

DATA PROTECTION POLICY

Policy reviewed and revised: End 2019. By: Ruth Putnam. Agreed by PCC: January 2020

1. Data Protection Act 2018

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

2. Data Protection Principles

There are 8 principles under which personal data may only be obtained, held or disclosed to others:

2.1 Personal data shall be processed fairly and lawfully.

In practice that means that you must:

- Have legitimate grounds for collecting and using the personal data;
- Not use the data in ways that have unjustified adverse effects on the individual's concerned;
- Be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- Handle people's personal data only in ways they would reasonably expect; and
- Make sure you do not do anything unlawful with the data.

2.2 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

2.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

2.4 Personal data shall be accurate and, where necessary, kept up to date.

2.5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

2.6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

2.7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

2.8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. Registration

By this process, a data controller (a person who controls the data) informs the Information Commissioner that he or she is processing personal data (information about a living person). **PCCs** are exempt from registration if all of the processing is covered by the following provisions:

- The processing is only for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit or providing or administering activities for individuals who are either members of the body or association or who have regular contact with it.
- Your data subjects (the people about whom you hold data) are restricted to any person the processing of whose personal data is necessary for this exempt purpose.
- Your data classes (the type of information you are processing) are restricted to data which are necessary for this exempt purpose.
- Your disclosures (the giving out of the information) other than those made with the consent of the data subjects are restricted to those third parties which are necessary for this exempt purpose.
- The personal data is not kept after the relationship between you and the data subject ends, unless and for so long as it is necessary to do so for the exempt purpose.
- In addition, processing is for staff administration, advertising, marketing and public relations or accounts and records.

4. Subject Access Rights

An individual will have the right to receive a copy of most information held about him or her by an organisation within 40 days of making a request. You may charge a fee of up to £10 for providing it. This covers all information held on computer and any correspondence and other papers which are reasonably accessible. You do not, therefore, have to scour through minutes etc for any mention of the individual but you would have to produce accessible information held by any church officers.

The general principle is that as much information as possible should be shared with the individual. There are, however, limited categories of material which you may withhold from the individual in the interests of protecting the rights of other individuals to privacy and for the protection of crime etc. You are able to withhold any references that you have given (but not any you have received). On sharing with an individual the information that you hold about them, you must remove anything which would identify a third party. You may also be entitled to hold back information containing serious allegations (for example, of child abuse) if to reveal that information would compromise the proper investigation of those allegations. In such cases, you should always seek advice from the Diocesan Secretary.

5. What should PCC Secretaries do?

- Identify a person responsible for compliance with the Act.
- Identify who holds what data and ensure that everyone is aware of the requirements and they only record information that could be shared if a subject access request is made.
- Work out whether or not you need to register and do so if necessary.
- Destroy material that you cannot justify still holding, especially if making the information available to the individual concerned would create difficulties.

- Inform people broadly what information is held about them and the purposes for which it is held. Tell them who they should contact with queries. This could be done in a paragraph in a notes and news sheet or on the church notice board.

6. St Kea Church

Is required to register under the Data protection act

The person responsible for compliance with the Act is the Church Administrator overseen by the PCC Representative, under the instruction of the Vicar who is the Data Controller

Amongst others those who hold information about individuals are:

Church office: details of those who are members of our church

Treasurer and/or Gift Aid Secretary: details of those who support the parishes regularly and claim gift aid on their donation.

Electoral Roll Officer: The Electoral Roll Officer holds details associated with maintaining the role of members of the parish church

Associate Minister for Families and Youth: holds information including contact details of the members and their parents/carers. This is renewed in September every year and updated during the year as necessary.

CAP Centre Manager: holds contact information for St Kea's Lanterns congregation

Ministry Team Leaders: currently Small Group Leader, Safeguarding Co-ordinator, DBS Co-ordinator, Pastoral Team Leader

Each of these data administrators will be expected:

To keep records for no longer than is necessary for that purpose or those purposes

To dispose safely of any personal details

To ensure that personal contact details are not shared with others unless express (usually written) permission is given to pass on the details to a third party

Other Data

Occasional Offices: Weddings, Baptisms and Funerals

Registers are public documents and therefore available to view on request. Our responsibility is to ensure they are kept safe, and filled in accurately.

This policy needs to be read in conjunction with the St Kea Safeguarding Policy/Booklet