Modbury Mission Community
Connecting people with God

St. George's Church Modbury

pray grow serve with joy

Data Privacy Policy
General Data Protection Regulation (GDPR)

This policy has been developed for St George's Church, Modbury using the guidance and checklist produced by the Archbishop's Council 2017.

INTRODUCTION

GDPR will take effect in May 2018 and places a much greater emphasis on transparency, openness and accountability of data protection than previous legislation. The PCC will need to keep documents that show compliance with the legislation. This means we cannot just state we are compliant; we must prove it and provide evidence.

Fortunately, much of what we do in maintaining pastoral support and administration is based on 'legitimate interest'. If in regular contact with people, then this is covered under 'legitimate interest'.

If not in regular contact, the person should be asked if they would like to stay in contact and if they indicate they'd like you to stay in touch, they must opt in by completing a consent form. They must also be told that the can opt out at any time.

A particular fear of some churches is that they will no longer be able to encourage people to pray for someone by name. If prayer requests are spoken in church, you do not need consent. However, if people's names and reasons for the prayer request are recorded and published on the church website or in a parish newsletter, you will need consent. If in doubt, simply let the family or individual know that you would like to widen the prayer circle, and give them the opportunity to decline

Before 25 May 2018 any personal data held by the Church should be reviewed to ensure that details of those who have moved, died or asked to be removed from the list are deleted. Regular data cleansing should be carried out to ensure that any lists remain current.

This document highlights the key changes and provisions of the regulation and details the decisions and actions required to ensure compliance.

BACKGROUND

In accordance with GDPR, the PCC will ensure that all personal data shall be:

(a) processed lawfully, fairly and in a transparent manner;

(b) collected for specified, explicit and legitimate purposes and not further processed. This means that individuals should be told what we are going to do with their personal data before it is used and consent to such use;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are used;

(d) accurate and, where necessary, kept up to date. Personal data that is found to be inaccurate should be deleted or corrected without delay. All personal data should be periodically checked to make sure that it remains up to date and relevant;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. For instance, records of pastoral care discussions should not be kept for a number of years without justification. Records could be kept, for instance, if all identification features were removed, referred to as "anonymization";

(f) kept securely. Personal data storage should be safe and secure – in lockable filing cabinets or in password protected computer files. Names and addresses of individuals should not be left unattended.

Key changes and provisions

Awareness. In demonstrating compliance, the PCC is required to review their approach to governance and how they manage data protection. Therefore, the PCC and those running activities need to appreciate the impact of GDPR and identify areas that could cause compliance problems.

Information Held. GDPR updates rights for a networked world and the need to show compliance with the data protection principles by having effective policies and documented procedures in place. Therefore, the PCC will maintain accurate records of processing activities, what personal data is held, where it came from and with whom it is shared.

Communication. In collecting personal data, the PCC is duty bound to produce a privacy notice to give people certain information and how we intend to use the information provided. The GDPR requires the information to be provided in concise, easy to understand and clear language.

Individual Rights. The PCC accepts that GDPR includes the following rights for individuals:

- the right to be informed
- the right of access
- he right of rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- the right not to be subject to automated decision making, including profiling.

Lawful Basis for processing data. Under GDPR, some individuals' rights will be modified depending on the lawful basis for processing their personal data. In the parish context the most relevant include:

- Legal obligation, (e.g. a legislative requirement, such as processing gift aid applications or processing data in relation to the electoral roll);
- Legitimate interest, (e.g. general administration of church groups – rotas);
- Consent, (e.g. sending out a newsletter), (see below for more details);
- Contract (e.g. leases granted in relation to the church hall).

Consent. In preparation for the GDPR there is no requirement to automatically 'repaper' or refresh all existing DPA consents. However, if we rely on individuals' consent to process their data, consent must be freely given, specific, informed and unambiguous. Consent cannot be inferred from silence, pre- ticked boxes or inactivity. Any consent wording has to be sufficiently strong to show that the consent given is unambiguous and the person knows exactly to what he/she is consenting. Records will need to demonstrate what the individual has consented to, including what they were told, and when and how they consented. Simple ways for people to withdraw consent will also be implemented.

