THE BENEFICE OF EGGARDON & COLMERS

DATA PROTECTION STATEMENT

1. Types of Data

Personal Data

This is any information which relates directly to an individual and can be linked directly to them. This includes: name, phone number, email address, photographs, genetic and economic data. This data is the focus of GDPR legislation and data protection.

Anonymous Data

Data which has been anonymised properly cannot be traced back to the original individuals in any way but can still be processed to conduct research. This is not covered by GCPR legislation as it contains no personal information to protect.

Pseudonymous Data

Some data, which has been properly pseudonymised, can only be connected back to an individual using a specific key or code. This can be an extra layer of security but the data is still treated as personal data under GDPR.

2. Principles of GDPR

GDPR legislation lays out six principles for processing of personal data: These are:

- **Lawfulness, fairness and transparency** – data should be gathered and used in a way that is legal, fair and understandable. The public have the right ot know what is being gathered and have this corrected or removed.
- **Purpose limitation** – Data should only be used for the purpose specified at the time of collection.
- **Data minimisation** – data collected should be limited only to what is required for the stated purpose.
- **Accuracy** – Personal data should be accurate, kept up to date and, if it is no longer accurate, should be rectified or erased.
- **Storage Limitation** – Personal data should only be stored as long as necessary. Data may be archived securely and used for research purposes in the future. Where possible the personally identifiable information should be removed to leave anonymous data.
- **Integrity and confidentiality** – Personal data should be held in a safe and secure way that takes reasonable steps to ensure the security of the information and avoid accidental loss, misuse or destruction.

3. Privacy Notices and Consent

If personal data is to be collected it should be accompanied by a privacy notice outlining the intended use of the information and how long the data will be kept. It should also provide the 'lawful basis' for collecting the information. (See Section 5). The information provided should be concise, transparent, intelligible, easily accessible and must use clear and plain language. Our forms should, therefore also contain a consent clause, requiring the person providing data to sign and date. The privacy information must be regularly reviewed and, if necessary, updated. (See Appendix A).

4. Individual's Rights

GDPR gives people clear rights over their data.

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

5. Lawful Basis

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply when personal data is to be processed:

a Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

b Contract: the processing is necessary for a contract you have with the individual.

c Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d Vital interests: the processing is necessary to protect someone's life.

e Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Most lawful bases require that processing is necessary for a specific purpose.

6. Subject Access Requests

Individuals have the right to know what data you hold on them, why the data is being processed and whether it will be given to any third party. As data held by the Benefice has been provided by individuals, it is unlikely that the church will receive a subject access request. However, should a request be received, the Benefice must be able to find the relevant data and comply within one month of receipt of the request by providing the information in permanent form.

7. Detecting, reporting and investigating personal data breaches

GDPR introducing a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority and, where feasible, to do this within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk of adversely affecting the individual's rights and freedoms, you must also inform those individuals without delay. A record of any personal data breaches, regardless of whether you are required to notify, should be kept. Some breaches should be reported to the Information Commissioner's Office (ICO). If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and

severity of the risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report. **You do not need to report every breach to the ICO.**

8. Responsible for data protection

The responsible officer in the Benefice is the Administrator, Sandy Hashimi.

9. Personal Data processed by The Benefice

Type of data	Lawful basis	Purpose	Storage details	Duration
Email contact list Personal data: Email Address	a,b	Provision of Pews News. All emails sent via bcc	Stored on Administrator's laptop, password protected and with Kapersky internet security	Ongoing
Wedding booking forms Personal data: Name, age, occupation, address, contact numbers, email address, marital status, father's occupation.	a,b,c	Wedding forms, for completion of Life Events Diary, provision of marriage ceremony, arrangements of Banns and legal requirements of registration and quarterly returns to the Records Office.	Forms stored on One Drive. Information disseminated into Excel database on One Drive, and also reproduced on the CofE Life Events Diary and Marriage Registers (see below).	10 years
Church Registers Personal data: As above.	c,e	The entry of personal data into church registers is a legal requirement in the UK.	Registers are kept in the relevant church buildings in a lockable safe. The minister and church wardens hold the keys.	Sent to GRO
Marriage Certificate counterfoils Personal Data: Name	a,b,c	Name and registration entry number.	Book of blank marriage certificates and counterfoils kept in the relevant church buildings.	Sent to GRO
Guests lists for weddings (Covid-19, Track and Trace Requirement) Name, tel. number	n/a	Kept by wedding couple.		
Completed monument forms. Personal Data: Name, address, age.	a,b	Information gathered by stonemason enabling the provision of monuments.	Duplicate forms – one sent back to the stonemason, copies kept by the Administrator in a locked filing cabinet.	10 years

Payee Details: Personal Data: Name, bank account details	a,b	To enable online payment through Nat West Online Banking App	Information processes and entered onto Benefice Spreadsheet and used to create accounts, stored on Dropbox. Accessible to Administrator and Church Treasurers; Pelham Allen and Nigel Guard.	10 years
Benefice Spreadsheet and Accounts Personal Data: Name, payments	a	Information regarding income and expenses of the Benefice required to reconcile accounts	Stored on Dropbox, as above.	10 years
Diocese Returns Personal Data: Name, Life event	a,b	Information required by the Diocese and processed from funeral directors.	Stored on Dropbox, as above and entered onto the Life Events Diary.	10 years
ECV Personal Data: Name, Life event	a	Information provided to the editor, Eggardon & Colmers View, in section 'from the registers' with monthly life events.	Copies of document sent to ECV editor saved on Administrator's laptop, passworded and with Kaspersky internet security.	2 years

20/07/2020 sh