Diocese of Rochester

# A GDPR Toolkit For Parishes

## New Data Protection Laws

March 2018

Called together
grow enrich resource

Winckworth Sherwood

## Contents

Foreword ..... 3
A Note from the Diocesan Legal Team ..... 3

PART ONE ..... 4

A brief introduction to the GDPR ..... 4
Introduction ..... 5
Underlying Principles ..... 6
The key changes ..... 6
Who will be affected? ..... 7
A gear shift in risk ..... 7
Examples of failures to comply with the new law ..... 7
Key Points for Parishes ..... 7
Why are there two privacy notices in Appendix 5? ..... 8
What do I need to do about Consent? ..... 8
NEXT STEPS: ..... 9

PART TWO ..... 10

A detailed guide to the GDPR ..... 10
Why implement new legislation? ..... 11
Consent, Rights and Accountability ..... 11
What is the scope of the GDPR? ..... 11
What's new? Legal rights of Data Subjects ..... 11
Accountability - What is it and how do I comply? ..... 12
What is a privacy notice? ..... 12
What are the additional data subject rights? ..... 12
Lawful basis for processing ..... 14
How do I show that I am processing personal data lawfully? ..... 15
When am I allowed to process 'sensitive personal data'? ..... 16
What do I need to do if there is a data breach? ..... 17
What's new? Notifying breaches ..... 17
Consent ..... 17
Can existing consents be relied on? ..... 18
What's new? Marketing consents ..... 19
The need to document your data processing ..... 19
Do I need to register (notify)? ..... 19
Processing personal data about children ..... 20
Will you need to appoint a Data Protection Officer? ..... 20
Deciding who will be responsible for Data Protection in the parish ..... 20
CCTV ..... 20
What's new? CCTV ..... 21
Key data - What to keep and for how long ..... 21
What about my contracts with suppliers and partners? ..... 21
What's new? Contracts with data processors and joint controllers ..... 21
What is a Data Protection Impact Assessment (DPIA) and when is it needed? ..... 22

Appendix 1 – Summary of the GDPR differences from the 1998 Act ..... 23
Appendix 2 – GDPR Action Plan Checklist ..... 25
Appendix 3 – Audit Questionnaire ..... 27
Appendix 4 – Consent Form ..... 30
Appendix 5 – Privacy Notices ..... 31
Appendix 6 – DPIA Assessment Checklist ..... 40

## Foreword

As has been well publicised, the General Data Protection Regulation (GDPR) will take effect in the UK from **25 May 2018**. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection regarding how their personal data is used by all organisations including parishes and other church groups and organisations. PCCs and other formally constituted church entities (e.g. Bishop's Mission Orders or church-related Trusts) must comply with its requirements, just like any other charity or organisation.

While the Diocese will endeavour to be as supportive as possible, responsibility for complying with the new Regulation rests formally with each PCC or other body. This guidance provides two practical tools to aid your GDPR compliance, in the form of a **GDPR Action Plan Checklist** and a **Data Audit Questionnaire**, in addition to templates for privacy notices and consent forms.

We recognise the burden that this new legislation places on already hard-pressed parishes – hence this guidance. Nonetheless, we all have to comply, and we strongly encourage those responsible in each place to take time to digest this guidance and work out the steps you need to take in order to ensure that your PCC or other body is compliant.

In the end this is about treating people with respect by taking due care with the information we hold about them. We, therefore, commend this GDPR Toolkit for use across the Diocese, and trust that it will provide helpful support as we all seek to meet the requirements of these new Data Protection laws.

James Langstaff
Bishop of Rochester

Geoff Marsh
Diocesan Secretary

## A Note from the Diocesan Legal Team

We have designed this GDPR Toolkit to take account of the National Church guidance, but to develop it further so that it is of greater relevance to parishes in the Rochester Diocese. 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 new law.

On a technical point, mainly relating to 'Annual Return' data on role holders (e.g. churchwardens, Deanery Synod reps and treasurers), it is important to note that in a small number of cases breaches of the law by a parish may cause the Diocese or the Bishop to be liable for the breach too. This is because the law treats each of the Parishes, the Bishop and the Diocese as a 'data controller' for data which is shared between us, and under the GDPR all the relevant controllers are ultimately liable for each other's actions.

# PART ONE

# A brief introduction to the GDPR

## Introduction

The GDPR will impose significant burdens on all organisations across Europe, including a substantial amount of additional reporting requirements and increased fines and penalties. The Government has made clear that the GDPR will continue to apply in the UK after Brexit.

This Toolkit contains a **checklist** which covers the actions outlined within it to help you monitor progress. 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 – Audit Questionnaire***.

One of the big changes in the law is you may need to obtain **consent** from those whose data you store or use. This will apply in most cases to members of the church community (such as ordinary church goers) but not to personal data which is processed in connection with a person's role in the church (even where the role is voluntary). Those with roles cannot give valid consent because consent has to be freely given, and can be withdrawn at any stage. This is not compatible with the situation in which a person must give consent in order to be appointed, and in which any later withdrawal of the consent would leave the parish in an impossible situation.

***Glossary:*** The jargon explained:

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

***Data controller*** is the person or organisation who determines the how and what of data processing.

***Data processor*** is the person or firm that processes the data on behalf of the controller.

***Data subject*** is the person about whom personal data is processed.

***Consent*** is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out.

***Privacy Notice*** is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.

***Processing*** is anything done with/to personal data (obtaining, recording, adapting or holding/storing) personal data.

