risk

## The huge increase in fines (from £500,000 in the UK to the greater of €20 million or 4% of global annual turnover) places significantly additional risk on organisations. The UK GDPR allows users to claim damages in the instance of data loss as a result of unlawful processing, including collective redress, the equivalent of a US-style class action lawsuit.

## Lastly, it is worth remembering the additional costs that can be incurred as well. A breach of the UK GDPR could expose organisations to a need to spend substantial time, money and effort on responding to requests for information, enforcement notices, internal and external press releases and minimising any negative publicity.

# Examples of failures to comply with the new law

## For a failure to get parental consent where personal data are collected about a child in the process of providing an "information society service" (e.g. online magazine/newspaper, buying/selling online), a fine of up to 10 million Euros or 2% of the data controller's annual worldwide turnover for the previous year. For a failure to provide adequate information to data subjects or to allow subject access, or to comply with the right of erasure (see above), a fine of up to 20 million Euros or 4% of the data controller's annual worldwide turnover for the previous year.

# Key Points for Parishes

## UK GDPR is a principles based legislation with a requirement for organisations to demonstrate how they are complying. Within a Parish the Incumbent and PCC as joint data controllers are responsible for demonstrating compliance with UK GDPR.

## In some cases the UK GDPR principles will be implemented differently to suit different parishes, for examples in how prayer lists are managed. In all cases our rule of thumb is to ensure that you would be happy for your own data to be treated in such a way and to ensure that data subjects are not surprised with how their data is processed.

## For direct marketing which includes advertising and fundraising letters that are sent to people’s email address or postal address you will need to ensure you have obtained opt in consent from the recipients. Consent for one element of data processing does not give you permission to do anything else with it so ensure that you are clear on what the consent you obtain is for. You can collect consent verbally, but you must record it and make a provision for people to withdraw their consent.

## For much of the processing of personal data within the Parish there will be another basis for processing the data such as **legitimate interest** (e.g. fulfilling safeguarding policy), requirement to fulfil a service (e.g. Hall hire) or a **legal requirement** (e.g. processing of marriage banns) so you will not need to rely on consent for most cases.

## Parishes must make a **privacy notice** available to their congregation normally via their website and with a hard copy within the building. The privacy notice should provide a point of contact in case someone would like to raise an issue, request processing their data is stopped or complain.

|  |
| --- |
| Next Steps:Read the summary of the main differences between the UK GDPR and the current law in Appendix 1 – A summary of the legislation changes.See the Action Plan checklist in Appendix 2 – UK GDPR Action Plan Checklist. This sets out a detailed step by step plan to help you ensure compliance.Review what data you hold, how you store it, and what basis you have for processing it using the audit questionnaire in Appendix 3. This will help you map what personal data you process and where it is.Review and refresh your existing consents. Use the example Consent Form to collect consent from existing church-goers who receive your communications.Develop your Data Privacy Notice using the template in Appendix 5.Use the Data Protection Impact Assessment (DPIA) checklist in Appendix 6 to help you decide where you will need to carry out a Data Protection Impact Assessment. Note you will not usually need to carry out a DPIA for existing systems or processes unless you upgrade or substantially overhaul these. |

# PART TWO

# A detailed guide to the UK GDPR

## 

# Why implement new legislation?

## The UK GDPR is not intended to restrict the processing of personal data, but rather align it to the modern digital world and ensure that such processing is done in a way that protects the data subject’s rights.

# Consent, Rights and Accountability

## Church members will need to give their consent before you send them certain communications. This needs to be clear and unambiguous - some form of positive action to 'opt-in’. You will need to gather this consent. We have included a Consent Form to go with the template General Privacy Notice but you can include the consent language in other forms you use.

## Data subjects have a number of rights, including that of knowing how data is used by the data controller, of knowing what data is held about them, of correcting any errors and generally the right 'to be forgotten' under certain circumstances. Data controllers, such as the PCC and Incumbent, will need to make provision for people to exercise these rights.

## The UK GDPR introduces a **stronger requirement on accountability** for data controllers. This means that you must be able to show that you are complying with the principles by providing evidence.

# What is the scope of the UK GDPR?

## Many of the existing core concepts under the previous DPA 1998 are reflected in the UK GDPR. Familiar concepts of personal data, data controllers and data processors are broadly similar in both the DPA and the GDPR. Currently there is a very broad definition of ‘processing’ under the DPA and this captures the retrieval, management, transmission, destruction and retention of personal data. This will continue to be the case under the UK GDPR as well.

## Organisations which are not in the EEA (now including UK based organisations) still have to comply with the EU GDPR. Non-EEA organisations that do business in the EEA with EEA data subjects’ personal data should designate a representative in the EU, as a point of contact for supervisory authorities (who are responsible for ensuring compliance with the EU GDPR) and data subjects. In the UK, the supervisory authority is the Information Commissioner’s Office (ICO). In addition, UK organisations sending data to EEA or other third countries or territories will continue to be able to rely on the same mechanisms as under the EU GDPR.

|  |  |
| --- | --- |
| What’s new? Legal rights of Data Subjects | |
| **Data Protection Act 1998** | **GDPR / DPA 2018** |
| Under the old law a Data Subject could request a copy of their data (Subject Access Request) on payment of a nominal fee and has a common law right of erasure or rectification of their personal data. | Under the UK GDPR, these rights are explicit and no longer require a fee. In addition, there is a right to have personal data extracted in an electronic portable format that will allow switching between different service providers. There are new rights to erase data too (if it is no longer needed). |

## Both UK and international organisations need to understand how data flows within the organisation and outside particularly when the data crosses international borders.

## Parishes should review their current policies and procedures in place in light of the flow of data across the parish and around the diocese.

*Under the* *UK GDPR,* ***personal data*** *now includes information relating to a living person, who can be identified* ***directly or indirectly*** *by such information (e.g.  name, ID number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic or social identity of that person). Under the UK GDPR,* ***special category personal data*** *(which has a higher threshold of protection) includes genetic data, biometric data and data concerning sexual orientation and sex life, in addition to the previous categories such as religious belief, race/ethnic origin, trade union membership, health and criminal records.*

# Accountability - What is it and how do I comply?

## The new accountability principle means that you must be able to show that you are complying with the principles set out on page 6 of this guide. In essence, you cannot just state you are compliant; you have to prove it and provide evidence. To do this there are a number of actions you should take, such as documenting the decisions you take about your processing activities and various other ways that show compliance - such as attending training, reviewing any policies and auditing processing activities.

# What is a privacy notice?

## The transparency requirements under the UK GDPR require organisations to provide individuals with extensive information about how their personal data is collected, stored and used. This information must be easily accessible, transparent and presented using clear and plain language. In practice, this means that parishes will need to include more information in their privacy policies, as well as retaining more detailed records of their data processing activities in relation to their role holders, employees, and other members of the church.

# What are the data subject rights?

## The new data subject rights may present practical issues for parishes, especially where personal data is spread across multiple or complex systems. PCCs will need to update the relevant policies and procedures to reflect the UK GDPR requirements. PCCs should review existing procedures in place when responding to data subject access requests to ensure the new time scales can be met.