Children. GDPR will bring in special protection for children's personal data. The PCC will determine what systems need to be put in place to verify individuals' ages and to obtain parental or guardian consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16.

GDPR & Giving Reviews. There is a perception that consent will be required for all processing of data. However, consent is but one legal basis for processing personal data. Fundraising communications should be capable of passing a 'legitimate interest' test given that anyone who has proactively joined an Electoral Roll should be aware that churches fundraise and run stewardship programmes and should thus have a "reasonable expectation" that parishes should engage in this activity. Therefore, consent is not required. The Privacy and Electronic Communications Regulations means it can't be done by email, text message without specific consent.

Access Requests. Access requests must be completed within a month, rather than the current 40 days. Unfounded or excessive requests can be refused but the individual must be told why and that they have the right to complain to the supervisory authority and to a judicial remedy. This must be done without undue delay and at the latest, within one month.

Data Breaches. A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. It is compulsory to inform the Information Commissioner's Office (ICO) and the individuals affected when there is a high risk to the individuals involved (for instance, through identity theft). The ICO must be notified of a data breach within 72 hours of finding out about the breach. It is important to seek the advice of the Diocesan registrar about any suspected breaches without delay. (Mr Martin Follett – Diocesan Registrar 01392 687415. Email: martin.follett@michelmores.com)

More details can be provided after 72 hours, but initially the ICO will want to know the potential scope and the cause of the breach, mitigation actions planned, and how the problem will be addressed.

Procedures need to be in place to effectively detect, report and investigate a personal data breach and when to notify the ICO.

Deletion of Data. Any lists of personal data must be reviewed regularly to ensure that the list is targeted and does not include data of people who have died, moved or opted out. Any request to delete data will be handled to the data controller who will circulate it to those who hold data on that person. All parties will then confirm that the data had been deleted and the data controller will confirm with the individual that their request has been completed. A record will be maintained

Data Controller. The responsibility of Data Controller is undertaken by the Church Wardens, who will ensure compliance and assess governance arrangements. The Incumbent is considered to be a separate data controller from the PCC because they are a separate legal entity.

ACTION REQUIRED

The following actions were completed by the PCC to ensure compliance and will be reviewed annually before the APCM:

- Data Audit – Annex A
    - Review the types of processing activities carried out – who has what and why?
    - Identify the lawful basis for processing data and document them to ensure compliance with the GDPR's 'accountability' requirements.
- Update procedures and plan on how to handle requests to cover all the rights of individuals, including how to locate and delete personal data or provide data electronically and in a commonly used format.
- Review how consent is sought, recorded and managed and whether any changes are required to meet the GDPR standard
    - Managing Consent Checklist - Annex B,
    - Consent Form - Annex C
- Put systems in place to verify children's ages and to obtain parental or guardian consent for any data processing activity - Annex D
- Develop procedures to detect, report and investigate a personal data breach.
- Complete GDPR Checklist – Annex E
- Data Audit Findings – Annex F (in GDPR File)
- Annual Review to complete Data Audit and review Data Privacy Policy to be completed before APCM
- Privacy Notice – Annex G
- Removal register – Annex H (In GDPR File)
- Record of people processing data and signature that they have read and understood the requirements of the policy - Annex I (In GDPR File)
- Document action taken – Annex J (In GDPR File)

Annexes:

A. Data Audit
B. Managing Consent Checklist
C. Consent Form
D. Parental Consent Form
E. GDPR Checklist
F. Data Audit Findings
G. Data Privacy Notice
H. Removal Register
I. Acceptance Record
J. Document Record

ST GEORGE'S PARISH DATA AUDIT – 1 May 2018

Getting ready for GDPR

Review all your databases, email lists, spreadsheets, paper documents and other lists of personal data. If there are any issues, identify what you need to do. If action is not clear, then highlight questions needing further insight. New consent forms, privacy notices, and new or revised policies or procedures may need to be implemented to ensure compliance with GDPR.