***Sensitive personal data*** is also described in the GDPR as 'special categories of data' and is the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; criminal offences; genetic data; and biometric data.

You will need to produce two types of Privacy Notice: one for church goers and members (a 'General Privacy Notice') and one for role holders such as churchwardens, PCC members, volunteers (such as Sunday school teachers) and clergy (a 'Role Holders Privacy Notice'). If you have a website, it is good practice to make the General Privacy Notice available online so people can access it. We provide a sample of both Privacy Notices in this GDPR Toolkit in ***Appendix 5 – Privacy Notices***. You can amend and adapt the templates to produce your own Privacy Notices.

The General Privacy Notice should be issued to members of the church with whom you communicate regularly – perhaps by sending a newsletter or asking for donations. It is important that you collect signed copies of the Consent Form which goes with the General Privacy Notice. If you have an interactive website, you may also be able to collect this consent electronically, so long as the Privacy Notice is clearly made available and the data subject has elected to give consent, such as by expressly ticking a checkbox. The Role Holders Privacy Notice does not need to be signed but should be issued to anyone holding a role in your Parish (even if voluntary) to make them aware of the processing that may take place.

Finally, whilst you may rely on consent for most of your communications, there will be some data processing you will want to do as part of normal church management for which you will not need to gain specific consent for that particular action - holding lists of group members, for example. This is covered by a special condition under the GDPR for religious not-for-profit bodies, provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

## Underlying Principles

The 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. New guidance around Subject Access Requests.
- **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 EEA will be strengthened**. This requires parishes 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** (DPIA) in order to design data privacy into any new systems and processes will often be mandatory. E.g. if new technology is deployed, where there is processing on a large scale of '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 ICO within 72 hours of the breach.
- A new **principle of 'accountability'** puts the burden on PCCs 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 EU and also to the export of personal data to countries outside the EU.

The 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 significant additional risk on organisations. The GDPR will allow 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. Similar to a breach of the Data Protection Act 1998 (DPA), a breach of the 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

Consent for one element of data processing does not give you permission to do anything else with it. You cannot mail everyone on your electoral roll, or even everyone for whom you have a Gift Aid declaration, with fundraising communications. You need further consent. Where you collect consents, e.g. to be added to an email mailing list, you will need to store those consents. You are likely to need several different consent forms (or elements within a single form) to cover different areas of data processing within the life of the church.

If the purpose of an individual supplying data to the PCC is clear and unambiguous, then a separate consent is not required. For example, a completed electoral roll application form provides sufficient consent to add them to the roll. Likewise, a completed Gift Aid declaration is sufficient consent for you to claim Gift Aid on the relevant donations. However, as stated above, you can't then use that data for other purposes.

Whilst the GDPR removes the requirement for data controllers to register with the Information Commissioner's Office (ICO), there will be an annual "data protection fee".

## Why are there two privacy notices in Appendix 5?

For role holders such as churchwardens, members of the clergy and volunteers, you cannot rely on their consent because under GDPR (and the present law) consent must be freely given. As it is necessary to process certain data for these role holders so that they can perform their roles, it is not the case that consent can be truly "freely given". Anyone can also withdraw their consent at any time. Therefore it is not appropriate to rely on consent as a legal ground for processing personal data for role holders. We have designed two types of Privacy Notice for role holders and non role holders and you can find these in ***Appendix 5 – Privacy Notices.*** We have designed the Privacy Notices so that one notice is sent to each individual so the individual data controllers will not have to send a separate Privacy Notice unless they start using personal data for a purpose not listed in the Privacy Notice or start sharing personal data with a third party not listed in the notice.

## What do I need to do about Consent?

If you currently have consent from members of the church to send them newsletters or keep them informed about church activities, then depending on how it was obtained, it is likely that you will need to obtain a new consent because the rules on consent in GDPR are very prescriptive making it harder to obtain it. We have set out some consent language in ***Appendix 4 – Consent Form*** for you to use for this. You can start using this straight away for new data you are collecting but for all existing church goers and other members of the community that you currently regularly make contact with, you should send out the Consent Form in ***Appendix 4 – Consent Form.*** **Please remember not to use the Consent Form for role holders.**

## NEXT STEPS:

1. **Read the summary of the main differences between the GDPR and the current law in *Appendix 1 – Summary of the GDPR differences from the 1998 Act*.**

2. **See the Action Plan checklist in *Appendix 2 – GDPR Action Plan Checklist* This sets out a detailed step by step plan to help you ensure compliance.**

3. **Review what data you hold, how you store it, and what basis you have for processing it. Use the *Appendix 3 – Audit Questionnaire*. This will help you map what personal data you process and where it is.**

4. **Develop Data Privacy Notices. Use the templates in *Appendix 5 – Privacy Notices* to create privacy notices for role holders and non-role holders in your parish.**

5. **Review and refresh your existing consents and obtain new consents well before May 2018. Start using the Consent Form in *Appendix 4 – Consent Form* for collecting new data, and send it to all existing church-goers except those who are role holders.**

6. **Use the Data Protection Impact Assessment (DPIA) checklist in *Appendix 6 – DPIA Assessment Checklist* to help you decide where you will need to carry out a Data Protection Impact Assessment. Please note you will not usually need to carry out a DPIA for existing systems or processes unless you upgrade or substantially overhaul these.**

**If you have data protection queries please e-mail: gdpr@rochester.anglican.org**

# PART TWO

# A detailed guide to the GDPR

## Why implement new legislation?

The 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

From May 2018, parishioners will need to give their consent before you send them communications. This will need 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.

