Information Management Policy Review for the Parish of Three Saints

Author: Ged Keele, Information Management Champion April 2018

1. Background

The Parish of Three Saints (TPoTS) set up a review of Information Management (IM) in September 2017. In early 2018 this review incorporated the requirements of the General Data Protection Regulations (GDPR). The new act of Parliament incorporates previous principles of the Data Protection Act 1998 and provides extra protection to the individual data subject. Under this legislation TPoTS is required to state a formal policy on the management of *personal data* that it processes. This policy document is divided into two sections. The first concentrates on the *extra* requirements generated by GDPR, and the second is concerned with the well established aspects of data protection.

2. Changes required to Parish IM procedures under GDPR.

The key changes in the new Act relate to the rights of individuals to control *personal data*. The organisation that is recording personal data is required to obtain *informed consent* from an individual and *record* the fact that they have obtained this consent. In this consenting process the rights of the individual in relation to their personal data must be explained in a *privacy notice*. There are various organisational requirements that need to be fulfilled under the act. The PCC becomes a *data controller* and is responsible for ensuring the requirement of GDPR are fulfilled. It is obliged to appoint someone to oversee the implementation of GDPR. In this policy we outline the **organisational approach** taken by the parish of three Saints, and detail the steps that we are taking to **implement the consent process** under the GDPR. As well as the new requirements under GDPR there are principles relating to **data security** under the old act. These are dealt with in the final section of this policy review.

2.1 TPoTS Organisational response

Initial steps:

- PCC members have been made aware of their responsibilities as *data controller*
- The role of Information Management Champion has been created
- The Information Management Champion and the Parish Administrator have both undertaken specific training in implementing the new regulations
- A data analysis has been undertaken to identify the areas in which personal data is held by the parish
- As a result of this analysis various actions as detailed below have been taken

Before we detail our response we wish to highlight some grey areas in the implementation of the act. We have been in correspondence with other Parish offices who have responsibility for

implementing the act and we recognise that there may be specific circumstances under which *consen*t from individuals need not be obtained through a *privacy notice*. Certain personal data can be exempted if it can be proved that there is a *legitimate reason* for processing the data. For example a person who is on the electoral roll can expect to receive communications about the parish on a wide range of matters, and these could include requests for financial support. There is therefore an argument that signing up to the electoral register roll *in itself* provides the consent for a wide range of communications. Some Parishes in the Diocese appear to be leaning towards the view that the argument over legitimate processing can be used to avoid issuing privacy notices in any circumstances. We recognise this argument and have incorporated it into our policy for implementation of the consent process. However, we stress that, in order to comply with the general principles of the act, we should be issuing privacy notices as a general rule. In arriving at this conclusion we have consulted the Church Of England Parish Resources website, which provides advice on circumstances in which it is possible to use the legitimate processing argument (http://www.parishresources.org.uk/gdpr/).

2.2 Consent and obtaining privacy notices

In our data usage personal data is confined to *contact details, volunteer roles, financial contributions made by individuals and visual images*. A further level of processing is added by the fact that data may be *analysed to establish details of personal activities eg church attendance*

In our initial discussions on implementation of GDPR we were concerned that this could add to the administrative workload of the Parish. The key areas that we thought would be impacted appeared to coincide with the need for a person to sign a form. We therefore decided to adopt the principle **that we would concentrate on modifying forms that record personal data so that they would incorporate a privacy notice**. This would allow us to maintain our current procedures for storing the forms in paper format. We were also concerned to ensure that **implementation of consent did not impact significantly on our organizational framework, including the structured recording of personal data.**

Attendance at the local training sessions raised a number of other procedural issues. In particular the **use of emails, the storing of telephone numbers and how we manage visual images.**

Following our Data Analysis we have arrived at the following classification of our personal data:

- Membership management e.g Electoral roll, Friends and Church
- Using email and telephone numbers for communication
- Managing PCC activities (PCC members personal data used)
- Managing data relating to volunteer activities which include rotas, pastoral care activity
- Managing stewardship and donations
- Managing baptisms, marriages and funerals
- Managing records of visual images
- Analysing data about membership activities
- Data held under safeguarding procedures

2.2.1 Membership management

The Parish has three broad levels of membership and there is overlap between all three. Many The largest membership category is the Electoral Roll, and Church members are very likely to be on that list. Some of the Friends membership overlaps with the Electoral Roll. All categories of Members are likely to be involved in financial transactions

***Action**: Membership forms for Electoral Roll will be redesigned to include a Privacy Notice that will be signed and retained. However, we will not do this for the Electoral Roll until a new Roll is set up in 2019. In the interim we consider that we can continue to hold and process the data on grounds that it continues to be legitimate to do so.*

