

BRIDGNORTH AND MORVILLE PARISHES TEAM MINISTRY	GUIDELINE No 4
TEAM COUNCIL COSTS AND BEST PRACTICE WORKING PARTY	GDPR

GENERAL DATA PROTECTION REGULATION (GDPR)

A new legal requirement on PCCs

An enhanced set of Data Protection requirements will come into effect in May 2018. These extend the existing Data Protection Act 1998 (DPA) requirements and place a legal responsibility on each PCC to comply. There are fines for non compliance.

Regrettably this area is complex and to comply requires a representative of each PCC to determine what steps are needed depending on the personal data held by the various members of the PCC. There is guidance material available from the Parish Resources web site (<http://www.parishresources.org.uk/gdpr/>) and there is no alternative to studying this. The main guides are detailed below:

- A 1 page GDPR checklist
- A 2 page GDPR introduction for PCC members
- A 12 page GDPR guide suitable for the person responsible for implementing GDPR in the parish/benefice

Before undertaking detailed study it is recommended that the following paragraphs are read through which are provided to point you in the right direction and address the main situations in the Bridgnorth benefice. Note that clergy can hold personal data in their own right (eg for pastoral care) which is subject to GDPR and must be addressed by them personally.

DPA 1998 Requirements

The DPA introduced requirements on management of personal data records through compliance with good practice principles, establishment of the Information Commissioners Office (ICO) and enactment of the right of individuals to obtain access to personal data held on them. Apart from complying with the record keeping principles the main impact on PCCs has been to ensure personal data is held “fairly and lawfully”. This can be achieved normally through the data being held for a legitimate purpose (eg gift aid details) or obtaining consent from the individual when they sign up to be included on a mailing list.

GDPR Requirements

The PCC is the **data controller** for the personal data it processes. The GDPR extends the DPA requirements making all data controllers, including PCCs, **accountable** for complying with the data protection principles. This means the PCC must detail the lawful basis for holding personal data – that is data which can identify a living individual. All lists of personal data which includes name, addresses and/or phone numbers and/or email accounts are subject to GDPR. It also requires organisations to have in place processes to meet the right of individuals to access their personal data. PCCs need to hold evidence that they have complied with the GDPR. It is important that personal data held for one reason is not used for something else unless evidence of consent from each individual is held for the additional purpose (eg a gift aid list cannot be used to issue a fund raising invitation).

Registration

Under current legislation PCCs, as not for profit organisations, are exempt from registering with the ICO **if data processing is limited to church membership list, gift aid, accounting and payroll records**¹ – this is expected to

¹ The ICO definition is – “you are only processing data for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are members of the body or association or have regular contact with it”.

BRIDGNORTH AND MORVILLE PARISHES TEAM MINISTRY	GUIDELINE No 4
TEAM COUNCIL COSTS AND BEST PRACTICE WORKING PARTY	GDPR

continue with GDPR. If any personal data at all, outside of church membership and financial records, is held and used the PCC will not be exempt from registering and paying the appropriate fee. This does NOT exempt the PCC from being subject to the GDPR legislation simply registration. Registration is required where for example pastoral records are kept on computer. If registration is required this can be undertaken on the ICO web site - cost is for tier 1 expected to be £40.

Steps Required

1. *Appoint a data representative* – each PCC needs a representative who can undertake a review of existing data sets and ensure the necessary steps are taken to comply with GDPR. In small parishes this could be the Secretary, Treasurer or a Church Warden.

2. *Undertake a data audit* – to show that the PCC has established the legal basis for the personal data it holds it needs to compile a list of the personal data sets maintained. Parish Resources website provides a template for this which should be used to list all personal data sets held by the PCC (see Appendix 1 below). The legal basis for holding the data should then be identified for each data set. There are a number of valid reasons for holding personal data but the “catch all” is that specific consent has been provided by the individual. However if the data is held for a specific purpose which is evident to the individual then consent is deemed to have been obtained (eg Electoral Roll, Gift Aid). Also, there is an exemption (section 9 (2) d) where personal data of church members and associated persons is held to discharge a specific function of the church– for example cleaning rota, tea/coffee rota, readers rota. The audit list will form the Register of Processing Activities (ROPA) when complete.

3. *Check compliance of the processes surrounding each data set and revise as necessary* – the requirements for maintaining, storing and retrieving data are summarised on page 7 of the Parish Guide. It is worth taking a common sense approach here as data sets are likely to be small and maintained on a laptop or sheets of paper. The principles to follow are listed on the summary guide as follows:

Personal data:

- will 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.
- collected on a data subject 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.

A pro forma table on Appendix 2 is detailed below to assist in this exercise.

If consent is required (eg. for a newsletter distribution list) and consent cannot be evidenced it will be necessary to obtain consent using one of the pro formas on Parish Resources.