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 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 GDPR?

Many of the existing core concepts under DPA are reflected in the 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 GDPR as well.

Organisations which are not in the EU still have to comply with the GDPR. Non-EU organisations that trade in the EU or who process EU 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 GDPR) and data subjects. In the UK the supervisory authority is the Information Commissioner's Office ("ICO").

**What's new? Legal rights of Data Subjects**

| DPA 1998 | GDPR/new Data Protection Bill 2017 |
|---|---|
| Under the current law a Data Subject can 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 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 will 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 into and out of the parish.

*Under the 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 GDPR, **sensitive personal data** (which has a higher threshold of protection) will include genetic data, biometric data and data concerning sexual orientation, 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 GDPR require parishes 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 employees, customers and third parties.

## What are the additional 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. Parishes will need to update the relevant policies and procedures to reflect the new the GDPR requirements. You 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 GDPR are the same as under the 1998 Act but with some significant additions. The GDPR includes the following rights for individuals, which are briefly explained here:

## 1. The right to be informed

Individuals continue to have a right to be given "fair processing information", usually through a privacy notice. Under the 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.

## 2. The right to access (includes subject access requests)

Under the GDPR the right of data subjects to request information about the personal data processed by parishes remains largely the same. However, under the new regime parishes 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 will be abolished which is likely to lead to a greater number of requests. It is estimated that 25% of requesters at present withdraw or do not pursue their request when asked to fill in a form and pay the current £10 fee. Parishes will need to consider if they have sufficient resources to deal with an increase in the volume of data subject access requests.

You will be able to 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.

## 3. The right to rectification (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, you must tell those third parties of the correction. You must also tell the individuals about the third parties to whom the data has been given.

## 4. 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 parishes 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.

## 5. 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.

### 6. The right to data portability

Data subjects will 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. Parishes 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 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.

### 7. 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.

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

The 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 1998 Act.

## Lawful basis for processing

The GDPR sets out **six lawful bases** for processing data. Unless an exemption applies, **at least one of these will apply in all cases**. It is possible for more than one to apply at the same time. One of the new requirements for Privacy Notices is that you must set out in the Privacy Notice which Lawful basis you are relying on. In the sample notices in ***Appendix 5 – Privacy Notices*** 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 (but not for role holders), 2 Legitimate interests, 3 – Contractual necessity (for example with contractors), etc. Slightly different lawful bases apply in each of the sample Privacy Notices as some will only apply to role holders.

The six lawful bases for processing personal data under the GDPR are:

### 1. 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.

### 2. 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. "Direct marketing" is recognised as a possible legitimate interest (as an alternative to consent).

### 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.

### 3. 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).

### 4. 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).

### 5. 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).

### 6. 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 Rules' provisions) would require the individual's consent.

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

Sensitive personal data, which the 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 GDPR adds the following new additional categories: genetic data, biometric data and sexual orientation. To process sensitive personal data one of the following should apply – however please note that:

(a) More than one of the criteria below can apply at the same time.
(b) 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:

1. **Explicit consent of the data subject** has been obtained (which can be withdrawn).
2. **Employment Law –** if necessary for employment law or social security or social protection.
3. **Vital Interests** – e.g. in a life or death situation where the data subject is incapable of giving consent.
4. **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.
5. **Data made public by the data subject** – the data must have been made public 'manifestly'.
6. **Legal Claims –** where necessary for the establishment, exercise or defence of legal claims or for the courts acting in this judicial capacity.
7. **Reasons of substantial public interest** – where proportionate to the aim pursued and the rights of individuals are protected.
8. **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.
9. **Public Health** – where necessary for reasons of public health e.g. safety of medical products.
10. **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 General Privacy Notice in ***Appendix 5 – Privacy Notices*** as this allows data to be shared within the church.

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

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Currently, data breaches do not have to be routinely notified to the ICO or others (although the ICO recommends that it is good practice so to do). The GDPR makes informing the ICO and the individuals affected **compulsory** in certain circumstances, (e.g. where there is a high risk to the individuals involved, for instance, through identity theft). Under the GDPR, you will have to notify the ICO of a data breach within 72 hours of finding out about this. It is important that those in the parish note this deadline and seek the advice of the diocesan registrar about any suspected breaches without delay.

| What's new? **Notifying breaches** | |
|---|---|
| **DPA 1998** | **GDPR/new Data Protection Bill 2017** |
| Currently the notification of breaches to the ICO is effectively voluntary. | The GDPR introduces a new obligation to notify certain breaches to the ICO within 72 hours and in some cases data subjects will have to be notified too. |

*Under the 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.*

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.

## 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 GDPR, consent must be freely given, specific, informed, unambiguous and able to be withdrawn. Also, you will need to record how and when the consent was obtained (and review this over time). 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 will require "clear affirmative action". Silence, pre-ticked boxes, inactivity, or a history of processing without complaints will not constitute consent.