Description	Why is the data held and what is it used for	Basis for processing data	Who holds the data and who can access it?	What security controls are in place?	How long is data kept for?	Is this covered by our privacy notice?	ACTION REQUIRED

MANAGING CONSENT CHECKLIST

Asking for consent

- ✓ We have checked that consent is the most appropriate lawful basis for processing.
- ✓ We ask people to positively opt in.
- ✓ We don't use pre-ticked boxes, or any other type of consent by default.
- ✓ We use clear, plain language that is easy to understand.
- ✓ We specify why we want the data and what we're going to do with it.
- ✓ We have named our organisation and any third parties.
- ✓ We tell individuals they can withdraw their consent.
- ✓ We ensure that the individual can refuse to consent without detriment.
- ✓ We don't make consent a precondition of a service.
- ✓ If we offer online services directly to children, we only seek consent if we have age-verification and parental-consent measures in place.

Recording consent

- ✓ We keep a record of when and how we got consent from the individual.
- ✓ We keep a record of exactly what they were told at the time.

Managing consent

- ✓ We regularly review consents to check that the relationship, the processing and the purposes have not changed.
- ✓ We have processes in place to refresh consent at appropriate intervals, including any parental consents.
- ✓ We consider using privacy dashboards or other preference- management tools as a matter of good practice.
- ✓ We make it easy for individuals to withdraw their consent at any time and publicise how to do so.
- ✓ We act on withdrawals of consent as soon as we can.
- ✓ We don't penalise individuals who wish to withdraw consent.

Modbury Mission Community

Connecting people with God

St. George's Church Modbury

pray grow serve with joy

CONSENT FORM

Your privacy is important to us, and we want to communicate with church members in a way which has their consent, and which is in line with UK law on data protection. As a result of a change in UK law, we now need to show your consent to how we contact you. Please fill in the contact details you want us to use to communicate with you:

Name: _____

Address: _____

_____

Email Address: _____

Phone Number: _____

By signing this form, you are confirming that you are consenting to the PCC holding and processing your personal data for church administration in including your details in the church directory, keeping you informed of events, news and appeals initiatives in the life of the church, and to enable the circulation of rotas.

Please tick the boxes where you grant consent:

I consent to the church contacting me by ☐ post ☐ phone or ☐ email.

☐ To including my details in the 'Church Directory' which is circulated to Church Members.

☐ To keep me informed about news, events, activities, appeals and services at St George's

☐ To enable the circulation of rotas

(note you can unsubscribe at any time)

Signed: _____ Dated: _____

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 to 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 PCC.

You can withdraw or change your consent at any time by contacting the PCC Secretary/ Parish Administrator via The Vicarage, Church Lane, Modbury, PL21 0QN. (01548 830260). Please note that all processing of your personal data will cease once you have withdrawn consent, other than where this is required by law, but this will not affect any personal data that has already been processed prior to this point.

Modbury Mission Community

Connecting people with God

St. George's Church Modbury

pray grow serve with joy

PARENTAL CONSENT

Your privacy and the protection of children is important to us, and we want to communicate with church members in a way which has their consent, and which is in line with UK law on data protection. As a result of a change in UK law, we now need to show your consent in how we contact your children. GDPR sets the age of consent at 16.

Please fill in the contact details you want us to use to communicate with you:

Name: _____

Address: _____

Email Address: _____

Phone Number: _____

Children's Names: _____

Children's Names: _____

Children's Names: _____

Children's Names: _____

By signing this form, you are confirming that you are consenting to the PCC holding and processing your personal data and that of your children for church administration.

I consent to the church contacting me by ☐ post ☐ phone or ☐ email.

(note you can unsubscribe at any time)

Signed: _____ Dated: _____

You can find out more about how we use your data from our "Privacy Notice" which is available from our website or from the PCC.

You can withdraw or change your consent at any time by contacting the PCC Secretary/ Parish Administrator via The Vicarage, Church Lane, Modbury, PL21 0QN. (01548 830260) Please note that all processing of your personal data will cease once you have withdrawn consent, other than where this is required by law, but this will not affect any personal data that has already been processed prior to this point.

