The Anglican and Methodist Church of St Andrew

Data Protection Policy

Date: 05.03.18, draft V2
Next Policy Review Date by Church Council:_____May 2018____

Contents

1. Introduction

This policy is required by law. The Anglican and Methodist Church of St Andrew (the Church) will publicise this policy on the church website.

The Church processes Personal Data (as defined below) in order to enable it to provide its Christian ministry and where there is a legal requirement to process the personal data (to ensure that it complies with its statutory obligations).

This Data Protection Policy ("Policy") regulates the way in which the Church obtains, uses, holds, transfers and processes Personal Data about individuals (including staff, members, parishioners, parents or carers, children and other individuals who come into contact with the Church) and ensures all of its staff, trustees and activity leaders know the rules for protecting Personal Data. Further, it describes individuals' rights in relation to their Personal Data processed by the Church.

The Church has practices in place in relation to its handling of personal information to ensure that the Church and its staff are acting in accordance with UK laws and regulatory guidance. These practices, together with this Policy and the Freedom of Information Policy, ensure that all staff, trustees, committee members and activity leaders of the Church fully understand the Church's obligation to abide by the data privacy laws and regulations of the UK.

The Church is committed to complying with data protection legislation at all times and all its staff and trustees are required to comply with this Policy. This policy was informed by the Information Commissioners Office guidance (www.ico.gov.uk).

2. Linked Policies

This policy relates to all the Church activities which involve the collection and storage of information about people. There is also a separate

- CCTV policy
- Privacy and Consent Notice document
- Website Cookie and Privacy Policy
- Website Terms and Conditions
- Safeguarding and Child Protection Policy

3. Responsibilities

The Church is the Data Controller for the purposes of the Data Protection Act and therefore the Trustees will have overall responsibility for compliance with the DPA.

The Trustees have delegated responsibility to the staff, church activity leaders and committee members for compliance with the DPA and to adhere to this policy within the day to day activities of the church. The Church will appoint a Data Protection Officer (DPO) for the church.

The DPO working alongside the Church Council is responsible for:

- notifying the Information Commissioner's Office (ICO) and renewing the Church's registration annually.
- keeping the ICO up to date with changes in how the church processes data
- working with the Church Office to ensure data protection statements are included on forms that are used to collect Personal data.
- acting as a central point of advice on data protection matters
- working with the Church Council to arrange appropriate data protection training for staff and members.
- keeping up to date with the latest data protection legislation and guidance.
- ensuring adequate systems are in place for compliance with this policy.

4. Definitions

"Personal Data Information" is any information (for example, a person's name) or combination of information about a living person which allows that living person to be identified from that information (for example a first name and an address). Examples of personal data the Church may use include names of staff and members, dates of birth, addresses, national insurance numbers, prayer requests, medical information, staff development reviews, payroll and salary details, business interests, disciplinary and attendance records, vetting checks, and images obtained through CCTV.

"Sensitive Personal Data" is Personal Data about a person's race or ethnicity, their physical or mental health, their sexual preference, their religious beliefs, their political views, trade union membership or information accusing an individual of any crime, or about any criminal prosecution against them, and the decision of the court and any punishment.

5. What Activities are regulated by this Policy?

The Church processes Personal Data (including Sensitive Personal Data, see below for more information) of individuals including its staff, members, parents or carers and children, contractors, church contacts, hall bookers, suppliers and any other individuals who come into contact with the Church, including job applicants, former staff, prospective and former members, depending on the relationship with them, for a number of purposes, including:

i. provision of ministry and other associated functions;
ii. personnel record keeping and management;
iii. employee performance management and professional development;
iv. employee benefits and succession planning;
v. payroll and pensions;
vi. donors, regular givers and gift aid

vii. contract performance, including buying and selling goods and services;
viii. recruitment;
ix. building and managing external relationships;
x. work and project scheduling;
xi. compliance programs and policies;
xii. security and the prevention of crime; and
xiii. other purposes required by law or regulation and/or as notified to you separately from time to time.

When the Church collects, stores, uses, discloses, updates or erases Personal Data for any of these purposes, this is called "**Processing**".

If you make use of Personal Data (e.g. read, amend, copy, print, delete or send Personal Data to another organisation, whether to another church within the Diocese or otherwise) this is also a type of Processing and is subject to the guidelines set out in this Policy. We may share Personal Data with the Diocese. We may also share Personal Data with any third party service providers, such as in relation to our human resources information systems, or other service providers, which we appoint in the future to Process Personal Data on behalf of the Church.

Where collected, Sensitive Personal Data should not be used unless strictly necessary. Extra care must be taken with it (in addition to the normal rules for Personal Data) and it must be kept more securely. Additional restrictions are placed on top of the lawful reasons for Processing Sensitive Personal Data mentioned above. For example, it is difficult to lawfully use such details without the consent of the individual, which has to be explicit, free, voluntary, in writing and obtained prior to processing any Sensitive Personal Data. The Church does not generally seek to obtain Sensitive Personal Data unless:

i. the individual concerned agrees in writing that we may do so, on the basis of a full understanding of why the Church is collecting the data
ii. the Church needs to do so to meet its obligations or exercise its rights under employment law and/or pastoral duties on behalf of parishioners
iii. in exceptional circumstances such as where the Processing is necessary to prevent and/or detect crime or to protect the vital interests of the individual concerned (ie in "life or death" circumstances)

The "legitimate interest" criteria described alone is not enough to process Sensitive Personal Data.

