Parochial Church Council of the Ecclesiastical Parish of All Saints' Sidmouth

Data Protection Policy

In approving and publishing this Policy, the PCC acknowledges that its procedures are not yet fully compliant. However, the PCC commits itself to working towards the complete implementation of this Policy by 25 May 2018.

Adopted 09/01/2018

1. Introduction to this Policy

As individuals, we want to know that personal information about ourselves is handled properly. We and others have specific rights to data privacy as set out in legislation. In the course of our activities at All Saints', we will collect, store and process personal data. We recognise that the correct and lawful treatment of this data is not only a statutory obligation but will also maintain confidence in the Church and can support operational efficiency.

The legal safeguards are set out in the Data Protection Act 1998 (the Act). The Act imposes restrictions on how we may process personal data, and a breach of the Act could give rise to criminal sanctions as well as adverse publicity.

The Data Protection Act will be superseded from 25 May 2018 by a new Act that supplements it and implements the General Data Protection Regulations (GDPR) set out by the EU. This policy includes compliance both with the current Act and GDPR. The main concepts and principles of the GDPR are very similar to those of the Act but it also introduces a greater emphasis on transparency, openness and the documents we need to keep in order to show that we comply with the legislation.

We will endeavour to comply with the requirements of current Data Protection legislation, with best practice as disseminated to us by the Diocese of Exeter and any specific advice provided by the Diocesan Registrar.

2. Scope of this Policy

This policy statement applies to all employees, to the Electoral Roll Officer, the Treasurer, the Safeguarding Team, the Pastoral Care Team and to all other volunteers who, as part of their responsibilities, process personal data and/or use that data to communicate information about the church.

3. Definitions

Personal data is information about a living individual which is capable of identifying that individual (a data subject). Personal data will be held on paper or on a computer or other electronic media. All personal data held by the Church in whatever format is subject to legal safeguards specified in the Act.

The **data subject** is the person about whom personal data is processed.

Processing is anything done with or to personal data, including storing it.

The **types of personal data** that we may need to process include information about current, past and prospective employees, volunteers, suppliers, members and customers.

The term "**members**" is used broadly to include anyone registered on the Electoral Roll or whose contact details have been provided for publication in the Church Directory or who has completed a

gift aid declaration form in favour of All Saints' or who has completed a general consent form to be included on a mailing list for church information or fund raising.

The term "**customer**" is used broadly to include anyone not a member, as defined above, but who participates or benefits from a service provided by the Church, for example, hiring the premises. We are not permitted to use personal data for customers to communicate information about the church or fund raising.

Data Subject Access Requests – any request from a data subject to view his/her personal data and the lawful basis for processing that data.

A **personal data breach** is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. Data Controllers and responsibility for implementing this policy

The **data controller** is the person or organisation who determines the how and what of data processing. In a church it is usually the Vicar or PCC.

The **PCC** is the data controller accountable for the personal data held by All Saints' Church. The church does not process personal data on a "large scale" so is not required to appoint a Data Protection Officer. However, it is important that one person takes the lead responsibility for compliance with the Act. The Church Administrator has that responsibility.

The **Vicar** is a separate data controller accountable for personal data he/she may hold and process. The legal role of a Vicar results in that role being viewed as a legal entity separate to the PCC.

All employees and volunteers included within the scope of this policy are responsible for complying with it.

5. Information Commissioners Office (ICO)

The ICO is the regulator for the Act. As a small, not for profit, charitable organisation we are exempt from notifying the (ICO) of the data we hold.

6. Underlying Principles

Personal data:

a) will be **processed** lawfully, fairly and transparently.
b) is used only for a **specific processing purpose** that the data subject has been made aware of and no other, without further consent.
c) 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.
d) must be **accurate and where necessary kept up to date.**
e) should **not be stored for longer than is necessary**, and that **storage is safe and secure**.
f) will be **accessible** to the individual identified by it so that they are aware of and can check the lawfulness of the use and the accuracy of the data (referred to as **subject access requests**)

7. Lawful Processing

All processing of personal data will be compliant with our **Data Privacy Notice** (see separate document).