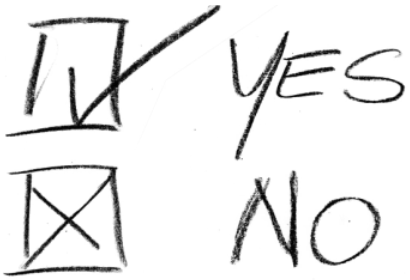
Therefore, if you wish to rely on consent, you will have to make sure that any consent wording is sufficiently strong to allow you to show that the consent given is unambiguous and the person knows exactly to what he/she is consenting. You will also have to tell individuals that they have the right to 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).

For example, you cannot use the personal data from the electoral roll to send mail to individuals about events at the church without seeking consent first. If you have not obtained consent from individuals to do this, you will not be able to use their personal data in this way. 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. Of course, if it was intended to share the names outside the church for another purpose, then you would need to obtain consent.

## Can existing consents be relied on?

You may need to review any existing consents you have on record to check whether they comply with the stricter rules under the GDPR. The basic rule is that if consent would have been valid under the soon-to-commence GDPR you can rely on it but if the consent was obtained using an opt out box or is ambiguous you cannot rely on it after 25 May 2018.




Under the 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. Parishes must also seek separate consents for separate processing operations. There is a presumption that these types of forced or omnibus consent mechanisms will not be valid: parishes will need to redesign consent mechanisms so as to present genuine and granular choice for consent to be valid.

| What's new? **Marketing consents** | |
|---|---|
| **DPA 1998** | **GDPR/new Data Protection Bill 2017** |
| Under current law an opt-out can be relied on by marketers for gaining marketing consent (for example, tick here if you don't wish to receive offers, etc.). | Under the GDPR, marketing consent must be explicit and in a form of:<br>▪ time limited opt-in<br>▪ in plain language<br>▪ easy way to opt-out and to say no to profiling<br>If consent can't be proved, parishes could face a big fine under the GDPR and an Enforcement Order to stop processing customer data. |

Processing does not need to be based on consent: other bases for processing still exist, including contractual necessity, compliance with a (Member State or EU) legal obligation and where the processing is necessary for the legitimate interests of the controller (or another organisation) provided that these interests are not overridden by the data protection rights of the individual. 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.

The Information Commissioner has recently published draft guidance on consent under the GDPR. This sets out that it is unlikely that an employer will be able to show that an employee has given valid consent under the GDPR (i.e. that it has been freely given) and employers should therefore rely on one of the other conditions for processing rather than consent.

## 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 parishes 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 (notify)?

The need for data controllers to register/notify with the ICO is removed under the GDPR. Nevertheless, it is important that you look at the various types of data processing you carry out, identify the purposes and legal basis for this processing and keep a written record of all your processing activities, security measures and data retention practices. Such information may need to be supplied to the ICO if requested.

However, the Data Protection Bill currently before Parliament allows the Secretary of State to make regulations requiring data controllers to pay a charge to the ICO and to provide information to the ICO to help the ICO identify the correct charge to be levied.

The ICO has confirmed that although there is no requirement to register/notify under the GDPR, there will be a new annual "data protection fee" which data controllers will be legally required to pay. The amount as yet has not been finalised but will depend on the size of the parishes, its annual turnover and the amount of personal data it processes. There will be exemptions from this fee and the ICO states that these will be similar to those

under the current registration/notification regime, (so PCCs should remain exempt and parish clergy should also be exempt unless records of pastoral care discussions, (e.g. that relate to beliefs, relationships, opinions etc. rather than purely factual information) are held on computer.

The ICO have stated that the new fee system will come into existence from 1 April 2018 but until that time data controllers should continue to register/notify as per usual. Once the new system is finalised the ICO has promised to let organisations know.

## Processing personal data about children

Under the GDPR itself, parental consent will be required for the processing of personal data of children under age 16. EU Member States may lower the age requiring parental consent to 13. In the draft Data Protection Bill recently published by the UK Government, the UK has adopted this option to reduce the age of consent to 13. This remains subject to Parliamentary approval.

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.

## Will you need to appoint a Data Protection Officer?

Data Protection Officers are specifically required in certain circumstances under the 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 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 Compliance Officer’ or similar, rather than ‘Data Protection Officer’ ought to be used, to avoid confusion with the 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: gdpr@rochester.anglican.org

## CCTV

Some parishes may have CCTV in place to try to protect the security of buildings. The 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 | |
|---|---|
| **DPA 1998** | **GDPR/new Data Protection Bill 2017** |
| The ICO has a code of conduct for CCTV users which recommends a sign is erected notifying visitors they are being recorded. | Parishes 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.

## What about my contracts with suppliers and partners?

PCCs should review their existing contracts in light of the 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 GDPR should be considered in future negotiations to ensure an adequate risk allocation with suppliers. In general, parishes should expect more lengthy and difficult negotiations with suppliers as they try to address their new exposure under the GDPR. If third party organisations provide parishes with services and they can access personal data then this applies to you.

| What's new? Contracts with data processors and joint controllers | |
|---|---|
| **DPA 1998** | **GDPR/new Data Protection Bill 2017** |
| The current law did not make contracts compulsory but it was regarded as good practice. | The 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 must be included?

- 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 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 PIAs, (https://ico.org.uk/media/for- organisations/documents/1595/pia-code-of-practice.pdf).

