DIOCESE OF GLOUCESTER

GENERAL DATA PROTECTION REGULATION (GDPR)

FACT SHEET FOR PCCS

1. Introduction

1.1 The General Data Protection Regulation (May 2018) replaces the Data Protection Acts and impacts every organisation – whether statutory, voluntary, or private.

1.2 The GDPR requires strong and robust processes in place regarding people's rights regarding information held about them; and about how information is requested, stored, shared or processed about any identifiable person.

1.3 The GDPR will have an impact on every PCC. The diocesan central offices will ensure that information is shared as widely as possible and advice and support given within capacity. The key link is: http://www.parishresources.org.uk/gdpr/ which has a series of templates that are useful e.g. privacy notices, consent forms, data audit etc.

2. Terminology – used throughout this policy and guidance

Personal Data	Information about a living individual who can be identified, either directly or indirectly from that information.
Processing	Anything done with/to personal data including using, sharing, deleting or updating personal data. Even just storing personal data counts as processing.
Data Controller	The person or organisation who is legally responsible for the personal data. In practice this is the person or organisation who decides "how" and "why" personal data are used. Sometimes there can be more than one data controller. For example, if a PCC shared information with the Bishop's Office following a complaint made by a parishioner then both the PCC and the Bishop's Office would be a data controller of that information.
Special Personal Data	This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, some

	biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. This replaces the definition of sensitive personal data under the Data Protection Act.
Subject Data Access	The right of the data subject to request to see all the personal data held about them within an organisation.

3. Overview and policy statement

3.1 At its core, the GDPR gives data subjects certain rights in their personal data. These rights are that the personal data:

- ✓ Will be collected and processed lawfully, fairly and transparently
- ✓ Will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- ✓ Will be collected on an `adequate, limited, and relevant' basis
- ✓ Will be accurate and where necessary kept up to date
- ✓ Will not be stored for longer than is necessary
- ✓ Will be kept secure

3.2 In addition to the principles, the GDPR gives individuals certain rights in their data. These rights are as follows:

- ✓ Right to be informed
- ✓ The right of access
- ✓ The right of rectification
- ✓ The right to be forgotten/erasure
- ✓ The right to restrict processing
- ✓ The right to data portability
- ✓ The right to object in certain cases
- ✓ Rights in relation to automated decision making and profiling

3.3 These rights are qualified and not absolute. For example, an individual is not entitled to all of the information held about them as some of it may be exempt. With the exception of the right to be informed, which we cover under section 6 below, further information on individuals' rights is set out in section 7 .

3.3 GDPR should be an item on the PCC agenda so that there is a shared understanding which can be further developed.

4. Where to start with the GDPR

4.1 As a first step you should carry out an audit to help you understand what personal data you hold. An example of a template to assist with this audit can be found here:

http://www.parishresources.org.uk/gdpr/dataaudit/

5. Accountability

5.1 One of the big changes with the GDPR is that it is not just enough to be compliant, PCCs must be able to "demonstrate" that compliance as well. Here we look at what this means in practice.

5.2 Record keeping generally: You should be keeping a record of the steps you are taking to become GDPR compliant, both before and after the GDPR comes into force.

5.3 Training and policies: You should ensure that everyone who handles personal data on behalf of the PCC is given training on data protection compliance. This should be backed up with a written policy. The key is to keep the training and policies simple and relevant to your practices rather than relying on legal jargon.

5.4 Privacy by design and by default: This can be quite a difficult concept to grasp in practice but it includes a requirement to:

i) Make data protection compliance an integral part of your practices. For example, if you were buying a new laptop for PCC use then you would need to be thinking about (and documenting) how the laptop will keep personal data secure in addition to the usual considerations, such as how much it costs and what features it has. For example, does the laptop come with built in encryption?

ii) Document how your practices comply with the data protection principles listed in paragraph 3.1 above. You could, for example, have a spreadsheet which lists the different ways in which you use personal data and how each use complies with the principles.

5.5 Data protection impact assessments (DPIAs): If you plan to use personal data in a way that is more risky than usual then you should carry out a DPIA. Examples could include sending out letters promoting a new after school club or social activities (this would, of course, be better done by handing out fliers or having accessible website information!). Each DPIA must include the following:

i) a description of the activity/initiative and its purpose;

ii) the nature of personal information that could be required and why what you are doing is necessary and proportionate;

iii) any risks associated with what you plan to do; and

iv) measures to be taken to prevent any risks. For example, to ensure that any appropriate practices around consents, storage, security and so on have been followed.