The **Data Privacy notice** will be published on our website and a copy placed on the notice board in the Hall lobby.

8. Consent

Electoral Roll – signed applications are sufficient evidence of consent for personal data to be entered on the Electoral Roll and for people on the Electoral Roll to be informed of Parish Meetings at which those on the Electoral Roll may vote.

Gift Aid – signed Gift Aid declarations are sufficient evidence of consent for personal data to be used to make Gift Aid claims and process personal data for that purpose.

Church Directory – an explicit consent must be obtained in order to include contact details for a person on the Church Directory. The standard consent form (see separate document) may be used for this purpose.

General communication to an individual - general information on the church, its activities, opportunities for service or giving may only be sent to those for whom explicit consent has been obtained. The standard consent form may be used for this purpose. The means of communication must be consistent with that agreed to on the consent form (post, telephone or email).

The standard consent form may be held in paper or electronic format.

9. Consent for Personal Data of children

There is special protection for children's personal data, particularly in relation to commercial internet services, such as social networking. If we offer online services to children and rely on consent to collect their information, a parent's or guardian's consent must be obtained in order to lawfully use that data. The age when a child can grant consent is set at 16 by the GPDR (although the UK Government has proposed in its Data Protection Bill, currently going through parliament, that this be reduced to 13).

We have to be able to show that consent has been given lawfully and ensure that the Data Privacy Notice used is written in a language that children can understand. Copies of consents must be kept.

10. Processing of Personal Data

We will only process personal data for the purpose for which it was obtained and for which consent has been given.

All personal data in paper form held on the church premises will be stored in a locked cabinet either in the Church Office or in the vestry. All personal data in paper form held at home by volunteers covered by this policy will be stored in a locked drawer, cabinet or cupboard. Where a locked drawer, cabinet or cupboard is not available, the documents must be stored on the church premises.

All personal data held in electronic form must be held on the church's cloud storage facility (currently Dropbox) or on a PC or hard drive that is stored in a locked cabinet on the church premises when not in use.

The Church Directory will have a notice on its front page alerting readers that it contains personal data and must not be shared with third parties.

Paper consent forms will be retained in accordance with regulatory requirements in the case of Electoral Roll applications and Gift Aid Declarations, and for as long as the personal data is used in the case of other consent forms, after which they will be destroyed.

Personal data held on any church database will be reviewed annually to ensure that it remains current and is supported by written or email consents. Subject to complying with current regulations on record keeping, all personal data will be deleted on request by the data subject and when the need for that data has expired.

11. If a Data Breach occurs

Whoever discovers the existence of the breach will notify the Church Administrator who will then notify the Vicar and Churchwardens. After consultation with at least the Vicar or one Churchwarden, the Church Administrator will notify the data subject and, if appropriate, the ICO within the timescales required by legislation.

12. Procedures

Procedures will be developed that document how this policy operates in practice.

13. Guidance and further information

Guidance on Data Protection and sources of further information are contained in Appendix A.

14. Review of this Policy

This policy will be reviewed at least every other year and as and when legislation or best practice changes.

Appendix A – Guidance on Data Protection Policy

1. Accountability

The GDPR introduces a new accountability principle that means that the Church must be able to show that it is complying with the principles. In essence, the Church cannot just state it is compliant; it has to prove it and provide evidence. To do this there are a number of actions to be taken, such as documenting the decisions made about processing activities and various other ways that show compliance – such as attending training, reviewing any policies and auditing processing activities.

2. Lawful processing

A Data Privacy Notice must be published that explains the lawful basis for processing personal data. This lawful basis will be explained when responding to Data Subject Access Requests.

For personal data to be processed lawfully, certain specific conditions have to be met. These include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. These lawful bases must be fully documented, which helps comply with the accountability requirement.