In ***Appendix 6 – DPIA Assessment Checklist*** there is a DPIA checklist to help you determine whether a DPIA is needed. 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 GDPR.

A short DPIA Assessment Questionnaire is in Appendix 6.

## Appendix 1 – Summary of the GDPR differences from the 1998 Act

The good news is that the GDPR's main concepts and principles are very similar to those contained in the current 1998 Act. The Information Commissioners Office (ICO) will still be in charge of data protection and privacy issues. Therefore, if you are complying with the 1998 Act, much of what you do will still apply. 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 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 Notices** | Under the 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 – Privacy Notices.*** |
| **Consent** | Consent is fundamental under the 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 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 DSAR has been reduced from 40 calendar days to one calendar month. The ability for a firm to charge up to £10 per DSAR has been removed and a breach must be processed free of charge. | The DSAR process will need to be reviewed and updated accordingly. |

## Appendix 1

| Change | Detail of Change | Impact of Change |
|---|---|---|
| **Data Privacy Impact Assessments (DPIA)** | The 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 – DPIA Assessment 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 you introduce a new IT system or launch a new website which collects data your 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 can only be retained where there are legitimate grounds or a legal obligation to retain the data. | 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 25th 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 parish. | 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 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 – GDPR Action Plan Checklist

| | |
|---|---|
| ① | **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 GDPR.<br><br>**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. |
| ② | **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 – Audit Questionnaire.*** |
| ③ | **Identify and document your 'lawful basis' for processing data** – To legally process data under the 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. |
| ④ | **Check your processes meet individuals' new rights** – The GDPR will give people more rights over their data. For example, the 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 8 rights.<br><br>**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. 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 GDPR the time limit for responding to SARs is reduced from 40 days to one month and the £10 fee is abolished. |
| ⑤ | **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 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 – Consent Form.*** |
| ⑥ | **Build in extra protection for children** – The GDPR says children under 16 cannot give consent (although this will be reduced to 13 in the UK) 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. |
| ⑦ | **Update your Policies & Notices**<br><br>**Policies** – Have clear, practical policies and procedures on information governance for staff to follow, and monitor their operation.<br><br>**Privacy Notices** - 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 privacy notices but they will all need to be updated. Under the 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 notices are in ***Appendix 5 – Privacy Notices.***<br><br>**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 24.<br><br>**Websites** – Control access to any restricted area. Make sure you are allowed to publish personal information (including images) on website/social media. |

## Appendix 2

⑦

**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 staff on the basics of information governance, where the law and good practice need to be considered, and know where to turn for advice.

⑧

**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 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.
7. Assist the controller with privacy impact assessments.
8. Assist the controller with security and data breach obligations and notify the controller of any personal data breach.
9. Return or delete data at the end of the agreement (but can keep a copy).
10. Demonstrate compliance with these obligations and submit to audits.
11. Inform the controller if their instructions would breach the law.

⑨

**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 will need to have the right procedures in place to detect, investigate and report a breach. The 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) attach – ensure up to date anti-virus software is in place.
  - Equipment theft – check security provisions.

⑩

**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 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, or reading it off a screen during a sales call. It includes transferring and altering data. Indeed, practically anything done to personal data constitutes processing.

| **Part A:** | **YOUR INFORMATION** | |
|---|---|---|
| 1. | 1. Person completing questionnaire<br>a) Name.<br>b) Role.<br>c) Telephone extension number.<br>d) Email. | a) .....<br>b) .....<br>c) .....<br>d) ..... |
| 2. | Data controller (e.g. PCC, Incumbent) | |
| 3. | Date you completed this survey | |
| **Part B:** | **COMMUNICATIONS DATA** | |
| 4. | 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:<br>**a) What type of information do we keep?**<br>E.g. Name, contact details Gift Aid information and congregational giving details such as bank details.<br>**b) Where do we get the data from?**<br>E.g. Individuals themselves, family members, clergy, other church sources, publicly available sources e.g. electoral register.<br>**c) Why do we collect or process the data – what do we do with it?**<br>For purposes relating to: e.g. church membership, and for contact regarding involvement in parish activities; advertising, outreach programmes [*Please list all reasons*].<br>**d) Who do we disclose communications data to?**<br>E.g. parish clergy, church members and contacts carrying out the work of the church, diocesan authorities, bishop, other church organisations.<br>**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.**<br>E.g. linked parishes, mission agencies, cloud storage | |

