The Parish of Kidderminster East
St Cassian's | St Cecilia's | St Chad's | St George's | St Mary, Stone

GDPR POLICY

The Parochial Church Council (PCC) and Clergy of The Parish of Kidderminster East

Introduction

The Parochial Church Council (PCC) and the Clergy of the Parish of Kidderminster East are the data controllers and complies with its obligations under the GDPR by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data. A Data Compliance Officer has been appointed. This policy describes what personal data is collected, where it is stored, who can use it and how the rights of individuals are protected. Individuals may have collected and stored personal data, for example email addresses, phone numbers and other personal data which they use for their personal use or to organise social or other events that are not directly associated with the management of the Parish. Such data is not in control of the Parish and therefore is not within the scope of this policy.

What is personal data?

Personal data is information relating to a living individual, who can be identified directly from that data or indirectly by reference to other data held. For example, name, contact details etc., reference numbers. Under some circumstances the data controllers may collect sensitive personal information relating for example to religion and health.

The use of personal data

Personal data is used for the following purposes:

- To provide a voluntary service for the benefit of the public in a particular geographical area as specified in the constitution
- To administer membership records
- To fundraise and promote the interests of the charity
- To manage employees and volunteers
- To maintain accounts and records (including the processing of Gift Aid applications)
- To inform interested parties of news, events, activities and services running in the Churches of the Parish of Kidderminster East

See the Register of Processing Activities (ROPA) for information on the following which may need to be supplied to the Information Commissioners Office (ICO) if requested and provides accountability:

- identifying the various types of data processing that are carried out;
- the purposes and legal basis for this processing
- a written record of all processing activities, security measures and data retention practices.

Personal data shall only be used in accordance with the permission, given by individuals, to use the data.

The use of photographs

Non-identifiable photographs e.g. group photographs or background photographs, may be used without prior consent. Any photo, when used with associated information that can uniquely identify an individual requires written consent before it can be published. Once consent has been obtained, the Parish must ensure they protect the confidentiality of said photographs until its point of destruction. It is good practice to clearly display a notice in the area where photographs are to be taken stating the details of who to contact if you do not wish to have your photo taken.

What are the restrictions on the use of personal data?

The GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- 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 you are going to do with their personal data before you use it and consent to such use. Personal data should not be shared with others without the individuals consent
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are used
- 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
- 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.

Storage and access of personal data

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. This applies whether the information is kept within the Church, Parish Office or at home.

Personal data should not be kept for any longer than absolutely necessary. The Parish retention schedules should be checked regularly to ensure data held is accurate, required and deleted when necessary. Retention periods for data, including Parish Registers, Electoral Rolls, Gift Aid declarations and a range of other information typically held by Parishes can be found in the guide to Parish record keeping “Keep or Bin: Care of Your Parish Records” which can be downloaded from the Church of England website and as specified in ROPA.

Personal data shall not be used for any other purpose and shall not be provided to third parties. Some personal data however is legally required to be kept and may be passed onto third parties for example to the Diocese for archiving or the tax office for Gift Aid purposes.

When using email addresses for example to communicate to many Church members the blind copy function (bcc) should be used for individual email addresses, such that the distribution list is hidden from recipients.

Personal data held online is only accessible to those who have login and password details. Login and password details are only given to those who need access to the data. The password will be changed when anyone with access no longer requires the data.

Personal data may be shared with other Church members for the purposes of managing a group, e.g. home group, rota lists etc.

Individual's right to be informed

Individuals continue to have a right to be given "fair processing information", through the Data Privacy Notice. When personal data is collected individuals must know who has collected it and what it is being used for.

GDPR requires that additional information is supplied. For instance, the following will need to be explained:

- the lawful basis for the processing of their data
- the data retention periods (how long you keep it for)
- who its shared with
- Individuals have a right to complain to the ICO if they think that there is a problem in the way that their personal data is being dealt with.

