St Peter's Wellesbourne & St James Walton d'Eivile

A Policy & Brief Guide to Data Protection

What's happening and why is it important?

The General Data Protection Regulation (GDPR) will take effect in the UK on 25th May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection in how their personal data is used by organisations. Parishes must comply with its requirements, just like any other charity or organisation. This guide tells you what you need to do.

Policy & Underlying Principles

The law is complex, but there are a number of underlying principles, including that personal data:

1. will be processed lawfully, fairly and transparently

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

3. 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.

4. must be "accurate and where necessary kept up to date."

5. should not be stored for longer than is necessary and storage is safe and secure.

Explaining the jargon:
Personal data is information relating to a living individual, who can be identified directly from that data or indirectly by reference to other data held.
Processing is anything done with/to personal data, including storing it.
The data subject is the person about whom personal data are processed.
The data controller is the person or organisation who determines the how and what of data processing, in a parish usually the incumbent or PCC.

Guidance for PCC's is provided by the Archbishops Council and an outline of the key points is detailed below.

Key Points for Parishes

1. There are several legal bases for processing data, of which consent is one. Others include legal obligation (e.g. processing Gift Aid or publishing the Electoral Roll), contract (e.g. letting out the church hall), or legitimate interest (routine church management involving rotas, lists of group members etc). For each area of processing, you will need to be clear on your legal basis for carrying out that processing.

2. You may need to have **consent** from people for some data processing; e.g. some email communications, or where data is shared with church members such as in a church directory.

This will need to be clear and unambiguous – some form of positive action to 'opt- in'. You must ensure you have this consent before processing.

3. 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'. The PCC will need to make provision for people to exercise these rights, including developing a Privacy Notice. 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. For example, where you process on the basis of consent, you should retain those consents. Since consent should be specific to a "purpose", you may need separate consent to cover different areas of data processing within the life of the church.

4. Where data "reveals religious belief" it becomes special category data – which requires additional care with regard to processing. We are currently clarifying what this means in the context of parishes. Until then we suggest that belief cannot be assumed simply because someone attends church or church events, becomes a "friend" or gives money to a church. However, where someone is required to have affirmed belief (e.g. that they are baptised or that they are a member of the Church) e.g. processing of the electoral roll, then this could be argued to reveal religious belief.
A second legal basis is required for processing special category data, but the GDPR allows religious (amongst others) not-for-profit bodies to process such data without specific consent as long as it 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.

5. Note that each incumbent or priest-in-charge is considered to be a separate data controller from their PCC because they are separate legal entities.

6. 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". The good news is that PCC's should remain exempt – we will let you know when further details are available.

Areas for Action

You may find our one page checklist helpful in making sure you've covered all the areas. Essentially parishes are likely to need to consider three areas for action:

1. This is the perfect time to review what data you hold, how you store it, and what basis you have for processing it. A simple audit template has been used.

2. We need to have a Data Privacy Notice. This has been prepared for consideration.

3. You may need to gain consent from some data subjects. Sample forms and guidance are available. Remember though that there will still be some data processing you can do as part of normal church management that doesn't need specific consent for that particular action – for example, lists of group members.

Further help available

1. This is a short guide for PCC members. There is a more detailed guide on the following website http://www.parishresources.org.uk/wp-content/uploads/Parish-Guide-to-GDPR.pdf

2. The Information Commissioner's Website has much helpful guidance: ico.org.uk