6. Transparency

6.1 Under the GDPR, data controllers such as PCCs must be transparent regarding how they use personal data. As part of this, they must make certain information available. For example, individuals have a right to know what data about them is collected, what it is used for and with whom it is shared. In addition, they should be made aware of their rights, be told for how long their personal data is kept, have the ability to challenge information, to make corrections, and so on. This information is usually provided in a document known as a privacy notice.

6.2 A sample privacy notice can be found here: http://www.parishresources.org.uk/gdpr/privacy/

6.3 Under the GDPR you have got to identify the legal basis that you are relying on to process personal data and the privacy notice must explain what bases are being relied on. One of the bases is consent, i.e. you are allowed to process personal data about an individual if they have consented. However, you should not be relying on consent if you can find another (more appropriate) legal basis. This is because valid consent can be quite difficult to obtain under the GDPR. In addition, an individual has a right to withdraw their consent, which could cause practical difficulties if you still needed to use someone's personal data after they had withdrawn their consent (for example, for legal reasons).

6.4 One area where consent may still be appropriate is in relation to marketing emails. Individuals must have consented before they are sent marketing communications (e.g. the electoral roll cannot be used as a basis for sending out fundraising/stewardship information, so a separate consent form is required to ensure that people have explicitly agreed to receive such information).

6.5 Consent must be freely given, specific, informed unambiguous and, in some cases, explicit as well. If you do rely on consent then any consent form must, in particular:

i) Clearly set out what the individual is consenting to. If you are asking someone to consent to more than one thing, then you should have separate tickboxes.

ii) Use an "opt-in" rather than an "opt-out" approach.

iii) Set out the individual's right to withdraw their consent.

iv) Be kept securely as a record that they have consented.

v) Not be "bundled up" with other matters. For example, you cannot make consent to receiving future marketing emails a pre-condition of attending a Parish event.

6.6 If you are processing special personal data then you will need to find an additional basis. As the definition of special personal data includes personal data about religious beliefs, much of the personal data you hold will count as special personal data. Your basis for processing special personal data can be explicit consent although we do not recommend consent if it can be avoided for the reasons set out above. In the absence of consent, a ground which may assist in many cases is that the processing is being carried out on condition that the processing "relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without consent."

7. Information security

7.1 The PCC will need to take steps to make sure that the personal data it holds is kept secure. This includes both technical measures as well as organisational / procedural measures. The requirements apply to personal data held on computer as well as most paper records. The sorts of measures you should be thinking about include the following:

i) Ensuring that confidential papers are kept in a secure location (e.g. in a safe) and that information held on computer is also secure (for example that it has been encrypted).

ii) Making sure there are rules around who can access information and how it is kept secure if you are travelling.

iii) Making sure that you have backups, for example, that you are able to restore personal data if a laptop used by the PCC is damaged beyond repair.

8. Data subject rights

8.1 The GDPR gives individuals new rights in their information (such as the "right to be forgotten") and also enhances existing rights (such as the right to make a subject access request).

8.2 Right of access: An individual has a right to request a copy of the personal data that the PCC holds about them. This is known as a subject access request (SAR). Under the GDPR, the time limit for responding to a SAR has been reduced to one month in most cases. The starting point is that the individual is entitled to all of the personal data that the PCC holds about them, but some information is exempt, for example, if disclosure would be unfair on a third party or would give rise to safeguarding concerns.

8.3 Right of rectification: An individual has a right to have inaccurate personal data corrected.

8.4 The "right to be forgotten" (erasure):In certain circumstances individuals have the right to request that their data is deleted. In such cases a PCC will review the reasons for that data being requested/processed, and follow up appropriately. The GDPR will allow a PCC to keep information, if appropriate, for example, if it is needed in order to defend a claim or to report safeguarding concerns.

8.5 Right of restriction: An individual has a right to require the PCC to restrict how their personal data is used. For example, if the individual claims that the personal data is inaccurate they can ask the PCC to restrict how it is used by the PCC until the inaccuracy is corrected.

8.6 Right to data portability: Individuals have a right to receive their personal data (or have it transferred to another organisation) in a format that can be read by computer. However, this right only applies in very limited

circumstances, specifically where the data was provided by the individual, is processed on a computer (as opposed to being in paper form) and the condition being relied on to process the data (see paragraph 6.3 above) is consent or necessary for fulfilment of a contract.

8.7 Rights in relation to automated decision making and profiling: Individuals have additional rights in some cases where their personal data is used to make decisions about them without human intervention. For example, if computer software is used as the sole means to determine if an employee would be given a pay rise.