2.2.2 Using email and telephone numbers for communication

There are a number of issues that need to be considered here. First, our training session stressed the need to try to separate Parish email use from personal use. Second, it is important to recognize that in sending emails it is very easy to pass on another person's details unwittingly. This is done by sending emails in **open copy ie "cc".** On the other hand sending them **blind copy ie "bc"** provides protection against sending other people's emails to recipients that they might not wish to have their email addresses. The advantage of sending open copy is that an *email conversation can be set up between all recipients*. On the other hand a circulation to a large group eg Electoral Roll, or Friends *must be sent by blind copy.*

***Actions**: 1. We have already set up a number of bespoke email addresses within the Parish. This list will be expanded to include the **Treasurer, the Pastoral Care Coordinator, and the Alzheimer's and Dementia Carers Group**. 2. We shall send out a Privacy Notices by email to all members of the PCC and the Readers/Stewards rotas to ensure that everyone understands the principles of shared use of emails*

2.2.3 Managing data relating to volunteer activities which include rotas, pastoral care activity

The Parish has an established set of IM procedures to record personal details that include spreadsheets and databases. Volunteer roles (eg readers, stewards, Friends etc) are recorded on one of the databases. There is an issue of how far the Parish should go in recording these roles. Some large charities, such as the National Trust, go to great lengths to record details about their volunteer activities. However, they utilise their data in their internal accounting procedures. The difficult from a management perspective is that these systems require constant updating to perform their function properly. Further, this updating is formally required under the basic principles of data protection:

This is largely a technical issue that will be dealt with in discussions about information management in the Parish Office. It is mentioned because decisions on how databases are set up will have an impact on the efficiency of Parish Administration.

2.2.4 Managing stewardship and donations

As everyone is aware the Parish runs regular Stewardship campaigns to raise money. We also receive ad hoc donations and membership subscriptions through Friends. In the process of receiving money we hope to add value by obtaining consent for claiming Gift Aid from the donors. There are some complex aspects to this process, and these are managed through established processes.

Action*: The forms that are signed by donors have been reviewed and some minor modifications will be required to ensure that the forms can perform the extra function of providing a Privacy Notice.*

2.2.5 Managing baptisms, marriages and funerals

There are two issues in relation to forms in this area. The first is the justification for storing the personal data and the second concerns passing personal details on to third parties. The first does not concern us under GDPR because our holding this personal data is justified by the principle on legitimate processing. The second is more problematic because there have been instances when third parties have obtained personal data and misused it. This is a difficult issue because we do not control what happens to the data if it is passed to someone else.

Action*: It should be possible to insert a clause into forms that are signed to the effect that personal details may be disclosed to third parties, but we probably need to go further than this and set up a protocol to ensure that those who are signing the forms can be in full control of this process.*

2.2.6 Managing records of visual images

The situation here appears to be confused. At our training session the speaker appeared to be saying that if an image was stored *all people in the picture required to be identified*. This makes storage such images a nightmare. However, complying with a request for data could include a request for all photos of the subject, *so how do you locate such "individual" pictures amongst all the others?!?* We shall have to discuss this. **But one thing is quite clear and that is that children should not have their photos taken unless there is prior parental approval. Whether this is done in writing needs to be discussed.**

2.2.7 Collating and analysing data about donations and volunteer activities

The Parish undertakes occasional surveys eg church attendance and the databases used for membership / volunteer roles have been configured so that data can be collated efficiently. People whose data is subject to these analyses need to be aware that this is happening. It is also important to stress that this data is held confidentially and not made available in an identifiable form.

Action: *a clause will be inserted into Privacy Notices to this effect*

2.2.8 Data held under safeguarding procedures

Data on safeguarding issues needs to be treated separately from other personal data. Since it will almost certainly relate either to physical / mental health or sexual issues it comes under the category of *sensitive personal data.* Further it is highly likely that the data could be used in future legal proceedings. Sensitive information must be protected with a higher level of security and it is recommended that sensitive records are kept separately in a locked drawer or filing cabinet. Sensitive personal data must never be kept on laptops, or portable storage (such as USB drives) unless the device or the file has been encrypted.

Action: *When safeguarding issues arise the information will be kept as a paper record and in a locked cabinet. It may be printed (and we would recommend that it is for legibility) but any files so created should not be saved to any electronic storage medium. The paper files should never be destroyed because of the possibility of future legal action.*

3. Data management, security and confidentiality

The Parish has to comply with the established principles of data protection, which are:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects (individuals) which are:
    1. To view and amend their data
    2. To request a copy of their data
    3. To request that data is deleted
- Appropriate measures shall be taken to secure the data against unauthorised or unlawful processing.