Much of the personal data processed by the PCC or Vicar is classed as sensitive (called special category personal data under the GDPR) because it relates to "religious belief" and therefore, the Church needs to identify additional bases for processing the personal data. For All Saints' the most relevant are:

a) Explicit consent from a person; or
b) Where the processing is a "legitimate activity" and relates to either members or former members or to individuals with whom there is regular contact, but is not disclosed to any third parties without consent

As a general guide, "legitimate activities" include:

a) Compiling and maintaining the Electoral Roll because it is a legitimate activity of the PCC, under the Church Representation Rules (these can be found at - https://www.churchofengland.org/about-us/structure/churchlawlegis/church-representation-rules/church-representation-rules-online.aspx)
b) Compiling and distributing rotas because these are required in order to carry out a service to other church members.
c) But sharing names and contact details outside the church for another purpose would need consent.

Personal data may only be processed when not for a legitimate activity where consent has been given. Personal data may only be processed for the specific purposes for which consent has been granted. It must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must provide explicit consent of the new purpose before any processing occurs.

3. Consent

To be valid, explicit consent must be freely given, specific, informed, unambiguous and able to be withdrawn. Also, there must be a record of how and when the consent was obtained, and that record must be reviewed over time.

Consent requires “clear affirmative action”. Silence, pre-ticked boxes or inactivity does **not** constitute consent. Any consent wording must be sufficiently strong to demonstrate that the consent given is unambiguous and the person knows exactly to what he/she is consenting. The consent wording must also inform individuals that they have the right to withdraw consent at any time. The procedure for withdrawing consent must be as simple as that for granting consent, (e.g. by sending an email or (un)ticking a box).

All consent records must be kept and be periodically reviewed (e.g. every 5 years) to ensure that they are still valid.

4. Restrictions on the use of personal data

The GDPR does not have principles relating to individuals’ rights or overseas transfers of personal data - these are specifically addressed separately.

The GDPR requires that 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 in a manner that is incompatible with those purposes. This means that individuals should be told what the Church will do with their personal data before it uses it 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 “anonymisation”); and
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.

5. The rights of individuals and how they operate

Generally, the rights of individuals that are granted under the GDPR are the same as under the 1998 Act but with some significant additions. The GDPR includes the following rights for individuals, which are briefly explained here: -

The right to be informed
Individuals have a right to be given “fair processing information”. This is done through the Church’s Data Privacy Notice which should be provided whenever personal data is collected.

The right to access (includes subject access requests)
Individuals have the right to be given confirmation that their data is being processed; access to their personal data and supplementary information. The latter is provided in the Data Privacy Notice, (i.e. information that is usually supplied in a privacy notice).

Subject Access Requests
Individuals are allowed to access their personal data so that they are aware of and can check the lawfulness of the use and the accuracy of the data. It will not be possible to make a charge for subject access requests. The Church has 1 month from the receipt of the request to comply. A request may be refused or a “reasonable fee” may be charged for requests that are manifestly unfounded, excessive or repetitive. Any refusal must be accompanied by an explanation of why and inform the individual that he/she has the right to complain to the ICO or go to court.

The right to rectification (correction)
Individuals have the right to have their personal data corrected (rectified) if it is inaccurate or incomplete. If the data has already been given to third parties, the Church must notify those third parties of the correction. The Church must also inform the individuals about the third parties to whom the data has been given.

The right to erasure (also known as the right to be forgotten)
Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This does not mean that a person can immediately request that his/her personal data is deleted. If the purposes for which the data was collected still exist, then a person will not be able to request the deletion of that data, unless it was given by consent and they are withdrawing their consent.

Common examples are:

a) Safeguarding information about an individual cannot be deleted if the retention is still necessary, reasonable and proportionate – e.g. to protect members of the public from significant harm.
b) Some financial information, such as that relating to gift aid, cannot be deleted immediately due to financial auditing regulations.
c) The personal data on the electoral roll can only be deleted in accordance with the Church Representation Rules; examples include if someone writes stating that they no longer wish to be included on the roll or a person no longer lives in the parish and no longer attends public worship there.
d) Information in parish registers cannot be deleted under any circumstances.

