

Data Protection Policy

Author and DP Lead	Richard Berrett
PCC Approval	March 7 2018
Date of publication	March 12 2018
Review date	2019

Introduction

On the 25th May 2018 the General Data Protection Regulation (GDPR) will be applicable and the current Data Protection Act (DPA) will be updated by a new Act giving effect to its provisions. Before that time the DPA will continue to apply.

This Policy sets out the manner in which personal data of staff, Trustees, committee members, volunteers and other individuals is processed fairly and lawfully.

All Saints ('the Church') collects and uses personal information about staff, committee member, volunteers and other individuals who come into contact with the Church. This information is gathered in order to enable it to provide its charitable, pastoral and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Church complies with its statutory obligations. Most if not all of our data processing will be as part of normal church management for which we will **not** need to gain specific consent for that particular action – holding lists of committee members or other groups, for example. This is covered by a special condition under the GDPR for religious not-for-profit bodies, provided that 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

The Church also operates as a commercial concern, principally through the hiring of its premises. The data in respect of this is mainly held by the Hall Lettings Manager who works from home and therefore must ensure that their own system, manual or electronic, complies with this policy.

The Church is a data controller and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The Church must be able to demonstrate compliance. Failure to comply with the Principles exposes the Church and staff to civil and criminal claims and possible financial penalties.

Objective

This Policy will ensure that:

The Church processes personal data fairly and lawfully and in compliance with the Data Protection Principles.

All Saints Church Findon Valley with St Peter's High Salvington

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy.

The data protection rights of those involved with the Church community are safeguarded.

There is confidence in the Church's ability to process data fairly and securely.

Scope

This Policy applies to:

Personal data of all Church employees, Trustees, committee members, volunteers and any other person carrying out activities on behalf of the Church.

The processing of personal data, both in manual form and on computer.

All staff and trustees.

The Data Protection Principles

The Church will ensure that personal data will be:

1. Processed fairly, lawfully and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Church will be able to demonstrate compliance with these principles.

The Church will have in place a process for dealing with the exercise of the following rights by Trustees, staff, committee members, volunteers and members of the public in respect of their personal data:

- to be informed about what data is held, why it is being processed and who it is shared with;
- to access their data;
- to rectification of the record;
- to erasure;

All Saints Church Findon Valley with St Peter's High Salvington

- to restrict processing;
- to data portability;
- to object to processing;
- not to be subject to automated decision-making including
- profiling.

Roles and Responsibilities

The PCC is responsible for implementing good data protection practices and procedures within the Church and for compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy

The PCC Secretary will act as the Data Protection Officer and will have responsibility for all issues relating to the processing of personal data and will report directly to the PCC.

The Data Protection Officer will comply with responsibilities under the GDPR and will deal with subject access requests, requests for rectification and erasure, data security breaches. Complaints about data processing will be dealt with in accordance with the Church's Complaint's Procedure.

Data Security and Data Security Breach Management

All staff, Trustees and Committee members are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties.

Access to personal data should only be given to those who need access for the purpose of their duties.

Staff who work from home, together with Trustees and volunteers must have particular regard to the need to ensure compliance with this Policy.

Data will be destroyed securely as and when appropriate.

All staff, Trustees and Committee members will be aware of and comply with the list of Do's and Don'ts in relation to data security in Appendix A

Subject Access Requests

Requests for access to personal data (Subject Access Requests)(SARs) will be processed by the Data Protection Officer. Those making a Subject Access Request will be charged a fee in accordance with Regulations. Records of all requests will be maintained.

The Church will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request. The statutory time limit of 40 days continues until 25th May 2018 when under the GDPR the statutory time period reduces to one calendar month of receipt of the request.

All Saints Church Findon Valley with St Peter's High Salvington

Sharing data with third parties and data processing undertaken on behalf of the Church.

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so and where the consent of the data subject has been obtained, unless such consent is not required. Any sharing will be undertaken by trained personnel using secure methods. Where a third party undertakes data processing on behalf of the Church e.g. by providing cloud based systems or shredding services, the Church will ensure that there is a written agreement requiring the data to be processed in accordance with the Data Protection Principles.

Ensuring compliance

All new staff will be trained on the data protection requirements as part of their induction.

Training and guidance will be available to all staff, Trustees and committee members.

The Church advises those members of the congregation/parish whose personal data is held, the purposes for which it is processed and who it will be shared with. This is referred to as a "Privacy Notice" and is available on the Church website or on application to the Parish office.

The Church will ensure its Privacy Notice contains the following information:

- Contact Data Controller and Data Protection Officer
- Purpose of processing and legal basis. Retentions period. Who we share data with.
- Right to request rectification, erasure, to withdraw consent, to complain, or to know about any automated decision making and the right to data portability where applicable.

Photographs, Additional Personal Data and Consents

Where the Church seeks consents for processing personal data, such as photographs at events, it will ensure that appropriate written consents are obtained. Those consent forms will provide details of how the consent can be withdrawn.

Where the personal data involves a child under 16 years written consent will be required from the adult with parental responsibility.

Appendix A

What staff should do:

DO get the permission of the PCC Secretary or a Churchwarden to take any confidential information home.

DO transport information from Church on secure computing devices (i.e. Password protected laptops).

DO wherever possible avoid taking paper documents out of the office.

DO use secure portable computing devices such as encrypted laptops and encrypted USB memory sticks when working remotely or from home.

DO ensure that any information on USB memory sticks is securely deleted off the device, or saved on a Church shared drive.

DO ensure that all paper based information that is taken off the premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.

DO ensure that any confidential documents that are taken to your home are stored in a locked drawer.

DO ensure that paper based information and laptops are kept safe and close to hand when taken out off premises. Never leave them unattended. Particular care should be taken in public places.

transport).

DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.

DO return the paper based information to the Church as soon as possible and file or dispose of it securely.

DO report any loss of paper based information or portable computer devices to The PCC Secretary or a Churchwarden immediately.

DO ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only'.

DO ensure that when posting/emailing information that only the specific content required by the recipient is sent.

DO use pseudonyms and anonymise personal data where possible.

All Saints Church Findon Valley with St Peter's High Salvington

What staff must not do:

DO NOT take confidential information to an entertainment or public place, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.

DO NOT unnecessarily copy other parties into e-mail correspondence.

DO NOT e-mail documents to your own personal computer, unless previously encrypted.

DO NOT store work related documents on your home computer.

DO NOT leave personal information unclaimed on any printer.

DO NOT leave personal information on your desk over- night, or if you are away from your desk in meetings.

DO NOT leave documentation in vehicles overnight.

DO NOT discuss pastoral issues concerning individuals either at social events or in public places.

DO NOT put confidential documents in non-confidential recycling bins.

DO NOT print off reports with personal data unless absolutely necessary.

DO NOT use unencrypted memory sticks or unencrypted laptops