## Generally, the rights of individuals that are granted under the UK GDPR are the same as under the 1998 Data Protection Act but with some significant additions. The UK GDPR includes the following rights for individuals, which are briefly explained here:

### **The right to be informed**

### Individuals continue to have a right to be given "fair processing information", usually through a privacy notice. Under the UK GDPR there is additional information that you will need to supply. For example, you will have to explain the lawful basis for the processing of their data; your data retention periods (how long you keep it for) and that individuals have a right to complain to the ICO if they think that there is a problem in the way that you deal with their personal data.

### **The right to access (includes subject access requests)**

### Under the UK GDPR the right of data subjects to request information about the personal data processed by organisations remains largely the same. However, under the new regime organisations must respond without undue delay and in any case within one month of receipt of the request. Additionally, the £10 fee for making a request has been abolished which is likely to lead to a greater number of requests. It is estimated that 25% of requesters withdrew or did not pursue their request when asked to fill in a form and pay the £10 fee.

### Organisations can refuse or charge a "reasonable fee" for requests that are manifestly unfounded, excessive or repetitive. If you do refuse a request you must tell the individual why and that he/she has the right to complain to the ICO or go to court.

### **The right to rectification (or correction)**

### Individuals have the right to have their personal data corrected (rectified) if it is inaccurate or incomplete. If the data has already been given to third parties, parishes must tell those third parties of the correction. PCCs must also tell the individuals about the third parties to whom the data has been given.

### **The right to erasure (also known as the right to be forgotten)**

### Data subjects have the right to request the removal or erasure of their personal data, for example if it is no longer necessary to process their data, the individual objects to such processing and/or the individual withdraws consent. Not only will organisations need to comply with such requests but they will also need to ensure that any third party with whom the data was shared also deletes such data.

### This does not mean that a person can immediately request that his/her personal data is deleted. If the purposes for which the data was collected still exist, then a person will not be able to request the deletion of that data, unless it was given by consent and they are withdrawing their consent. This is one reason why consent is not the appropriate lawful basis for data processed in connection with a person’s role in the Church. For instance, safeguarding information about an individual cannot be deleted if the retention is still necessary, reasonable and proportionate, e.g. to protect members of the public from significant harm. Another example is that some financial information, such as that relating to Gift Aid, cannot be deleted immediately due to financial auditing regulations.

### **The right to restrict processing**

### Individuals have the right to restrict processing of their personal data in certain circumstances (for instance if a person believes his/her personal data is inaccurate or he/she objects to the processing). If processing is restricted, you can still store the data but cannot otherwise use the data.

### **The right to data portability**

### Data subjects have the right to request that their personal data be provided to them (or a third party) in a machine readable portable format free of charge. Parishes should consider how and where the personal data is held and if such data can be easily transferred in a safe, secure manner without impacting the usability of such data by the data subject. The Parish will need to comply with such requests without undue delay, and in any event within one month.

### This is a new right introduced by the UK GDPR. Individuals have the right to obtain and reuse personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT system to another. It only applies in certain circumstances and is highly unlikely to affect parishes.

### **The right to object**

### Individuals have the right to object to processing in certain circumstances, e.g. if a parish has relied on legitimate interest to process data without consent and an individual is not happy with this they have the right to object to the parish processing their data.

### **The right not to be subject to automated decision-making including profiling**

### The UK GDPR provides protection against the risk that a potentially damaging decision is taken without human intervention. This right is similar to that contained in the Data Protection Act 1998.

# Lawful basis for processing

## The UK GDPR sets out **six lawful bases** for processing data. Unless an exemption applies, **at least one of these must apply in all cases**. It is possible for more than one lawful basis to apply at the same time.

## One of the new requirements for your Privacy Notice is that you must set out in the Privacy Notice which lawful basis you are relying on. In the sample Privacy Notice in Appendix 5 you will notice that we have opted to rely on more than one lawful basis. For most parishes, the relevant ones will be: 1 Consent, 2 Legitimate interests, 3 Contractual necessity (for example with contractors), 4 Compliance with legal obligation (for example processing wedding banns).

## he six lawful bases for processing personal data under the UK GDPR are:

###### Consent

## A controller must be able to demonstrate that consent was given. Transparency is key: consents given in written declarations which also cover other matters must be clearly distinguishable, and must be intelligible, easily accessible and in clear and plain language. Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject’s wishes – either by a statement or by a clear affirmative action.

###### Legitimate interests

## This involves a balancing test between the controller (or a third party’s) legitimate interests and the interests or fundamental rights of and freedoms of the data subject – in particular where the data subject is a child. The privacy policy of a controller must inform data subjects about the legitimate interests that are the basis for the balancing of interests.

## The balancing test for legitimate interest:

### Identify your legitimate interest

### What is the purpose of the processing and why is it important?

### Carry out a necessity test

### Is there another way of achieving your legitimate interest? If the answer is no, then it is necessary.

### Carry out a balancing test

### Does the data subject’s right override the legitimate interest?

### Consider the nature of the processing, its impact and what mitigation you can put in place.

### What possible negative impacts for privacy could there be.

###### Contractual necessity

## Personal data may be processed if the processing is necessary in order to enter into or perform a contract with the data subject (or to take steps prior to entering into a contract).

###### Compliance with legal obligation

## Personal data may be processed if the controller is legally required to perform such processing (e.g. complying with the provisions of the Church Representation Rules; reporting of race or ethnic origin or gender pay data).

###### Vital interests

## Personal data may be processed to protect the ‘vital interests’ of the data subject (e.g. in a life or death situation it is permissible to use a person’s medical or emergency contact information without their consent).

###### Public interest

## Personal data may be processed if the processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

# How do I show that I am processing personal data lawfully?

## For example: The lawful basis for processing the personal data contained in applications for enrolment on the Church Electoral Roll is ‘compliance with a legal obligation’. (This is because this processing activity is a requirement of legislation, i.e. The Church Representation Rules). However, disclosure of a person’s details to a third party (e.g. ‘The Friends of the Church’ – which falls outside Church Representation Rules’ provisions) would require the individual’s consent.

# When can I process ‘special category data’ (sensitive personal data)?

## Sensitive personal data, which the UK GDPR refers to as ‘special category data’, means information about a person’s racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, criminal history and allegations. The UK GDPR adds the following new additional categories: genetic data, biometric data and sexual orientation.

## To process sensitive personal data one of the following criteria should apply, however please note that:

### more than one of the criteria below can apply at the same time.

### data controllers need to establish a lawful basis for processing any personal data (see previous section - Lawful basis for processing)**and,** if they are processing sensitive personal data they must also establish that **at least one** of the criteria below applies:

###### Explicit consent of the data subject has been obtained (which can be withdrawn).

###### Employment law – if necessary for employment law or social security or social protection.

###### Vital interests – e.g. in a life or death situation where the data subject is incapable of giving consent.

###### Charities, religious organisations and not for profit organisations – to further the interests of the organisation on behalf of members, former members or persons with whom it has regular contact such as donors. Note, however, that explicit consent is required for the personal data to be shared with a third party.