3.1 Data management

Modern data processing applications can provide efficient solutions to these problems, but problems can arise when the technology becomes over complicated. For example, encryption of data may be part of an effective solution to data security but the need to encrypt/decrypt files can introduce practical problems of implementation. Further, databases may provide efficient vehicles for inputting and outputting data, but the more complicated data outputs may demand that excessive amounts of data must be input. There is often a delicate balance to be struck in the use of information technology. Having said that an effective and efficient system of information management can be developed with standard applications of word processor, spreadsheet and database. These tools can also be used to publish data in secure documents and to communicate via email and the web.

3.1.1 Our approach to managing personal data

The Parish uses standard Microsoft tools for most of its data processing eg Word, Excel, Access and Publisher. For recording personal details we currently use a both Excel and Access. The latter is a database and recording data using this tool allowa us to have a central reference point for all our personal data. Once the data has been input it should be possible to transfer it throughout the Parish applications without amendment. The key features of an Access database are that forms can be set up reasonably simply for input of data. Once the data is input creating output in the form of rapid analysis queries, reports that can be tailored to user requirements and the export of data becomes relatively simple.

If we now look at the principles of data protection

3.1.2 Personal data

The key elements of personal data that we record are *contact details*, and *roles in the Parish*. these are held on a database. If the data is held on a database this makes the requirement to *view, copy, amend or delete data* a simple process.

3.1.3 Adequacy and relevance of data

The requirement for data to be *adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed* will be dealt with by ensuring that our data management systems do not require excessive data and are not overcomplicated. An example is the use of data in rota systems. It is perfectly possible for the Parish to use an Access database application for *all rotas* within the Parish. However, this would require us to record data on all personal roles within the Parish. We shall confine ourselves to using the database to manage the relatively complex data requirements of the Worship and Steward/Refresher rotas. By contrast cleaners rotas are simple and can be done on a word processor.

3.1.4 Accurate data that is kept up to date

Personal data shall be accurate and, where necessary, kept up to date. This requirement is self-explanatory. Nevertheless, certain practical points should be noted. The principle of inputting data *once and once only* is easier to state than put into practice. Email addresses are an example of this. We may be able to set up a central database with a current email address, but we do not currently have a database that can support automated email delivery. We have the facility to create appropriate lists of email addresses but uploading them into the appropriate contact lists remains a problem. Administrative vigilance is required both from our data subjects, who must notify us of changes, and ourselves to ensure that changes are implemented throughout our circulation lists.

3.1.5 Deleting data

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. Essentially this means that the Parish must ensure that data is deleted when the status of a person changes

3.2 Security and confidentiality

In our data analysis we have covered both paper and electronic records

3.2.1 Paper processes

Our review has included the paper processes on which we record personal data. In particular we have had a concern to ensure that sensitive financial and personal details e.g bank details and copies of passports are not exposed either to casual inspection in the office or by an office burglary.

Action*: a protocol has been set up to ensure that sensitive personal details are kept in a locked filing cabinet (we have mentioned safeguarding data in section 228 of this report)*

3.2.2 File security

In the data analysis we have undertaken we have reviewed security as applied to electronic files that record personal data.

Action*: the principle we are adopting is that all files that list personal data should be doubly protected. The device used for recording should have a password set to prevent unauthorised access. This is particularly important for laptops and mobile phones that are prone to theft and loss. The files themselves should also be password protected on the actual device.*

3.2.3 Backup

File backup is part of the process of data security. One difficulty we face is that the office computer is not the only device on which people store data. We also wish to take a reasonable review of the problem and apply rules for backup that fit the relative importance of the data that is being backed up. Critical files such as financial data core database records and PCC records are essentially for the ongoing administrative support of the PCC and will be treated differently from non-critical files that support activities but would not cause a major administrative issue if they were lost. We have decided to adopt a cloud based approach to backup and have selected Google Drive as a general back-up framework. Our data analysis has shown that this can now be achieved by backing up the files of three, possibly four devices to Google Drive

Action*: ensure that the office PC, the treasurer's laptop and the Data Champions PC are backed up to Google Drive. It is important to ensure that those who own their own devices for recording Parish data use sound backup procedures.*

3.2.4 Protection of computers

Computers must be protected from data loss caused by computer malfunction and malicious damage to data by viruses and adware.

Action*: Protection of data loss will be ensured through by virtue of the fact that we have the means to restore our system from rescue files and downloading an data from the cloud backup media. Protection against viruses and adware will be achieved through using commercial software.*