GDPR CHECKLIST

Included in Master Document

GDPR Data Audit Findings

Modbury Mission Community
Connecting people with God

St. George's Church Modbury

pray grow serve with joy

Data Privacy Notice

The Parochial Church Council (PCC) of St George's, Modbury

1. Your personal data – what is it?
Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

2. Who are we?
The PCC of St. George's Church, Modbury is the data controller (contact details below). This means it decides how your personal data is processed and for what purposes.

3. How do we process your personal data?
The PCC of St. George's, Modbury complies with its obligations under the "GDPR" by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

We use your personal data for the following purposes: -

- 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 administer membership records;
- To fundraise and promote the interests of the charity;
- To manage our employees and volunteers;
- To maintain our own accounts and records (including the processing of gift aid applications);
- To inform you of news, events, activities and services running at St George's;
- 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.

4. What is the legal basis for processing your personal data?

- Explicit consent of the data subject so that we can keep you informed about news, events, activities and services and process your gift aid donations
- Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;

- Processing is carried out by a not-for-profit body with a religious or aim provided: -
    - the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and
    - there is no disclosure to a third party without consent.

5. Sharing your personal data

Your personal data will be treated as strictly confidential and will only be shared with other members of the church in order to carry out a service to other church members or for purposes connected with the church. We will only share your data with third parties outside of the parish with your consent.

6. How long do we keep your personal data[1]?

We keep data in accordance with the guidance set out in the guide "Keep or Bin: Care of Your Parish Records" which is available from the Church of England website [see footnote for link].

Specifically, we retain electoral roll data while it is still current; gift aid declarations and associated paperwork for up to 6 years after the calendar year to which they relate; and parish registers (baptisms, marriages, funerals) permanently.

7. Your rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- The right to request a copy of your personal data which the PCC of St. George's Church, Modbury holds about you;
- The right to request that the PCC of St. George's Church, Modbury corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for the PCC of St. George's Church, Modbury to retain such data;
- The right to withdraw your consent to the processing at any time
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable) [*Only applies where the processing is based on consent or is necessary for the performance of a contract with the data subject and in either case the data controller processes the data by automated means*].
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable) [*Only applies where processing is based on legitimate interests (or the performance of a task in the public interest/exercise of official authority); direct marketing and processing for the purposes of scientific/historical research and statistics*]
- The right to lodge a complaint with the Information Commissioners Office.

---

[1] Details about retention periods can currently be found in the Record Management Guides located on the Church of England website at: - https://www.churchofengland.org/about-us/structure/churchcommissioners/administration/librariesandarchives/recordsmanagementguides.aspx

8. 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.

9. Contact Details

To exercise all relevant rights, queries of complaints please in the first instance contact the PCC Secretary / Parish Administrator via The Vicarage, Church Lane, Modbury, PL21 0QN.

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.

GDPR – People who have requested to be removed from mailing list

In accordance with the GDPR regulations the following people have asked that their personnel data be removed from church records or have registered an objection.

NAME	DATE	ACTION	REMARKS

Acceptance Record

NAME	DATE	DATA HELD (rota, group, etc)

Document Record & Log

DATE	ACTION	WHO	REMARKS
Mar 18	Review Regulations		Parish Resources
22 Mar 18	Brief PCC, coordinate responses	Robin Chambers	
22 Mar 18	Data audit started		
4 Apr	Draft Data Privacy Notice		
15 Apr	APCM briefed on impact of GDPR – Privacy Notice issued to all attending, also copies in church	Robin Chambers	Copies issued to church members and held in church
22 Apr – 20 May	Impact of GDPR included in weekly notices	Robin Chambers	Copy in document folder
23 Apr	Review procedures, Summary and action required list produced		
6 May	Draft Data Handling and Protection Policy		
6 May	Managing consent Checklist Completed		
6 May	Develop Breach management procedures		
10 May	Data audit Completed		
12 May	Data Audit Findings produced and circulated to PCC	Robin Chambers	
12 May	GDPR Policy circulated to PCC for comment	Robin Chambers	
17 May	GDPR Policy Approved	PCC	Discussed at PCC meeting – recorded in Minutes of Meeting
17 May	Set Annual Review Date		Before APCM so changes can be briefed
27 May	GDPR Checklist complete		
28 May 18	GDPR Compliant		