###### Data made public by the data subject – the data must have been made public ‘manifestly’.

###### Legal claims – where necessary for the establishment, exercise or defence of legal claims or for the courts acting in this judicial capacity.

###### Reasons of substantial public interest – where proportionate to the aim pursued and the rights of individuals are protected.

###### Medical diagnosis or treatment – where necessary for medical treatment by health professionals including assessing work capacity or the management of health or social care systems.

###### Public health – where necessary for reasons of public health e.g. safety of medical products.

###### Historical, statistical or scientific purposes – where necessary for statistical purposes in the public interest for historical, scientific research or statistical purposes.

## In a parish context the most relevant lawful bases for processing under Special Category Data are likely to be 1 and 4, namely:

### Explicit consent from a person; or

### Where the processing is the legitimate activity of the organisation (ours being a ‘religious organisation’) and relates to either members or former members or to individuals with whom there is regular contact, but is not disclosed to any third parties without explicit consent.

## “Explicit consent” language is included in the Privacy Notice in Appendix 5 as this allows data to be shared within the church.

# What do I need to do if there is a data breach?

|  |  |
| --- | --- |
| What’s new? Notifying breaches | |
| **Data Protection Act 1998** | **UK GDPR / DPA 2018** |
| The notification of breaches to the ICO was effectively voluntary. | The UK GDPR contains an obligation to notify certain breaches to the ICO within 72 hours and in some cases data subjects will have to be notified too. |

## A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Under the DPA 1998 data breaches did not have to be routinely notified to the ICO or others (although the ICO recommends that it is good practice to do so). The UK GDPR makes informing the ICO and the individuals affected **compulsory** in certain circumstances;

## If there is likely to be a risk to the rights and freedoms of individuals, you must notify the ICO within 72 hours of becoming aware of the breach.

## If the breach is likely to result in a high risk to the rights and freedoms of the individuals, for example through identity theft, you must also notify the individuals affected without undue delay.

## Under the UK GDPR, you have to notify the ICO of a data breach within 72 hours of finding out about any such breach. It is important that those in the parish note this deadline and seek the advice of the Diocese about any suspected breaches without delay.

## More details can be provided after 72 hours, but before then the ICO will want to know within that time the potential scope and the cause of the breach, mitigation actions you plan to take, and how you plan to address the problem.

*Under the* *UK GDPR, organisations will be required to report a personal data breach that meets the reporting criteria, within 72 hours to the Information Commissioner. In line with the accountability requirements, all data breaches must be recorded along with details of actions taken. PCCs should ensure that there is a person, or a group of people, who are responsible for dealing with any data breaches which may occur, outline a response plan and set out a procedure detailing how, when and to whom data subjects should report data breaches.*

# Where to use consent

## The common area where we expect Parishes to use consent as the basis for processing data is where advertising or fundraising information is sent by email or postal address. This activity could be defined as direct marketing and would therefore require data subjects to provide their explicit consent.

## Where you rely on consent as the lawful basis for processing any personal data, you need to be aware that to be valid under the UK GDPR, consent must be freely given, specific, informed, unambiguous and able to be withdrawn. Also, you need to record how and when the consent was obtained (and review this over time). You will also have to tell individuals that they have the right to withdraw consent at any time and ensure that the procedure for withdrawing consent is just as simple as granting consent, (e.g. by sending an email or (un)ticking a box). You will need to keep records of all consents received and periodically review them (e.g. every 5 years) to ensure that they are still valid.

## You should note that consent may not be appropriate in every case. Remember there are other lawful bases for processing personal data. For example, you would not have to obtain consent to share the names of individuals on the readers rota or after service tea/coffee rota with other church members. In that instance, the information is shared with others in order to carry out a service to other church members or as part of the legitimate interest of the organisation which are different processing bases. Of course, if it was intended to share the names outside the church for another purpose, then you would need to obtain consent.

## The ICO notes that it is unlikely an employer would ever be able to show that an employee has given valid consent under the UK GDPR (i.e. that it has been freely given). Employers should therefore rely on one of the other conditions for processing rather than consent.

## Processing in order to prevent fraud, for direct marketing and for network security are all cited as examples of processing carried out for a legitimate interest. Sharing data within a group of undertakings may also be necessary for a legitimate interest.

# Can existing consents be relied on?

## As much of the data processed by a PCC in a parish is sensitive (relates to "religious belief”), if consent is needed this will have to be explicit consent. Consent requires "clear affirmative action". Silence, pre-ticked boxes, inactivity, or a history of processing without complaints will not constitute consent.

## You will have to make sure that any consent wording is sufficiently strong to allow you to show that the consent given is unambiguous and the person knows exactly to what he/she is consenting. You may need to review any existing consents you have on record to check whether they comply with the stricter rules under the UK GDPR. The basic rule is that if consent would have been valid under the UK GDPR when it was obtained you can rely on it, but if the consent was obtained using an opt-out box or is ambiguous you cannot rely on it now.

## Under the UK GDPR**, consent must be unambiguous**. Consent to process sensitive personal data must be explicit, however, consent to process other types of personal data does not need to be explicit. Consent must, however, still be specific, informed and active: silence or inactivity is not sufficient.

## **Consent must be freely given and individuals must be able to withdraw consent** (without detriment). Entering into a contract, or receiving a service, should not be ‘tied’ to the user giving consent to the processing of data which is not, in fact, necessary for the service to be delivered. Organisations must also seek separate consents for separate processing operations. These types of forced or omnibus consent mechanisms will not be valid: organisations will need to redesign consent mechanisms so as to present genuine and granular choice for consent to be valid.

|  |  |
| --- | --- |
| What’s new? Marketing consents | |
| **Data Protection Act 1998** | UK **GDPR / DPA 2018** |
| Under the old law an opt-out could be relied on by marketers for gaining marketing consent (for example, tick here if you don’t wish to receive offers, etc.). | Under the UK GDPR, marketing consent must be explicit and in a form of:time limited opt-inin plain languageeasy way to opt-out and to say no to profilingIf consent can’t be proved, an organisation could face a significant fine under the UK GDPR and an Enforcement Order to stop processing data. |

# The need to document your data processing

## Controllers and processors must keep and make available to supervisory authorities very comprehensive records of data processing which in turn requires organisations to start work on detailed data mapping exercises to determine what data is collected, how and why, where it is stored, who has access to it and whether there is a legal justification to process it.

# Do I need to register or pay a fee to the ICO?

## The need for data controllers to register with the Information Commissioner’s Office (ICO) is removed under the UK GDPR. However, under the Data Protection (Charges and Information) Regulations 2018 there is still an obligation to pay a data protection fee to the ICO.

## There is an exemption under the Data Protection (Charges and Information) Regulations 2018 which states that a not-for-profit organisation would not have to pay if it carries out processing for establishing and maintaining membership of an organisation, or for providing activities for individuals who are members or who have regular contact with it. Our legal advice is that this is unlikely to apply even to small parishes because the nature of the processing done will often go beyond this limit. For example, data processed when someone hires a church hall, or sensitive personal data held with relation to safeguarding, will be beyond the scope of this exemption. PCCs will still have to pay the fee.