## Appendix 3

| | | |
|---|---|---|
| **Part C:** | **SUPPLIERS, COMPANIES, AND OTHER ORGANISATIONS WE CONTRACT WITH** | |
| 5. | About individuals or representatives of organisations which supply us with services such as for church repairs, or with whom we are in contact<br>**a) Who do we keep personal data about?**<br>E.g. Trades people, surveyors, architects, builders, suppliers, advisers, payroll processors, donors to appeals [Please list any others].<br>**b) What type of information do we keep?**<br>E.g. Name, contact details, qualifications, financial details, details of certificates and diplomas, education and skills [Please list any others].<br>**c) Where do we get the data from?**<br>E.g. the individuals, companies suppliers, [Please list any others].<br>**d) Why do we collect or process the data?**<br>E.g. church repairs and upkeep; maintain services e.g. electrical , gas, insurance [Please list any other reasons]. | |
| **Part D:** | **GENERAL QUESTIONS ABOUT PERSONAL DATA** | |
| 6. | 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? | |
| 7. | Do any procedures exist for rectifying, deleting, suppressing or blocking, personal information? If so, please provide details. | |
| 8. | 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. | |
| 9. | Can we provide a copy of all existing data protection or privacy notices and consents used? | |
| 10. | 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. | |
| 11. | Are we aware of any policies, processes or procedures to check the accuracy of personal data? | |
| 12. | In the event of a data security breach occurring, does the PCC have in place processes or procedures to be followed? What are these? | |
| 13. | 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? | |
| 14. | Can we locate a copy of the 'consent' language currently used for communications? | |
| 15. | 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? | |
| 16. | 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? | |
| 17. | Can we provide a copy of all website privacy notices and privacy policies? | |
| 18. | 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? | |
| 19. | 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? | |
| 20. | 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? | |
| **Part E:** | **PERSONAL DATA** | |
| 21. | 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.<br>**a) Who do we keep personal data about?**<br>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]<br>**b) What type of information do we keep?**<br>E.g. Name, contact details, date of birth, child registration information, Safeguarding information, information on employees. [Please list anything else]<br>**c) Where do we get the data from?**<br>E.g. The individuals themselves, other parishes, diocesan authorities, bishops, National Church, Deanery officers companies and recruitment agencies. [Please list anyone else]<br>**d) Why do we collect or process the data?**<br>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]<br>**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?<br>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]<br>**f) Who do we disclose the data to?**<br>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] | |
| 22. | 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:<br>(a) computer networks and connections<br>(b) CCTV and access control systems<br>(c) communications systems<br>(d) remote access systems<br>(e) email and instant messaging systems<br>(f) telephones, voicemail, mobile phone records<br>(g) intranet and Internet facilities<br>[Please list anything else].<br>Please provide copies of all notices, policies or procedures relevant to this monitoring. | |

# Appendix 4 – Consent Form

**(INSERT YOUR PCC LOGO HERE)**

**CONSENT FORM**

**Suggested introduction:**

"Your privacy is important to us and we would like to communicate with you about the church and its activities. To do so we need your consent. Please fill in your name and address and other contact information below and confirm your consent by ticking the boxes below."

You can find out more about how we use your personal data by reading our privacy notice which you can find here: [insert website url].

| | | If you are aged 13 or under your parent or guardian should fill in their details below to confirm their consent |
|---|---|---|
| Name | …… | …… |
| Address | …… | …… |
| | …… | …… |
| | …… | …… |
| Signature | …… | …… |
| Date | …… | …… |

Please confirm your consent to one or more of the following[1]:

☐ **Newsletters and other communications**

We may contact you to keep you informed about what is going on in the local or neighbouring parishes, other churches and the work of the Diocese including news, events, meetings, clubs, groups and activities. These communications may also sometimes appear on our website, the Diocese website or in printed or electronic form (including social media).

☐ **Activities and groups**

We may contact you about groups and activities you may be interested in participating in. We sometimes work with similar groups in other churches within or outside the Diocese or with the Diocese itself. Occasionally names and photos may appear in newsletters, bulletins or on websites, or social media.

☐ **[Optional Additional Activities for parishes to add if not included above.]**

**Keeping in touch:**

☐ Yes please, I would like to receive communications by email
☐ Yes please, I would like to receive communications by telephone
☐ Yes please, I would like to receive communications by mobile phone including text message
☐ Yes please, I would like to receive communications by social media
☐ Yes please, I would like to receive communications by post

[1] *You can grant consent to all the purposes; one of the purposes or none of the purposes. Where you do not grant consent we will not be able to use your personal data; (so for example we may not be able to let you know about forthcoming services and events); except in certain limited situations, such as where required to do so by law or protect members of the public from serious harm. You can find out more about how we use your data from our "Privacy Notice" which is available from our website or from the Parish Office or at [insert url]. You can withdraw or change your consent at any time by contacting the Parish office.*

# Appendix 5 – Privacy Notices

**[Insert Parish logo here]**

**GENERAL PRIVACY NOTICE**

(Note: This Privacy Notice is for non-role holders. See explanatory note on Privacy Notices on p.8)

**Your personal data – what is it?**

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the information alone or in conjunction with any other information. The processing of personal data is governed by *[the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the "GDPR" and other legislation relating to personal data and rights such as the Human Rights Act 1998*].

**Who are we?**

This Privacy Notice is provided to you by the Parochial Church Council (PCC) of [insert name of parish] which is the data controller for your data.

The Church of England is made up of a number of different organisations and office-holders who work together to deliver the Church's mission in each community. The PCC works together with:

- the incumbent of the parish (that is, our [vicar or rector]);
- the bishops of the Diocese of Rochester; and
- the Diocesan Office, which is responsible for the financial and administrative arrangements for the Diocese of Rochester.

As the Church is made up of all of these persons and organisations working together, we may need to share personal data we hold with them so that they can carry out their responsibilities to the Church and our community. The organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data.

Each of the data controllers have their own tasks within the Church and a description of what data is processed and for what purpose is set out in this Privacy Notice. This Privacy Notice is sent to you by the PCC on our own behalf and on behalf of each of these data controllers. In the rest of this Privacy Notice, we use the word "we" to refer to each data controller, as appropriate.