9. Breaches and challenges

9.1 Where it is discovered that a PCC has breached its GDPR responsibilities it will need to investigate the alleged breach and to review the causes, and any remedial actions needed. In addition it may be required to report to the ICO (Information Commission Office). Under the GDPR, a breach must be reported to the ICO within 72 hours unless the breach is unlikely to result in a risk to individuals. When the breach is likely to result in a high risk to the rights and freedoms of individuals, the PCC will need to inform individuals affected by the breach as well.

9.2 PCCs should ensure that they have insurance provision for any data protection breaches under the GDPR. PCCs should also ensure that their insurers are involved in most cases where there is a breach, to ensure that the PCC does not inadvertently do something to invalidate insurance cover.

10. GDPR and Children

10.1 The GDPR explicitly requires organisations to be extra careful when handling personal data about children. Our policy is that information that is kept about any child is only kept with the express permission of the parents/guardians. (This excludes any safeguarding records that should be discussed separately with the diocesan safeguarding team).

10.2 No child under 12 should be included on social media without their parents' consent. For children aged 12 years and older we suggest getting consent from the parent and the child (assuming the child is mature enough to understand their rights).

11. GDPR and notes held on files regarding pastoral meetings

11.1 It will be usual in a parish for a number of people with pastoral roles to have notes of visits, supervision sessions and so on.

11.2 Notes should always be anonymised and not shared. Where personal data about an individual from a pastoral visit is to be shared for example on an intercessions list compiled on someone's computer – the individual should agree that they would like their name added to the list. Or where a child is on the intercessions list, their parents should have agreed to that.

12. GDPR and notes held on files regarding safeguarding concerns

12.1 There will be times when safeguarding records are required, parish checklists updated, new parish safeguarding nominated people, and `casework' concerns raised.

12.2 Safeguarding records should be kept securely and encrypted.

12.3 Advice about how long to keep a casework record should be discussed with the safeguarding team. In some cases where general advice was sought there will only be the need for the minimal and anonymised information to be kept – for others with specific needs, follow up, offender agreements etc, these will need to be kept securely, usually by the Incumbent, the Parish Safeguarding Nominated Person only.

12.4 In a vacancy the Archdeacons and Area Dean should be aware of any offender agreements in place and any risk assessments being undertaken, in order to join up information. The diocesan safeguarding team have the responsibility for this.

13. GDPR and information about people on teams, volunteers, group leaders etc

13.1 Incumbents and PCCs will have all sorts of details about individuals who run or are part of teams, who run all sorts of activities.

13.2 Information stored should be kept to a minimum and individuals should be told very clearly what happens to their personal data. In some cases their consent may be required.

13.3 When an individual leaves a team or no longer volunteers or moves on, and there is no legal reason to keep their details, then their record should be deleted.

14. GDPR and storage of records

14.1 Where a PCC employs people directly, you should not ask for consent to keep their personal data. Instead you should ensure that they are given a privacy notice which clearly sets out how their data is used. Consent will only be appropriate to specific uses of employee data, if at all.

14.2 The national church guidance currently for the length of time to keep records is:

a) For children's activities – the simple details of where there were Sunday Schools, holiday clubs, choirs etc **= 50yrs after the activity has ceased**

b) Where there were safeguarding records relating to concerns raised or any risk assessments etc **= 70yrs after the last contact with the individual.**

(The diocese could retain these records for a PCC but a separate agreement about records storage will need to be agreed and a PCC minute of what has been agreed so that there is always clarity of access).

c) Personnel files for employees (or volunteers where these are available) for anyone working with children or vulnerable adults **= 75yrs after employment**.
(The diocese could retain these records for a PCC but a separate agreement about records storage will need to be agreed and a PCC minute of what has been agreed so that there is always clarity of access).

d) Application forms for those not successful at application stage **=1yr after the role has been filled. Then the form should be shredded and destroyed.**

15. GDPR and general parish records

15.1 The **Electoral Roll** is a legal roll and records cannot be destroyed. Applications should follow the Church Representation Rules. However the person retaining the forms should keep them secure and they should be encrypted.

15.2 If a PCC wishes to use the electoral roll as a basis for sharing information it will need to be satisfied that such use is lawful. For example, if the PCC wishes to use the electoral roll to send people information about events and activities then this will usually require consent. All forms should be kept secure and encrypted.