## The fee should be paid to the ICO on an annual basis, based on the number of staff. If a parish has 10 members of staff or fewer, the fee will be £40. If it has between 11 and 250 members of staff, the fee will be £60. There is a £5 discount for all fees paid by direct debit.

## PCCs may have already registered with the ICO under the old law. If this is the case, PCCs do not have to pay the registration fee until their registration comes up for renewal. If a PCC has not previously registered, as data controllers, all PCCs must pay the fee as soon as possible. If you fail to pay the fee, the maximum fine which the ICO could give is £4,350 (150% of the highest fee).

The self-assessment tool below is provided by the ICO to highlight if an organisation is required to pay the fee:

<https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/>

The fee can be paid online here:

<https://ico.org.uk/for-organisations/data-protection-fee/>

# Processing personal data about children

## Under UK GDPR parental consent will be required for the processing of personal data of children under age 16. EEA Member States may lower the age requiring parental consent to under 13. The DPA 2018 adopted this option to reduce the **age of data processing consent to 13**.

## You should also remember that you have to be able to show that you have been given consent lawfully and therefore, when collecting children's data, you must make sure that your privacy/data protection notice is written in a language that children can understand and copies of consents must be kept.

## You do not have to ask for a child’s consent just because they are over 13 years old; the law on what age a child becomes an adult is not changing. If you feel it is more appropriate to ask a parent or guardian’s consent where a child is under 18, you can choose to do so.

# Will I need to appoint a Data Protection Officer?

## Data Protection Officers (DPOs) are specifically required in certain circumstances under the UK GDPR, such as where organisations process sensitive (special category) personal data on a "large scale". The processing of sensitive personal data by the PCC and/or incumbent is unlikely to be classed as "large scale". Parishes are highly unlikely to be required to have a Data Protection Officer.

# Deciding who will be responsible for Data Protection in the Parish

## This is the first point of the checklist and is an important one to aid UK GDPR compliance. The Incumbent and another member of the PCC could take responsibility for compliance. The person who takes on this role should have the authority of the PCC. Their role should include providing support and guidance for others. If a staff member is to take on this role, it does not need to be a new member of staff, but rather added to the duties of an existing member of staff.

## The term ‘Data Protection Manager’ or similar, rather than ‘Data Protection Officer’ ought to be used, to avoid confusion with the UK GDPR required Officer, to which specific conditions are attached under the legislation.

## If a data protection issue comes up and you are unsure how to respond, you are welcome to email your query to [data@southwark.anglican.org](mailto:data@southwark.anglican.org)

# CCTV

## Some parishes may have CCTV in place to try to protect the security of buildings. The UK GDPR does not specifically change the rules about CCTV but the new transparency requirements mean that Parishes should check whether there are adequate signs erected containing the right level of detail.

|  |  |
| --- | --- |
| What’s new? CCTV | |
| **Data Protection Act 1998** | **UK GDPR / DPA 2018** |
| The ICO produced a code of conduct for CCTV users which recommends a sign is erected notifying visitors they are being recorded. | Organisations should revisit the signs to ensure full transparency – for example does the sign state that automatic number plate recognition software is used and list all the purposes the data collected will be used for? |

# Key data - What to keep and for how long

## How long to keep information, including Parish Registers, Electoral Rolls, Gift Aid declarations and a range of other information typically held by parishes can be found in the guide to parish record keeping "Keep or Bin: Care of Your Parish Records" which can be downloaded from the Church of England or Lambeth Palace Library websites at: <http://www.lambethpalacelibrary.org/content/recordsmanagement>.

Southwark Diocese *A Safe Church* policy also provides requirements for record keeping relating to safeguarding:

<http://southwark.anglican.org/safeguarding/diocesan-policies-and-procedures>

# What about contracts with suppliers and partners?

## PCCs should review their existing contracts in light of the UK GDPR, assessing current policies and procedures in place in light of the flow of data across the parish. Going forward, the increased obligations and liability under the UK GDPR should be considered in future negotiations to ensure an adequate risk allocation with suppliers. In general, organisations should expect more lengthy and difficult negotiations with suppliers as they try to address their new exposure under the UK GDPR. If third party organisations provide parishes with services (such as ChurchDesk) and they can access personal data then this applies to you.

### What must be included in contracts?

### Processor must process data only on the instructions of the data controller.

### People authorised to access data are subject to confidentiality.

### Ensure security of processing.

### Assist the controller in complying with data subjects rights (where possible).

### Assist the controller with regard to security measures, breach reporting and DPIAs.

|  |  |
| --- | --- |
| What’s new? Contracts with data processors and joint controllers | |
| **Data Protection Act 1998** | **UK GDPR / DPA 2018** |
| The current law did not make contracts compulsory but it was regarded as good practice. | The UK GDPR requires contracts to be entered into and stipulates eleven mandatory topics which must be included. If organisations fail to do this by May 2018 both controllers and processors can be fined. |

# What is a Data Protection Impact Assessment (DPIA) and when is it needed?

## A Data Protection Impact Assessment is a type of audit **used to help assess privacy risks**. A large organisation might carry out a DPIA if it was going to outsource its payroll function for the first time. A school or parish might carry out a DPIA if it was installing CCTV which included cameras pointed at public areas.

## A DPIA assesses the impact of any proposed processing operation, for example the use of new technology, on the protection of personal data. A DPIA should be carried out before the processing of the personal data starts and then updated throughout the lifetime of any project. The ICO has produced a 51-page Code of Practice on DPIAs (<https://ico.org.uk/media/for-%20organisations/documents/1595/pia-code-of-practice.pdf>).

## A short DPIA Assessment Questionnaire is in Appendix 6.

## The content of a DPIA usually includes:

## A description of the processing activities and their purpose;

## An assessment of the need for and the proportionality of the processing; and

## The risks arising and measures adopted to try and prevent any risks, in particular any safeguarding or security measures to protect data and comply with the UK GDPR.

# Appendix 1 – A summary of the legislation changes

## The good news is that the main concepts and principles of the UK GDPR (brought into force by the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) are very similar to those contained in the previous 1998 Data Protection Act. The Information Commissioner’s Office (ICO) is still the organisation in charge of data protection and privacy issues. Therefore, if you are compliant with the 1998 Data Protection Act, much of what you do still applies. However, there are some changes and additions, so you may have to do some things for the first time and some things differently (these are highlighted below).