**What data do the data controllers listed above process? They will process some or all of the following where necessary to perform their tasks:**

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to our mission, or where you provide them to us, we may process demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you make donations or pay for activities such as use of a church hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The data we process is likely to constitute sensitive personal data because, as a church, 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 categories of sensitive personal data: racial or ethnic origin, sex life, mental and physical health, details of injuries, medication/treatment received,

political beliefs, labour union affiliation, genetic data, biometric data, data concerning sexual orientation and criminal records, fines and other similar judicial records.

**How do we process your personal data?**

The data controllers will comply with their legal obligations 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, and 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 following purposes:

- To enable us to meet all legal and statutory obligations (which include maintaining and publishing our electoral roll in accordance with the Church Representation Rules);
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments;
- To minister to you and provide you with pastoral and spiritual care (such as visiting you when you are gravely ill or bereaved) and to organise and perform ecclesiastical services for you, such as baptisms, confirmations, weddings and funerals;
- To deliver the Church's mission to our community, and to carry out any other voluntary or charitable activities for the benefit of the public as provided for in the constitution and statutory framework of each data controller;
- To administer the parish, deanery, archdeaconry and diocesan membership records;
- To fundraise and promote the interests of the Church and charity;
- To maintain our own accounts and records;
- To process a donation that you have made (including Gift Aid information);
- To seek your views or comments;
- To notify you of changes to our services, events and role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other fundraising activities;
- To process a grant or application for a role;
- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;
- Our processing also includes the use of CCTV systems for the prevention and prosecution of crime.

**What is the legal basis for processing your personal data?**

Most of our data is processed because it is necessary for our legitimate interests, or the legitimate interests of a third party (such as another organisation in the Church of England). An example of this would be our safeguarding work to protect children and adults at risk. We will always take into account your interests, rights and freedoms.

Some of our processing is necessary for compliance with a legal obligation. For example, we are required by the Church Representation Rules to administer and publish the electoral roll, and under Canon Law to announce forthcoming weddings by means of the publication of banns.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the hire of church facilities.

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

Where your information is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

**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 first 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):

- The appropriate bodies of the Church of England including the other data controllers;
- Our agents, servants and contractors. For example, we may 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 Rochester 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 Permissions may participate in our mission in support of our regular clergy;
- Other persons or organisations operating within the Diocese of Rochester including, where relevant, the Rochester Diocesan Board of Education;
- On occasion, other churches with which we are carrying out joint events or activities.

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

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits. In general, we will endeavour to keep data only for as long as we need it. This means that we may delete it when it is no longer needed.

**Your rights and your personal data**

You have the following rights with respect to your personal data:

When exercising any of the 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.

1. The right to access information we hold on you
   - At any point you can contact us to request the information we hold on you as well as why we have that information, who has access to the information and where we obtained the information from. Once we have received your request we will respond within one month.
   - There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee.

2. The right to correct and update the information we hold on you
   - If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. The right to have your information erased
   - If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold.

- When we receive your request, we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).

4. The right to object to processing of your data
   - You have the right to request that we stop processing your data. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you exercise your right to object, we may continue to hold your data to comply with your other rights or to bring or defend legal claims.

5. The right to data portability
   - You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.
   - You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. The right to object to the processing of personal data where applicable.

8. The right to lodge a complaint with the Information Commissioner's Office.

**Transfer of Data Abroad**

Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

**Further processing**

If we wish to use your personal data for a new purpose, not covered by this 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.

**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 details]
Email:

You can contact the Information Commissioners Office on 0303 123 1113 or 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 5

**[Insert Parish logo here]**

**PRIVACY NOTICE**
**ROLE HOLDERS**
(e.g. Churchwardens, PCC Secretaries, PCC Treasurers, Deanery Synod reps, Safeguarding officers etc.
See explanatory note on Privacy Notices on p.8)

**Your personal data – what is it?**

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the information alone or in conjunction with any other information. The processing of personal data is governed by *[the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the "GDPR" and other legislation relating to personal data and rights such as the Human Rights Act 1998*].

**Who are we?**

This Privacy Notice is provided to you by the Parochial Church Council (PCC) of [insert name of parish] which is the data controller for your data.

The Church of England is made up of a number of different organisations and office-holders who work together to deliver the Church's mission in each community. The PCC works together with:

- the incumbent of the parish (that is, our [vicar or rector]);
- the bishops of the Diocese of Rochester; and
- the Diocesan Office, which is responsible for the financial and administrative arrangements for the Diocese of Rochester.

As the Church is made up of all of these persons and organisations working together, we may need to share personal data we hold with them so that they can carry out their responsibilities to the Church and our community. The organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data.

Each of the data controllers has their own tasks within the Church and a description of what data is processed and for what purpose is set out in this Privacy Notice. This Privacy Notice is sent to you by the PCC on our own behalf and on behalf of each of these data controllers. In the rest of this Privacy Notice, we use the word "we" to refer to each data controller, as appropriate.