4. *Draft and Agree a Privacy Notice* - each PCC will need a Privacy Notice to be adopted at a PCC meeting and displayed appropriately for the data types in use. A draft version of a Notice appropriate for a small parish is detailed in Appendix 3. Alternatively there is a more comprehensive version available on Parish Resources for you to customise to your PCC requirements. Where the data types amount to Electoral Roll, Gift Aid and other lists relevant to the church operation (eg rotas) the notice could be displayed on a notice board in church. If personal data is being collected on a web site the Privacy Notice will need to be visible on the web site so that consent is given with due regard to it.

BRIDGNORTH AND MORVILLE PARISHES TEAM MINISTRY	GUIDELINE No 4
TEAM COUNCIL COSTS AND BEST PRACTICE WORKING PARTY	GDPR

5. *Minute GDPR work at your PCC Meeting* – since there will be a legal obligation to comply it is recommended that the results of the data audit as well as the Privacy Notice are formally adopted by each PCC to evidence the PCCs actions.

Summary

To be ready for 25 May 2018 will require a degree of effort, the amount depending on the extent of personal data held. ***In all cases Bridgnorth PCCs need to undertake a full review of their personal data documentation to confirm they are in compliance.***

Author Tim Morris - timothy.morris@btinternet.com January 2018 (Updated April 2018)

APPENDIX 1

PARISH DATA AUDIT

Parish _____
Prepared by _____
Date _____

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. *It is suggested that this table format is used to create your own form to identify the data sets in use by your PCC. Use a format based on Appendix 2 as a working sheet to check compliance of each data set. This list will provide your Register of Processing Activities (ROPA) which must be retained.*

Description	Why is the data held and what is it used for	Basis for processing data – see Note 1 (e.g. consent, 9(2)d ²)	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
<i>Example: Gift Aid Declarations</i>	<i>For claiming Gift Aid</i>	<i>Consent given by completion of declaration</i>	<i>Held by Gift Aid Officer. Also accessed by treasurer</i>	<i>On paper, kept in a filing cabinet</i>	<i>Six complete calendar years after last gift claimed on the declaration</i>	<i>No – not yet written a privacy notice</i>	<i>Write privacy notice</i>

² Section 9(2)d is a special processing basis which allows religious (amongst others) not-for-profit bodies to process data 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.

BRIDGNORTH AND MORVILLE PARISHES TEAM MINISTRY	GUIDELINE No 4
TEAM COUNCIL COSTS AND BEST PRACTICE WORKING PARTY	GDPR

Note 1 - What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- (a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose (see example wording below).
- (b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests:** the processing is necessary to protect someone's life.
- (e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Possible wording for gaining consent would be

We hope you've enjoyed being with us and we would love to stay in touch with you. If you would like to be informed of future events and other church news please tick the box below and let us have your contact details.

Name _____
 Email Address: _____

If you tick the box, we will add you to our mailing list. You can unsubscribe at any time, [either by clicking on the unsubscribe link at the bottom of our emails, or] by contacting the Church Office (info@stagschurc.org.uk, ☎ 01234 567890).

BRIDGNORTH AND MORVILLE PARISHES TEAM MINISTRY	GUIDELINE No 4
TEAM COUNCIL COSTS AND BEST PRACTICE WORKING PARTY	GDPR

APPENDIX 2

CHECKS	DATA SETS USED BY PCC							NOTES
	Electoral Roll	Gift Aid and Planned Giving	Cleaning Rotas	Email list for News	Prayer Groups			
Legal Basis for processing	To meet legal obligation	Consent on form	Section 9 (2)d	Consent	Section 9 (2)d			
Evidence of consent maintained	n/a	Gift aid declarations	n/a		n/a			Exercise to obtain consent if not maintained
Is data used for another purpose?								Consent required for each use
Minimum amount of individual data held								Only data relevant to the purpose can be maintained
Completeness and accuracy controls in place								Evidence of data origination maintained
Data updated regularly								
Data confidentiality assured								Data must not be visible publically unless consent given
Data stored safely and securely								Data should be kept in a locked cupboard and if on computer, password protected
Retention periods operated								See Cof E 'Keep or Bin' leaflet for retention periods
Forms to collect data obtain consent adequately	n/a	n/a	n/a					Consent must be unambiguous and state how consent can be withdrawn.
Process to respond to access requests	n/a	n/a						Keep evidence of any access requests and how they were satisfied

APPENDIX 3

EXAMPLE – for illustrative purposes only. This will not be applicable in every Parish. If you wish to reapply this, you will need to replace the PCC name with your own throughout the document and put in relevant contact details in the highlighted place in Section 9.

DATA PRIVACY NOTICE**The Parochial Church Council (PCC) of ?????****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 ????? 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 ????? 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 ?????;
- 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 and keep you informed about diocesan events.
- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union 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 data³?

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 [redacted] holds about you;
- The right to request that the PCC of [redacted] 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 [redacted] to retain such data;
- The right to withdraw your consent to the processing at any time
- 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 lodge a complaint with the Information Commissioners Office.

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 at [insert contact details].

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.

³ 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>