## One of the main changes to note is that the UK GDPR places a much greater emphasis on transparency, openness and the documents you need to keep in order to show that you are complying with the legislation. This is incorporated within the idea of "accountability".

| **Change** | **Detail of Change** | **Impact of Change** |
| --- | --- | --- |
| **Record Keeping** | Each Data Controller must maintain a record of processing activities under its responsibility. Data Processors must also keep a record of the processing activities it carries out on behalf of the Data Controller. | The level of detail is the same as contained in an ICO registration and the log can be requested at any time by the ICO. |
| **Privacy Notice** | Under the UK GDPR privacy notices must be more transparent, using clear and plain language, and easily accessible. | Privacy notices will need to be reviewed and updated to make them clearer, more transparent and easily accessible. See Appendix 5 for template Privacy Notice. |
| **Consent** | Consent is fundamental under the UK GDPR as individuals have more rights to decide how their data may be processed and their rights to opt in and opt out of such processing. Where processing data is based on consent, the PCC must be able to evidence the consent. Consent must be by an “opt in” method. | The processing activities which require the consent of the individual need to be identified and for consent to be captured in a UK GDPR manner. |
| **Breaches** | Data Controllers must report personal data breaches to the ICO without undue delay, where reporting is required and, where feasible no later than 72 hours after having become aware of the breach. An individual who has suffered damage can claim compensation from the Data Controller or the Data Processor. | Incident management process for data breaches needs to be reviewed and enhanced where required. Training will be required to increase awareness of what constitutes a breach and how to escalate investigation into the breach. |
| **Right of Access (Data Subject Access Requests)** | The time limit to comply with a Data Subject Access Request (DSAR) has been reduced from 40 calendar days to one calendar month. The ability for an organisation to charge up to £10 per DSAR has been removed and a breach must be processed free of charge. | The Data Subject Access Request process will need to be reviewed and updated accordingly. |
| **Data Privacy Impact Assessments (DPIAs)** | The UK GDPR introduces a mandatory requirement for DPIAs to be carried out in certain situations. DPIAs will need to contain a description of the processing and the purpose of the processing and would need to identify any risks to the personal data and the rights and freedoms of the individuals, and the measures and safeguards to mitigate risks. | DPIAs will need to be introduced where new technologies are used for high-risk data processing activities, large scale processing of sensitive data or when there are systematic and extensive activities which use automated processing to evaluate, analyse or predict behaviour. See Appendix 6 – Data Privacy Impact Assessment (DPIA) Checklist. |
| **Privacy by Design** | When developing, designing or using products, services or applications which involve processing personal data, Data Controllers and Processors should adopt internal policies and measures to ensure personal data is protected. | If a parish introduces a new IT system or launch a new website which collects data, the processes should include checkpoints for compliance with data privacy. |
| **Right to Object** | Individuals must be advised of their right to opt out of processing activity, and direct marketing which must be explicitly brought to their attention in a clear way and separately from other information. | Unsubscribe methods will need to be reviewed. Any reasonable objection requests need to be stored and evidenced. |
| **Right to Erasure** | An individual has a right to request for their data to be deleted. The Data Controller must delete personal data on request and data can only be retained where there are legitimate grounds or a legal obligation to retain the data. The Data Controller must also ensure third parties delete personal data on request. | Data deletion processes will need to be introduced so that data is not retained indefinitely. It’s likely a data cleanse exercise will need to be carried out prior to 25 May 2018 so that the PCC is not storing data it no longer require or have a need to store. |
| **Profiling** | An individual has the right not to be subject to a decision based solely on automated processing, including profiling. Profiling for marketing purposes will always require explicit consent. | Activities that rely or use profiling need to be identified to establish whether consent is required. Processes need to be put in place to intervene, where possible, where an individual may object to profiling. |
| **Data Protection Officer** | A Data Protection Officer (DPO) may need to be appointed. This does not need to be a standalone role but the DPO should report to the highest level of management and must be informed about all data protection issues within the organisation. | Parishes are highly unlikely to meet the criteria for appointing a DPO but should appoint someone responsible for data protection matters. |
| **Right of Portability** | The UK GDPR introduces a new right of data portability. This right allows for the data which the individual provided to the Data Controller to be provided to the individual in a structured format, to allow it to be transmitted to another Data Controller. | It will be important to understand where the data is being stored and in what format to establish the ease of moving data and receiving data in from a third party. |

# 

# Appendix 2 – UK GDPR Action Plan Checklist

|  |  |  |
| --- | --- | --- |
| **** | **Raise awareness** – PCC members, church administrators, incumbents and other key data users should be made aware that the law is changing. Ensure they undergo training, and that records are kept. They need to know enough to make good decisions about what you need to do to implement the UK GDPR.  **Decide who will be responsible for data protection** – The incumbent and another member of the PCC should take responsibility for compliance with data protection legislation and should have the knowledge and authority to do this effectively. | |
| **** | **Data Audit –** If you do not know what personal data you hold and where it came from you will need to organise an audit to find out. This means all personal data including employees and volunteers, service users, members, donors and supporters and more. You should document your findings because you must keep records of your processing activities. You should also record if you share data with any third parties. See Appendix 3. | |
| **** | **Identify and document your ‘lawful basis’ for processing data** – To legally process data under the UK GDPR you must have a ‘lawful basis’ to do so. For example, it is a lawful basis to process personal data to deliver a contract you have with an individual. There are a number of different criteria that give you lawful basis to process and different lawful basis give different rights to individuals. Understand and document your lawful basis for processing data. | |
| **** | **Check your processes meet individuals’ new rights** – The UK GDPR will give people more rights over their data. For example, the UK GDPR gives someone the right to have their personal data deleted. Would you be able to find the relevant data and who would be responsible for making sure that happened? Ensure you have the systems in place to be able to deliver the eight rights.  **Know how you will deal with ‘subject access requests’** – Individuals have the right to know what data you hold on them, why the data is being processed and whether it will be given to any third party. They have the right to be given this information in a permanent form (hard copy). This is known as a ‘subject access request’ or “SAR”. You need to be able to identify a SAR, find all the relevant data and comply within one month of receipt of the request. Under the UK GDPR the time limit for responding to SARs is reduced from 40 days to one month and the £10 fee is abolished. | |
| **** | **Review how you get consent to use personal data** – If you rely on consent as your lawful basis for processing personal data, then you need to review how you seek and manage consent. Under the UK GDPR consent must be freely given, specific and easily withdrawn. You can’t rely on pre-ticked boxes, silence or inactivity to gain consent instead people must positively opt-in. See our consent language in Appendix 4. | |
| **** | **Build in extra protection for children** – The DPA 2018 says children under 13 cannot give consent so you will have to obtain consent from a parent or guardian. You will need to be able to verify that person giving consent on behalf of a child is allowed to do so. Privacy notices should to be written in language that children can understand. | |
| **** | **Update your Policies & Notice**  **Policies** – Have clear, practical policies and procedures on information governance for staff to follow, and monitor their operation.  **Privacy Notice** - You must always tell people in a concise, easy to understand way how you intend to use their data. Privacy notices are the most common way to do this. You may well already have a privacy notice but it will all need to be updated. Under the UK GDPR, privacy notices must give additional information such as how long you will keep data for and what lawful basis you have to process data. Our sample privacy notice is in Appendix 5.  **Data Retention & Disposal** – Ensure you update your data retention policy and inform all data subjects how long you will retain data. When disposing of records and equipment, make sure personal information cannot be retrieved from them. To assist, see the link to the Church of England website for ‘Keep or Bin: care for your Parish Records’ on page 18.  **Websites** – Control access to any restricted area. Make sure you are allowed to publish personal information (including images) on website/social media. | |
| **** | **Data sharing** – Be sure you are allowed to share information with others and make sure it is kept secure when shared.  **CCTV** – Inform people what it is used for and review retention periods. Ensure you have the correct signage on display and a suitable policy in place.  **Training** – Train role holders and staff on the basics of information governance, where the law and good practice need to be considered and know where to turn for advice. | |
| **** | **Update your contracts to deal with processing by others** – Recognise when others are processing personal data for you and make sure they do it securely. You will need to ensure your contracts are updated to include the UK GDPR required clauses and put in place an audit programme to supervise them. Consider also how you select suppliers. There must be a written contract which imposes these obligations on processors: | |
| 1. Follow instructions of the controller. 2. Ensure their personnel are under a duty of confidence. 3. Keep the personal data secure. 4. Allow Controllers to consent to sub-contractors. 5. Flow down obligations to sub-contractors (but remain responsible for actions of the sub-contractor(s)). 6. Assist the controller when individuals exercise their rights to access, rectify, erase or object to processing of data. | 1. Assist the controller with privacy impact assessments. 2. Assist the controller with security and data breach obligations and notify the controller of any personal data breach. 3. Return or delete data at the end of the agreement (but can keep a copy). 4. Demonstrate compliance with these obligations and submit to audits. 5. Inform the controller if their instructions would breach the law. |
| **** | **Personal Data Breaches - Get ready to detect, report and investigate these** - A data breach is a breach of security leading to ‘accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data’. You need to have the right procedures in place to detect, investigate and report a breach. The UK GDPR introduces a duty to report certain types of data breaches to the ICO and in some cases to the individuals concerned. You need to be able to demonstrate that you have appropriate technical and organisational measures in place to protect against a breach.  The Data Protection Compliance Officer and other back-ups need to be recognised by data users as those to whom any breaches should be reported. They therefore need to be briefed on the procedure for dealing with data breaches.  All data users should be briefed on personal data breach avoidance, and on what to do in the event that a breach occurs.  Examples of personal data breaches and steps to avoid them include:   * Emails and attachments being sent to the wrong person, or several people – it is easy to click the wrong recipient. Slow down, check thoroughly before clicking ‘send’. * The wrong people being copied in to emails and attachments. – Use BCC (Blind Carbon Copy) where necessary. * Lost memory sticks – The PCC should put protocols in place for memory stick usage. * Malware (IT) attack – ensure up to date anti-virus software is in place. * Equipment theft – check security provisions. | |
| **** | **Build data protection into your new projects** - Privacy by design means building data protection into all your new projects and services. It has always been good practice, but the UK GDPR makes privacy by design an express legal requirement. To achieve this, data protection impact assessments should be undertaken where new technology is being deployed, where profiling may significantly affect individuals or sensitive categories of data will be processed on a large scale. Clarify who will be responsible for carrying out impact assessments, when you will use them and how to record them. See our DPIA assessment checklist in Appendix 5. | |