**How do we process your personal data?**

The data controllers will comply with their legal obligations 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, and 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 following purposes (for example some of the role-holders are volunteers and no financial information will be processed for these role holders): -

- To enable those who undertake pastoral care duties as appropriate (e.g. visiting the bereaved);
- To enable us to meet all legal and statutory obligations (which include maintaining and publishing our electoral roll in accordance with the Church Representation Rules);

## Appendix 5

- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments;
- To deliver the Church's mission to our community, and to carry out any other voluntary or charitable activities for the benefit of the public as provided for in the constitution and statutory framework of each data controller;
- To administer the parish, deanery, archdeaconry and diocesan membership records;
- To fundraise and promote the interests of the church and charity;
- To manage our employees and volunteers;
- To maintain our own accounts and records;
- To seek your views or comments;
- To notify you of changes to our services, events and role holders
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other fundraising activities;
- To process a grant or application for a role;
- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;
- To share your contact details with the Diocesan office so they can keep you informed about news in the diocese and events, activities and services that will be occurring in the diocese and in which you may be interested.
- We will process data about role holders for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations, for example to pay role-holders, monitor their performance and to confer benefits in connection with your engagement as a Role Holder. "Role Holders" includes volunteers, employees, contractors, agents, staff, retirees, temporary employees, beneficiaries, workers, treasurers and other role holders.
- We may process sensitive personal data relating to Role Holders including, as appropriate:
  - information about an Role Holder's physical or mental health or condition in order to monitor sick leave and take decisions as to the Role Holder's fitness for work;
  - the Role Holder's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- Our processing also includes the use of CCTV systems for the prevention and prosecution of crime.

**What data do the data controllers listed above process?**

- Names, titles, and aliases, photographs.
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our mission, or where you provide them to us, we may process demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving license numbers, vehicle registration numbers, taxpayer identification numbers, employee identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as salary, bonus, record of earnings, tax code, tax and benefits contributions, expenses claimed, creditworthiness, car allowance (if applicable), amounts insured, and amounts claimed.

- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Other employee data (not covered above) relating to Role Holders including emergency contact information; gender, birth date, referral source (e.g. agency, employee referral); level, performance management information, languages and proficiency; licences/certificates, citizenship, immigration status; employment status, retirement date; billing rates, office location, practice and speciality; publication and awards for articles, books etc.; prior job history, employment references and personal biographies.
- The data we process is likely to constitute sensitive personal data because, as a church, 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 categories of sensitive personal data: racial or ethnic origin, sex life, mental and physical health, details of injuries, medication/treatment received, political beliefs, labour union affiliation, genetic data, biometric data, data concerning sexual orientation and criminal records, fines and other similar judicial records.

**What is the legal basis for processing your personal data?**

Most of our data is processed because it is necessary for our legitimate interests, or the legitimate interests of a third party (such as another organisation in the Church of England). An example of this would be our safeguarding work to protect children and adults at risk. We will always take into account your interests, rights and freedoms.

Some of our processing is necessary for compliance with a legal obligation. For example, we are required by the Church Representation Rules to administer and publish the electoral roll, and under Canon Law to announce forthcoming weddings by means of the publication of banns.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the hire of church facilities.

We will also process your data in order to assist you in fulfilling your role in the church including pastoral and administrative support or if processing is necessary for compliance with a legal obligation.

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

Where your information is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

**Sharing your personal data**

Your personal data will be treated as strictly confidential. It will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with

- The appropriate bodies of the Church of England including the other data controllers;
- Our agents, servants and contractors. For example, we may 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 Rochester 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 Permissions may participate in our mission in support of our regular clergy;

- Other persons or organisations operating within the Diocese of Rochester including, where relevant, the Rochester Diocesan Board of Education;

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

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits. In general, we will endeavour to keep data only for as long as we need it. This means that we may delete it when it is no longer needed.

**Your rights and your personal data**

You have the following rights with respect to your personal data: -

When exercising any of the 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.

1. The right to access information we hold on you
   - At any point you can contact us to request the information we hold on you as well as why we have that information, who has access to the information and where we obtained the information from. Once we have received your request we will respond within one month.
   - There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee.
2. The right to correct and update the information we hold on you
   - If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.
3. The right to have your information erased
   - If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold.
   - When we receive your request we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).
4. The right to object to processing of your data
   - You have the right to request that we stop processing your data. Upon receiving the request we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you exercise your right to object, we may continue to hold your data to comply with your other rights or to bring or defend legal claims.
5. The right to data portability
   - You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.
6. The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. The right to object to the processing of personal data where applicable.

8. The right to lodge a complaint with the Information Commissioners Office.

**Transfer of Data Abroad**

Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

**Further processing**

If we wish to use your personal data for a new purpose, not covered by this Data Protection 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.

**Changes to this notice**

We keep this Privacy Notice under regular review and we will place any updates on this web page [add url]. This Notice was last updated in November 2017.

**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, [Add Parish details]
Email:

You can contact the Information Commissioners Office on 0303 123 1113 or 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 – DPIA Assessment Checklist

The 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.

1. Profiling is in use. Example: you monitor website clicks or behaviour and record people's interests. ☐
2. Automated-decision making. Example: when processing leads to the potential exclusion of individuals. ☐
3. CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects. ☐
4. Sensitive data. Examples: information about individuals' political opinions, as well as personal data relating to criminal convictions or offences. ☐
5. 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. ☐
6. Linked databases - in other words, data aggregation. Example: two datasets merged together, that could "exceed the reasonable expectations of the user". E.g. you merge your mailing list with another church, club or association. ☐
7. 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. ☐
8. "New technologies are in use". E.g. use of social media, etc. ☐
9. Data transfers outside of the EU. ☐
10. "Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking. ☐

**A more detailed DPIA Assessment Checklist can be found here [insert url]**