Individual's right to access

Individuals have the right to be given confirmation that their data is being processed if they ask. The GDPR continues to allow individuals 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.

In most cases the Parish will no longer be able to charge for subject access requests. These requests must be dealt with within 1 month from the receipt of the request. The Parish will be able to refuse or charge a "reasonable fee" for requests that are manifestly unfounded, excessive or repetitive. If a request is refused, the individual must be told why and that he/she has the right to complain to the ICO or seek a judicial remedy.

Individual's right to rectification

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 third parties must be told of the correction. The individuals must be told about the third parties to whom the data has been given.

Individual's right to erasure

Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

This means that although a person can request that his/her personal data be deleted immediately, if the purposes for which the data was collected still exist then unless it was given by consent and they are withdrawing their consent, the Parish does not have to agree. For instance, 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. Another example is that some financial information, such as that relating to gift aid, cannot be deleted immediately due to financial auditing regulations. 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. Information in parish registers cannot be deleted under any circumstances.

Individual's right to restrict processing

Individuals have the right to restrict processing of their personal data in certain circumstances, for instance they may consider the processing to be unlawful and rather than request erasure, they ask that it be restricted, i.e. that the processing is limited in some respect; or where there is a challenge as to its accuracy, the Parish may need to restrict the processing until this is resolved. If processing is restricted, the data can still be stored but cannot otherwise be used, and sufficient information should be retained to alert you to the restriction applied.

Individuals right to data portability

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 Parishes.

Individual's right to object

Individuals have the right to object to processing in certain circumstances – e.g. If a Parish has relied on legitimate interest to process data and an individual is not happy with this they have the right to object to the Parish processing their data.

Individual's right not to be subject to automated decision-making including profiling

The GDPR provides protection against the risk that a potentially damaging decision is taken without human intervention. This right is similar to the 1998 Act.

Processing personal data about children

The GDPR brings into effect special protection for children's personal data, particularly in relation to online services, such as social networking. If online services are offered directly to children and rely on consent to collect their information, a parent's or guardian's consent may be needed to lawfully use that data if they are under the age of 13 (this is the age proposed in the Data Protection Bill and is subject to Parliamentary approval).

The Parish must be able to show that consent has been given lawfully and therefore, when collecting children's data, the Data Privacy Notice must be written in a language that children can understand, and copies of consents must be kept. When processing children's personal data that is not part of an online service there are no specific additional requirements. The GDPR does state that specific protection is needed where children's personal data is used for marketing purposes or creating personality or user profiles. Children's personal data must be protected from the outset and systems and processes must be designed with them in mind.

Data Protection Impact Assessment (DPIA)

One way of ensuring compliance is by carrying out a DPIA. This is mandatory under GDPR for certain types of processing e.g. the large-scale processing of sensitive personal data. Although it is unlikely that Parishes will be processing sensitive personal data on a large scale, it is still worth considering carrying out a DPIA at the start of a project to ensure that appropriate protection is in place.

A DPIA assesses the impact of any proposed processing operation, for example the use of data for new purposes, 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, the GDPR requires that a DPIA includes: -

• A description of the processing activities and their purpose;

• An assessment of the need for and the proportionality of the processing; and

• The risks arising, and measures adopted to try and prevent any risks such as safeguarding or security measures to protect personal data.

Changes of Roles and Responsibilities

From time to time, people will naturally change their roles and responsibilities as active members of the Parish. This requires actions to take place to comply with GDPR. These are:

- Handover all new data to the new person in the role
- Remove and dispose of all data from personal files (both printed and digital)
- New person in role to change all passwords

What to do if there is a 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. The GDPR makes it compulsory 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). Under the GDPR, the Parish will have to notify the ICO of a data breach within 72 hours of finding out about this. It is important that those in the Parish note this deadline and consult with their Diocesan Office 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, mitigating actions the Parish has taken or plan to take, and how the Parish will address the problem.