# Appendix 3 – Audit Questionnaire

## To be used for Record keeping.

## This form is designed to help Parishes to audit their personal data processing. It is important to complete this form as comprehensively as possible.

## **‘Personal Data’** is any information about a living person which can identify them. This is not just someone's name and address but any ID information. For example, a phone number or email address is personal data. Any other contact information or a person's employment history, medical conditions, criminal record or credit history are all personal data.

## **‘Processing’** personal data means storing or deleting any personal data on a computer, database or some manual files (e.g. HR personnel files). The word 'processing' also covers selecting a name for a mailing list. It includes transferring and altering data. Indeed, practically anything done to personal data constitutes processing.

|  |  |
| --- | --- |
| 1. : | **A. YOUR INFORMATION** |
|  | **1. Person completing questionnaire**  a) Name  b) Role  c) Telephone number  d) Email |
|  | Data controller (e.g. PCC, Incumbent) |
|  | Date you completed this survey |
| 1. : | **B. COMMUNICATIONS DATA** |
|  | This section relates to communications with church members and other parishioners including contacts (e.g. via outreach activities, weddings, baptisms, funerals). Communications include mailing lists for newsletters or requests for donations.  **a) What type of information do we keep?**  E.g. name, contact details Gift Aid information and congregational giving details such as bank details.  **b) Where do we get the data from?**  E.g. individuals themselves, family members, clergy, other church sources, publicly available sources e.g. electoral register.  **c) Why do we collect or process the data – what do we do with it?**  For purposes relating to: e.g. church membership, and for contact regarding involvement in parish activities; advertising, outreach programmes [Please list all reasons].  **d) Who do we disclose communications data to?**  E.g. parish clergy, church members and contacts carrying out the work of the church, diocesan authorities, bishop, other church organisations.  **e) Do we ever send communications data overseas and if so where to and to which company? This might include overseas companies providing database or email services.**  E.g. linked parishes, mission agencies, cloud storage |
|  | **C. SUPPLIERS, COMPANIES AND OTHER ORGANISATIONS WE DO BUSINESS WITH** |
|  | About individuals or representatives of organisations which supply us with services such as for church repairs, or with whom we are in contact.  **a) Who do we keep personal data about?**  E.g. Trades people, surveyors, architects, builders, suppliers, advisers, payroll processors, donors to appeals [Please list any others].  **b) What type of information do we keep?**  E.g. Name, contact details, qualifications, financial details, details of certificates and diplomas, education and skills [Please list any others].  **c) Where do we get the data from?**  E.g. The individuals, companies, suppliers, [Please list any others].  **d) Why do we collect or process the data?**  E.g. Church repairs and upkeep; maintain services e.g. electrical, gas, insurance [Please list any other reasons]. |
| 1. : | **D. GENERAL QUESTIONS ABOUT PERSONAL DATA** |
|  | How do we store the personal data collected? Do we take any steps to prevent unauthorised use of or access to personal data or against accidental loss, destruction or damage? If so, what? How do we manage access to data – what is the process involved in getting access? |
|  | Do any procedures exist for rectifying, deleting, suppressing or blocking, personal information? If so, please provide details. |
|  | Who has access to / is provided with the personal data (internally and externally)? Is there an authorisation procedure for accessing personal data? If so, please provide details. |
|  | Can we provide a copy of all existing data protection or privacy notice and consents used? |
|  | So far as we are aware, has any personal data which was gathered for one purpose (e.g. electoral roll membership) been used for another purpose (e.g. circulating details of church services & activities?) If so, please provide details. |
|  | Are we aware of any policies, processes or procedures to check the accuracy of personal data? |
|  | In the event of a data security breach occurring, does the PCC have in place processes or procedures to be followed? What are these? |
|  | If someone asks for a copy of information that the parish holds about them, i.e. they make a ‘subject access request’, is there a procedure for handling such a request? Who do we send the request to? |
|  | Can we locate a copy of the 'consent' form currently used for communications? |
|  | Are cookies used on our parish website? If so, can we provide a copy of the form of consent used? Do we allow individuals to refuse to give consent? Do we provide information about the cookies used and why they are used? |
|  | Are any communications files which may be used checked against marketing suppression lists where relevant, such as the Mailing Preference, Fax and Telephone Preference Services? |
|  | Can we provide a copy of all website privacy notices and privacy policies? |
|  | What data protection training do people in the PCC and other key data users (e.g. church administrator, Sunday school co-ordinator, youth leader, stewardship officer, hall bookings secretary) receive? What does the training involve? |
|  | Does anyone in the PCC have responsibility for reviewing personal data for relevance, accuracy and keeping it up to date? If so, how regularly are these activities carried out? |
|  | What do we do about archiving, retention or deletion of personal data? How long is personal data kept before being destroyed or archived? Who authorises destruction and archiving? |
| 1. : | **E. PERSONAL DATA** |
|  | This is intended as a full coverage of the parish’s personal data and processing activities, which is in addition to (rather than repeating) information provided in Parts B and C.  **a) Who do we keep personal data about?**  E.g. Church role and office holders (such as churchwardens, PCC Secretaries, Deanery Synod members, church Safeguarding officer, Sunday School co-ordinator, youth leaders/workers), church members, clergy, volunteers, children, youth, staff, employees, hall hirers, and contractors. [Please list anyone else]  **b) What type of information do we keep?**  E.g. Name, contact details, date of birth, child registration information, Safeguarding information, information on employees. [Please list anything else]  **c) Where do we get the data from?**  E.g. The individuals themselves, other parishes, diocesan authorities, bishops, National Church, Deanery officers, companies and recruitment agencies. [Please list anyone else]  **d) Why do we collect or process the data?**  E.g. To further the mission and ministry of the church including by carrying out activities, advertising services and events, outreach programmes, employee administration and payroll, operational reasons. [Please list anything else]  **e) Do we collect any sensitive information (other than religious beliefs)**: relating to racial or ethnic origin, political opinions, trade union membership, physical or mental health or criminal records?  If so for what reason: e.g. criminal records for Safeguarding compliance; physical or mental health information relating to employees; racial and ethnic origin relating to equal opportunities monitoring. [Please list anything else]  **f) Who do we disclose the data to?**  E.g. Parish clergy, church members and contacts carrying out the work of the church; diocesan authorities, bishop, other church organisations, suppliers. [Please list anyone else] |
|  | Please identify any monitoring of the following systems that takes place. ‘Monitoring’ includes all monitoring of systems including without limitation intercepting, blocking, recording or otherwise accessing systems whether on a full-time or occasional basis. The systems are:  (a) computer networks and connections  (b) CCTV and access control systems  (c) communications systems  (d) remote access systems  (e) email and instant messaging systems  (f) telephones, voicemail, mobile phone records  (g) intranet and Internet facilities  [Please list anything else].  Please provide copies of all notices, policies or procedures relevant to this monitoring and hold in a secure place. |