15.3 **Stewardship details, gift aid** etc – are `direct marketing' issues where data can be both legally requested and processed. However at the time of being collected there should be specific consent obtained, along with privacy notice information that reassures that the information will not be shared and will only be used for the purposes for which it was requested. All forms should be kept secure and should be encrypted.

15.4 Information collected at, and follow up visits from; baptisms, weddings and funerals: the simplest way to ensure that individuals are happy to be contacted following such an event is to tell them in person that the church would like to invite them to e.g. an annual service of remembrance; anniversary of baptism event etc. If they agree, ask them to sign the letter and pop it back to the incumbent/parish office etc so that they have expressly consented to being contacted. All such letters should be kept secure and where records are kept on a personal computer the file should be encrypted. You may want to do this for a fixed period e.g. 2 or 3 years and then review or update your lists.

15.5 In very general terms it is fine for a death or anniversary of death to be announced in a parish newsletter as the GDPR refers to people who are living and can be identified because of the information requested/kept.

15.6 For Baptisms and Weddings - just to contact a family after an event for the purposes of following up specifically from that event is fine. If you want to

contact them, for example, with information about stewardship or events this is `direct marketing' and as such requires specific consent.

16 GDPR and PCC, officers, and Churchwardens

16.1 At the outset of a new PCC year it would be sensible to ensure that each member is aware that their information (address, phone, email for example) will be shared for specific reasons e.g. circulating minutes, agenda, papers, information sharing, general church business related emails etc. This way any communication done electronically is shared appropriately – and if an individual then decides they do not want their information further shared then you can consider that request further.

17 GDPR and PCCs and Incumbents

17.1 Incumbents are separate from the PCC because they are separate legal entities. They are separate data controllers. However, there is likely to be overlap of information held or shared through parish administrators, treasurers, pastoral teams, administrators, etc – so the same provisions throughout this fact sheet apply to both the PCC for ensuring governance and oversight, and for incumbents managing their own information.

18. GDPR and parish newsletters and noticeboards

18.1 There will probably be lists that people have for the distribution of newsletters etc. These people will need to have consented to receiving the newsletter etc, so add this to your list of people to contact. Spreadsheets of information should be encrypted. In some cases you will need consent before sending communications to organisations as well.

18.2 Good idea to check on the noticeboards post-May that there isn't anyone named that doesn't know that their name is there!

19. GDPR and CCTV cameras, or where there are centrally employed staff working in offices with IT equipment.

19.1 A new policy will be needed regarding CCTV in churches – and there is further advice about this https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

19.2 Where a PCC wishes to have an HR policy regarding staff accessing unsuitable material on the internet, or using the internet/emails at work for personal use – this will require a separate policy which is then included in the employment handbook and staff should be given a copy so that there is an audit trail of it being received and understood. In addition, the PCC should carry out a DPIA (please see paragraph 5.5 above).

20. GDPR preparation

There is a really helpful checklist on the http://www.parishresources.org.uk/gdpr/ website. This includes:

	Activity	When?	Y/N
1	Read this guidance alongside: http://www.parishresources.org.uk/gdpr/		
2	Nominate someone from the Parish to be the data person to help support the PCC	Jan-March	
3	Review all the information you have about any individuals or groups of individuals and check you still want that information and why it is used http://www.parishresources.org.uk/gdpr/ pg 7 If you don't need that information anymore ensure it is properly deleted/destroyed/shredded. If you do need that information write to the individuals to give them a copy of your privacy notice. In some cases you may need consent as well. Retain all your letters or enquiries and keep them secure and in an encrypted file.	Jan-March	
4	Check what security systems are already in place and where there are gaps that need attention.		
5	Ensure that there is one overarching list of information along with what processing takes place, who is responsible for it, who has access to it, and why it's a justified reason for asking/processing that data. Do this for each new activity too so that you have a checklist for GDPR compliance and aren't at risk of any breach. http://www.parishresources.org.uk/gdpr/ pg 11		
6	Draft a letter to go to all those for whom you now need to have consent to hold their records/information - check you keep letters securely and files updated and encrypted. http://www.parishresources.org.uk/gdpr/ Gaining Consent		
7	Check your church website has a Privacy Notice on it – the http://www.parishresources.org.uk/gdpr/ has		

	a template you can use		
8	Check the lists for those who receive parish newsletters or bulletins Check if any information about anyone is on a noticeboard – where they may not know!		
9	Check that GDPR is on a PCC agenda, so that the members are aware of responsibilities and risks		
10	Please do visit our GPDR website page, work through the templates and guidance and email any questions to our FAQ page - gdpr@glosdioc.org.uk		

Jan2018