Sensitive Personal Data should not be emailed or disclosed unless measures are taken to encrypt or otherwise secure that information due to the potential for harm or distress if the email is received by unintended recipients or otherwise goes astray. Sensitive Personal Data should be collected and used as little as possible, be kept separate from other details, be subject to more limited and strictly need to know access and used subject to greater security measures than other details.

6. Data Protection Requirements

The DPA stipulates that anyone processing Personal Data must comply with eight principles of good practice. The principles require that Personal Data:-

- shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met.
- 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.
- be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
- be accurate and where necessary, kept up to date.
- not be kept for longer than is necessary for that purpose or those purposes.
- be processed in accordance with the rights of data subjects under the Act.
- be kept secure eg protected by an appropriate degree of security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The GDPR provides the following rights for individuals:

- The right to be informed (i.e. transparency over how you use personal data)
- The right of access to the data that you have on them
- The right to rectification to data held
- The right to erasure
- The right to 'block' or suppress processing of personal data
- The right to data portability (allows individuals to obtain and reuse their personal data for their own purposes)
- The right to object
- Rights in relation to automated decision making and profiling (e.g. making a decision solely by automated means without any human involvement)

7. Notification

The laws governing how we can use Personal Data apply whether the Personal Data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word processed document) or in structured paper records (for example, in paper files, card indexes or filing cabinets). Data protection laws are enforced in the UK by the Information Commissioner's Office ("ICO"). The Church maintains a notification with the ICO which sets out how it Processes Personal Data and for what purposes. The Church shall ensure that this notification is kept up to date and renewed annually.

8. Data Gathering

Whenever the Church collects new information about individuals we will ensure individuals are made aware:

- that the information is being collected,
- of the purpose that the information is being collected for,
- of any other purposes that it may be used for,
- with whom the information will or may be shared
- and how to contact the Data Controller.

The Church will only obtain relevant and necessary Personal Data for lawful purposes and will only process the data in ways which are compatible with the purpose for which it was gathered. Data Privacy statements should be included on the website and on forms that are used to collect personal data.

9. Data Storage

Personal Data will be stored in a secure and safe manner. The following measures are taken to help ensure this:

- electronic data will be protected through secure password, encryption software and firewall systems operated by the Church.
- computer workstations in administrative areas will be positioned so that they are not visible to casual observers.
- manual Personal Data will be stored securely where it is not accessible to anyone that does not have a legitimate reason to view or process the data.
- particular attention will be paid to the need for security of Sensitive Personal Data, for example health and medical records will be kept in a locked cupboard.
- Personal Data will not be left out visible on desks.
- the physical security of church buildings and storage systems will be regularly reviewed.
- Staff will be trained on this policy and related data protection procedures.

10. Data Checking

Systems will be put in place to ensure the Personal Data that the Church holds is up to date and accurate. For example the Church will ensure that parents are asked at least once a year to confirm their contact details. Any inaccuracies discovered or reported will be rectified as soon as possible.

11.Data Disclosure

We sometimes need to share the personal information we process with the individual themself and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons. Where necessary or required we share information with:

- family, associates and representatives of the person whose personal data we are processing
- church council
- the Diocese
- police forces, courts
- current, past or prospective employers
- voluntary and charitable organisations
- business associates, professional advisers
- suppliers and service providers
- financial organisations

Personal Data will only be disclosed to organisations or individuals for whom consent has been given to receive their data, or organisations that have a legal right to receive the data without consent being given. When requests to disclose Personal Data are received by telephone, the Church will ensure that the caller is entitled to receive the data and that they are who they say they are. In some circumstances the Church may call the caller back to check the identity of the caller. Personal Data will not be included on the website, in newsletters or to other media without consent of the individual (or his/her parents where appropriate). Routine consent may be requested from parents to avoid the need for frequent, similar requests for consent being made by the Church.

12.Data Subject Access Requests

Any person whose Personal Data is held by the Church is entitled, under the DPA, to ask for access to this information. The request must be in writing. The right is to view or be given a copy of the Personal Data, rather than to the whole document which contains Personal Data. When a request is received, this should be passed to the office without delay. The church office and DPO will liaise with the relevant data holders to collate all Personal Data records.

The request must be dealt with promptly by all relevant data holders; a response must be provided as soon as possible and no later than within 40 calendar days from the date the request was received. A record will be kept of all data subject access requests made that require formal consideration.

13.Freedom of Information Requests

Any Freedom of Information Requests received by the church must be forwarded immediately to the Incumbent who will ensure they are dealt with appropriately.

14.Destroying Data

Out of date information will be securely destroyed if no longer relevant. Personal Data will only be kept for as long as reasonably needed, for legal or church business purposes.

15.Breach of the Policy

Non-compliance of this policy and data protection legislation by a member of staff is considered a disciplinary matter which, depending on the circumstances, could lead to dismissal.

Any breach of GDPR should be notified to the church office who will log and notify the DPO. Personal data breaches which are likely to result in a risk to people's rights and freedoms must be reported by the DPO to the ICO when the General Data Protection Regulation comes into force from 25 May 2018.

16.Monitoring, Evaluation and Review

The DPO will monitor the implementation and effectiveness on this policy and report his/her evaluation to the Church Council on an annual basis. The DPO will report back on the policy and its implementation and effectiveness annually. The Council will then review the policy, making any amendments necessary.

Appendices (see separate document):

- Guidance notes e.g. Email, forms
- Privacy and Consent Notices
- CCTV policy
- Website Cookie Policy
- Website terms and conditions
- Website Privacy policy