# Appendix 4 – Consent Form

**(INSERT YOUR PCC LOGO HERE)**

**CONSENT FORM**

As a member on the electoral roll or as an individual or family who are church members your contact details will be collected and may be used for pastoral or discipleship purposes; and to promote the activities and interests of the Church and charity, which constitutes processing under lawful basis of legitimate interests

In addition we would like to obtain your consent by checking the box below to keep in touch and provide additional information about church activities, events, news and fundraising requests:

|  |  |
| --- | --- |
| **🞎** | **I would like to receive information about church activities, events, news and fundraising requests.** |

**Please select preferred communication method and provide your contact information below:**

🞎 I would like to receive communications by email

🞎 I would like to receive communications by telephone

🞎 I would like to receive communications by mobile phone via text message

🞎 I would like to receive communications by post

|  |  |  |
| --- | --- | --- |
|  | | |
| **Name\*** | …………………………………………………………..… | …………………………………………………………..… |
|  |  |  |
| **Email** | …………………………………………………………..… | …………………………………………………………..… |
| **Mobile** | …………………………………………………………..… | …………………………………………………………..… |
| **Phone** | …………………………………………………………..… | …………………………………………………………..… |
| **Address** | …………………………………………………………..… | …………………………………………………………..… |
|  | …………………………………………………………..… | …………………………………………………………..… |
|  |  |  |
| **Signature** | …………………………………………………………..… | …………………………………………………………..… |
| **Date** | …………………………………………………………..… | …………………………………………………………..… |

**\*** If you are aged under 13 your parent or guardian should fill in their details below to confirm their consent

# Your privacy is important to us and you can find out more about how we use your personal data by reading our Privacy Notice which accompanies this consent form and which you can find here: [insert website url].

# Appendix 5 – Privacy Notice

**[Insert Parish logo here]**

**GENERAL PRIVACY NOTICE**

1. **Your personal data – what is it?**

“Personal Data” is any information relating to an identified or identifiable natural living person, commonly referred to as the ‘data subject’. Identification can be by the information alone or in conjunction with any other information that the data controller may possess or be likely to obtain. The processing of personal data is governed by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1. **Who are we?**

The Parochial Church Council (PCC) of [insert name of parish] is the data controller for your data. This means that it decides how your personal data is processed and for what purposes. The PCC works in close conjunction with the incumbent of the parish that is, our [vicar or rector]. We may need to share personal data we hold with the incumbent so that they can carry out their responsibilities. The incumbent acts as joint data controller for your data. This means we are both responsible to you for how we process your data.

This Privacy Notice is provided to you by the PCC on behalf of the PCC and on behalf of the incumbent as joint data controllers. In the rest of this Privacy Notice we use the word “we” to refer to the joint data controllers.

1. **How do we process your personal data and what is the legal basis of processing your data?**

The data controllers will comply with their legal obligation to keep personal data up to date; to store and destroy it securely; to not collect or retain excessive amounts of data; to keep personal data secure; to protect personal data from loss, misuse, unauthorised access and disclosure; and to ensure that appropriate technical measures are in place to protect personal data.

We use your personal data for some or all of the below purposes.

As a visitor:

* To send you communications which you have requested and that may be of interest to you. These may include our newsletter, and information about campaigns, events and other fundraising activities (by email and/or hard copy);
* To process photos taken of you, with your consent, which we may use to publicise our activities;
* [Delete as required] Our premises have CCTV cameras which capture digital images, which constitutes processing under the lawful basis of legitimate interests for security purposes;
* [Delete as required] If you login to our Wi-Fi, we will capture information from your personal electronic device which is required as part of our terms of service;
* [Delete as required] Our website uses cookies to capture user information which is used to optimise the service we provide to you.

As a participant in a church service relating to a life event:

* Where you are enquiring about or participating in life events such as a baptism, marriage or funeral then we will process your contact information and other personal information relating to the event, which constitutes processing necessary for our legitimate interests, or processing in compliance with a legal obligation(for example we are required to announce forthcoming weddings by means of Wedding Banns);
* [Delete as required] For reasons of pastoral care or support we may contact you and or make you aware of other courses or events which you may be interested in (for example an All Souls service Easter or Christmas Services, marriage course), which constitutes data processing under the lawful basis of legitimate interests.

As a member on the electoral roll or as an individual or family who are church members:

* Your contact details will be collected and may be used for pastoral or discipleship purposes; and to promote the activities and interests of the Church and charity, which constitutes processing under lawful basis of legitimate interests;
* If you join the electoral roll, your title, name and address along with a declaration are legally required to fulfil Church Representation Rules 2017 (CRR);
* [Delete as required] If you sign up as a volunteer on a rota your contact information may be shared with others on the list to enable volunteers to swap duties which is processing under the lawful basis of legitimate interests;
* [Delete as required] If you consent to being part of our church directory, your contact information will be shared with other church directory recipients;
* Your personal information relating to demographics may be collected and used to support the development of our mission, which constitutes processing under lawful basis of legitimate interests;
* Your financial information, such as bank account and card numbers, relating to planned donations and reclaiming gift aid. We may share these details with third parties, such as HMRC, under the lawful basis of legal obligation, and we may contact you in relation to further fundraising opportunities under the lawful basis of legitimate interests.