The right to restrict processing
Individuals have the right to restrict processing of their personal data in certain circumstances (for instance if a person believes his/her personal data is inaccurate or he/she objects to the processing). If processing is restricted, the Church can still store the data but cannot otherwise use the data.

The right to data portability
This is a new right introduced by the GDPR. Individuals have the right to obtain and reuse personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT system to another. It only applies in certain circumstances, and is highly unlikely to affect churches.

The right to object
Individuals have the right to object to processing in certain circumstances – e.g. If a church has relied on legitimate interest to process data without consent and an individual is not happy with this, they have the right to object to the church processing their data.

The right not to be subject to automated decision-making including profiling
This provides protection against the risk that a potentially damaging decision is taken without human intervention.

6. Processing personal data about children

The GDPR brings into effect special protection for children's personal data, particularly in relation to commercial internet services, such as social networking. If the Church offers online services to children and relies on consent to collect their information, it may need a parent's or guardian's consent in order to lawfully use that data. The GDPR sets the age when a child can grant consent at 16, (although the UK Government has proposed in its Data Protection Bill, currently going through parliament, that this be reduced to 13).

The Church has to be able to show that it has been given consent lawfully and therefore, when collecting children's data, it must make sure that its Data Privacy Notice is written in a language that children can understand. Copies of consents must be kept.

7. Data breach

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

From 25 May 2018 it is compulsory for the Church to inform the ICO and the individuals affected in certain circumstances, (e.g. where there is a high risk to the individuals involved, for instance, through identity theft). A data breach must be notified to the ICO within 72 hours of finding out about it. It is important that all employees and officials note this deadline and seek the advice of the Diocesan Registrar about any suspected breaches without delay.

More details can be provided after 72 hours, but before then the ICO will want to know the potential scope and the cause of the breach, mitigation actions the Church plans to take, and how it plans to address the problem.

8. Ensuring best practice on data protection

The protection of data should be considered when deciding what personal data the Church needs and how it is going to process it, including how it will be collected, stored, shared and disposed of. Data protection by design and by default means implementing appropriate technical and organisational measures to safeguard personal data, including limiting access to it; storing it in a pseudonymised format (the processing of data in such a way that the data can no longer be linked to a specific person without using additional information, which is kept separately. This could be in the form of a unique reference number for each person) and ensuring data is only used and retained as long as necessary for the purpose for which it was obtained.

It is vitally important that everyone is aware of and understands the importance of data protection. Privacy and data protection must be a core part of any project design and planning and not merely an afterthought relegated to a world of data protection specialists and lawyers. It is important that those designing and developing tools and projects consider data protection in the early planning stages in order to ensure a compliant solution. For example, when creating new IT systems for storing or accessing personal data; developing policy or strategies that have privacy implications; embarking on data sharing projects; or using data for new purposes.

9. Data Protection Impact Assessments

One way of ensuring compliance with Data Protection legislation, is by carrying out a data protection impact assessment ("DPIA"). Although a DPIA is only compulsory for certain types of processing (e.g. the large-scale processing of sensitive personal data) and is unlikely to apply to churches, it is still worth carrying out a DPIA, at the start of any project, to ensure compliance and that appropriate security is in place.

A DPIA assesses the impact of any proposed processing operation, for example the use of new technology, on the protection of personal data. A DPIA should be carried out before the processing of the personal data starts and then updated throughout the lifetime of any project. As a minimum a DPIA should include: -

a) A description: of the processing activities and their purpose;
b) An assessment: of the need for and the proportionality of the processing; and
c) the risks arising, and measures adopted to try and prevent any risks, in particular any safeguarding or security measures to protect personal data.

[The ICO has produced a 51-page Code of Practice on PIAs, (https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf).]

10. Sources of further advice

The ICO publish useful and up-to-date guidance in relation to all aspects of privacy law – including data protection – see https://ico.org.uk/for-organisations/data-protection-reform/ and for smaller organisations here.

The Article 29 Working Party, a body representing data protection authorities across the EU, is issuing new guidance to help organisations comply with the GDPR – See http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

The National Church Institutions Records Management staff can be contacted via archives@churchofengland.org