As a user of a church building:

* Where you are enquiring about or using our buildings we will process your contact information and payment information under the lawful bases of legitimate interest, or, in cases where you hire our facilities, contractual necessity;

As a paid employee or contractor working on behalf of the PCC:

* We will process your data under lawful bases of legitimate interest, contractual and legal obligations for legal, personnel, administrative and management purposes. Where we process sensitive personal data, we may rely on a number of lawful bases, including (but not limited to) your consent, or processing necessary for the purposes of exercising or performing any right or obligation relating to your employment.
* We may process sensitive personal data including, as appropriate:
  + information about your physical or mental health or condition in order to

monitor sick leave and take decisions as to your fitness for work;

* + your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  + information in order to comply with legal requirements and obligations to third parties.
* We will process data relating to your work, performance, ability and suitability for the role.
* We will process your financial information and other employment related information.

As a trustee including a member of the PCC, church warden, PCC secretary and deanery synod representative:

* Your contact details will be processed to enable registration and update of the Diocesan directory and or with the Charity Commission, which is processing under lawful bases of legal obligation and legitimate interests.
* We may collect and process data relating to your ability and suitability regarding the trustee role as part of our due diligence, which is processing under the lawful basis of legitimate interests.

As a person requiring a Disclosure and Barring Service (DBS) check due to working with children or vulnerable adults:

* Your contact details and any other relevant documents as required for a DBS check will be processed under the lawful bases of legitimate interests, and processing necessary for the safeguarding of children and of individuals at risk.

In addition to the above, the data we process is likely to constitute sensitive personal data because, as a church organisation, the fact that we process your data at all may be suggestive of your religious beliefs. Where you provide this information, we may also process other sensitive personal data.

Religious organisations are permitted under UK GDPR to process information about your religious beliefs to administer membership or contact details.

In circumstances where your personal data is used on the basis of obtaining your consent, you may indicate your consent in a number of ways, including, as permitted by law, ticking a box (or equivalent action) to indicate your consent.

1. **Sharing your personal data**

Your personal data will be treated as strictly confidential. It will only be shared with third parties where it is necessary for the performance of our tasks or where you give us your prior consent.

It is likely that we will need to share your data with some or all of the following (but only where necessary):

* [Delete as required] Other members of the congregation to carry out a service for your benefit or where it is in the legitimate interest of the Church. For example, sharing contact details on a rota to enable swapping of duties;
* Our agents, servants and contractors. For example, we use a third party to process our DBS checks and we may also ask a commercial provider to send out newsletters on our behalf, or to maintain our database software;
* Other clergy or lay persons nominated or licensed by the bishops of the Diocese of Southwark to support the mission of the Church in our parish. For example, our clergy are supported by our area dean and archdeacon, who may provide confidential mentoring and pastoral support.
* Assistant or temporary ministers, including curates, deacons, licensed lay ministers, commissioned lay ministers or persons with Bishop’s Permission To Officiate (PTO) who may participate in our mission in support of our regular clergy.
* As a trustee including a member of the PCC, church warden, PCC secretary and deanery synod representative your contact details will be shared with the Diocese of Southwark and or the Charity Commission.
* In accordance with our Diocesan Safeguarding Policy “A Safe Church” personal data relating to safeguarding may be shared confidentially between the Parish Safeguarding Officer and the Diocesan Safeguarding team.

<http://southwark.anglican.org/safeguarding/diocesan-policies-and-procedures>

1. **How long do we keep your personal data?**

We keep data in accordance with the guidance set out in the guide “Save or Delete: the Care of Parish Records” which is available from the Church of England website at https://www.churchofengland.org/more/libraries-and-archives/records-management-guides. We will only keep data for as long as we need it, however we may keep some records permanently if we are required to do so.

Where we no longer need to process your personal data for the purposes set out in this Privacy Notice, we will delete your personal data from our systems.

1. **Your rights and your personal data**

To exercise your rights, please send your request to us in writing (using the contact details below). When exercising your rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights:

* The right to access information we hold on you
* The right to correct and update the information we hold on you
* The right to have your information erased: *In the case that you request that we erase the data we hold, we will confirm whether the data has been deleted or the reason why it cannot be deleted (e.g. because we need it for our legitimate interests or a regulatory purpose).*
* The right to object to processing of your data*.*
* The right to data portability*.*
* The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.
* The right to object to the processing of personal data where applicable.
* The right to lodge a complaint with the Information Commissioner’s Office.

**7. Transfer of Data Abroad**

From 1st January 2021, the UK will become a third country outside the European Economic Area (EEA). Any electronic personal data transferred either to countries or territories inside the European Economic Area (EEA) or to other third countries, will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the United Kingdom. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas. We take all reasonable steps to ensure that your personal data is processed securely and will only transfer your personal data outside the United Kingdom where it is compliant with applicable data protection legislation or is part of a contract with specific individuals or organisations and the means of transfer provides adequate safeguards in relation to your personal data.

**8. Further processing**

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

**9. Contact Details**

Please contact us if you have any questions about this Privacy Notice or the information we hold about you or to exercise all relevant rights, queries or complaints at: The Data Controller, [insert Parish contact or office], or email: [insert email address]

If you are unhappy with how your personal data has been processed, you have the right to lodge a complaint with the Information Commissioners Office at any time. You can contact the Information Commissioners Office on 0303 123 1113 via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

# Appendix 6 – Data Privacy Impact Assessment (DPIA) Checklist

The UK GDPR requires that organisations carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. For a parish examples might include, introducing a new safeguarding protocol which involves sharing data with multiple agencies or using CCTV to monitor public areas.

If two or more of the following apply, it is likely that you will be required to carry out a DPIA. This does not apply to existing systems but would apply if you introduced a new system.

|  |  |  |
| --- | --- | --- |
|  | Profiling is in use. For example: you monitor website clicks or behaviour and record people’s interests. | 🞎 |
|  | Automated decision making. For example: when processing leads to the potential exclusion of individuals. | 🞎 |
|  | CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects. | 🞎 |
|  | Sensitive data. For example: information about individuals’ political opinions, as well as personal data relating to criminal convictions or offences. | 🞎 |
|  | Large scale data processing. There is no definition of “large scale”. However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed. | 🞎 |
|  | Linked databases - in other words, data aggregation. Example: two datasets merged together, that could “exceed the reasonable expectations of the user”. For example: you merge your mailing list with another church, club or association. | 🞎 |
|  | Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. employee-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients. | 🞎 |
|  | “New technologies are in use”. For example: the use of social media. | 🞎 |
|  | Data transfers outside of the UK. | 🞎 |
|  | “Unavoidable and unexpected processing”. For example, processing performed on a public area that people passing by cannot avoid. For example: Wi-Fi tracking. | 🞎 |