****

**St. Augustine of Canterbury, North Springfield Church Council**

**Data Protection Policy**

**Policy agreed on 7 April 2022**

**Policy to be reviewed by May 2023**

**THIS POLICY RELATES TO THE ANGLICAN, METHODIST AND URC PARTNERS ONLY AS THE ROMAN CATHOLIC COMMUNITY HAS ITS OWN POLICY**

**1. Introduction**

St. Augustine of Canterbury is a local ecumenical partnership (LEP) consisting of Anglican, Methodist, United Reformed Church (URC) and Roman Catholic communities. We share the same church building and the Anglican, Methodist and URC communities form a single congregation. The Roman Catholic Community has its own services and its own policies relating to the General Data Protection Regulations 2016 (GDPR) as implemented by the Data Protection Act 2018.

The Church Council has adopted the Anglican Church policies and procedures for the purposes of the GDPR. In a purely Anglican setting its functions would be carried out by the Parochial Church Council (PCC) and the incumbent or priest in charge. However, in order to enable all the partners to participate fully in the life of the church and its decision making it has delegated all its functions to the St Augustine North Springfield Church Council (the Church Council) except for those matters where the law prescribes otherwise.

 The legislation contains a general exemption for non-profit making religious organisations from the need to register with the Information Commissioner’s Office (ICO.).However, the Church Council is required to register with the ICO under the GDPR as we have CCTV in the church building and the car park. We may also store and process sensitive personal data.

The Church Council is responsible for ensuring the CCTV systems are operated solely for purposes of:

* Security of property and premises
* Preventing and investigating crime
* Security of lone workers

The Church Council is also responsible for the storage and processing of personal data held.

As data concerning religious belief is defined as sensitive data under the GDPR, specific consent to process such data is required and must be freely and explicitly given (i.e. people must positively ‘opt-in’).

However, a considerable amount of data processing may be done as part of normal church management that does not need specific consent for that particular purpose. This is covered by a special processing condition under the GDPR for religious not-for-profit bodies, provided the processing is a ‘legitimate activity’ and 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. For example, processing electoral roll data can be said to be a legitimate activity under Church Representation Rules provided this data is not used for any other purpose without specific consent, and is not divulged to a third party. Sharing names of individuals on a coffee rota with other church members on the rota would also not require consent, as the information is shared in order to provide a service to other church members. Where, however there is, for example a church directory which is likely to be shared with people who are not members or former members, specific consent is needed

We are required to follow and abide by the Data Protection Principles which state that personal data must be:

* Processed lawfully, fairly and transparently.
* Only used for a specific processing purpose that the data subject has been made aware of and no other, without further consent,
* Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is used (i.e. only the minimum amount of data should be kept for specific processing).
* Accurate and, where necessary, kept up to date. Personal data should be periodically checked and any data that is found to be inaccurate or unnecessary should be deleted or corrected without delay.
* Not be stored for longer than necessary and storage must be safe and secure (e.g. in lockable filing cabinets or password protected files).
* Processed in a manner that ensures appropriate security and protection. Although no longer a principle, personal data must not be transferred to other people or other organisations outside the EU without adequate protection and specific consent.

This policy applies to all employees and volunteers of the LEP and sets out how we ensure that this happens for all activities involving the Church Council.

Our Data Protection Officer is Douglas Hayton (douglas.hayton@btinternet.com). He is responsible for ensuring compliance with the GDPR. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with him.

This policy is not part of any contract of employment but it is a condition of employment that employees and others who process personal data will adhere to the rules of the policy. Any breach of the policy will be taken seriously. Any volunteer or employee who considers that the policy has not been followed in respect of personal data about themselves or others should raise the matter with the Data Protection Officer in the first instance.

1. **Definitions in the GDPR**

The GDPR defines personal data and its processing in the following terms:

* **Data** is recorded information whether stored electronically on a computer, in paper based filing systems or other media.
* **Data subjects** include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.
* **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can even include a simple email address.

The types of personal data that the Church Council may be required to handle include information about current, past and prospective parishioners, employees, volunteers, customers, suppliers, conference and course attendees, those running or leading courses and others with whom we communicate.

* **Data controllers** are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The Church Council is the data controller under the terms of the GDPR
* **Data users** include the Church Council’s employees and volunteers whose work involves using personal data held by the church. Data users have a duty to protect the information they handle by following our data protection and security policies at all times
* .**Data processors** include any person who processes personal data on behalf of a data controller. This excludes the Church Council’s volunteers or employees (who are data administrators or data users), but does include, for example, outside suppliers who are **contracted to handle personal data on our behalf.**
* **Processing** is any activity that involves use of the data. It includes obtaining, recording of

holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

* **Sensitive personal data** includes information about a person's ethnicity, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual orientation, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.
1. **Data held by St. Augustine of Canterbury, North Springfield Church Council**
	1. **Types of data held**

Personal data held will be adequate, relevant and not excessive. In most cases, it consists of:

A Name

B Address

C Telephone number

D Email address

E Bank details

F Amount of giving

G Contact name & number in case of an emergency

H Date of birth

J Age

K Occupation

L Parents’ names

M DBS Certificate information

* 1. **Data held by whom**

The following people hold information about individuals to facilitate the administration and day-to-day ministry at St Augustine’s, including pastoral care, oversight, calls and visits, and keeping people informed of church events and activities.

| Data Subjects | Data held | Data Processor holding data | Purpose |
| --- | --- | --- | --- |
| Full contact details of congregation  | A B C D | ClergySuperintendent Minister | Ability to contact congregation members |
| A B C D | Church WardensChurch StewardsCircuit Steward | Ability to contact congregation members |
| A B C D | Pastoral Assistant | Ability to contact congregation members |
| A B C D | Electoral Roll Officer | Statutory requirement |
| A B C D | Church Council Secretary | Ability to contact congregation members on behalf of the PCC or clergy |
| Employee details  | A B C D M | Safeguarding Lead Recruiter | For DBS purposes |
|  | A B C D E H J | Church Council Treasurer | Payment of legitimate expenses |
| Details of those giving under the Parish Giving Scheme | A B C D E F | Church CouncilTreasurer | To ensure gift aid is received |
| Details of those giving via standing order  | A B C D E F | Church Council Treasurer | To claim gift aid on donations |
| Details of those giving via envelope scheme  | A B C D F | Church Council Treasurer | To claim gift aid on donations |
| Contact details Choir members  | A B C D | Organist/choir master | To notify of practice and service dates |
| Contractors, suppliers and hirers | A B C D  | Joint Management | To let/manage contract/supply |
| A B C D E | Joint Management | For payment |
| Baptisms, Weddings, Blessings, Pastoral Care, Funerals | A B C D H J K L | Clergy | Ability to contact for legal and pastoral reasons |

1. **The six lawful bases for processing data under the GDPR are:**
* **Consent**: A controller must be able to demonstrate that consent was given. Transparency is key. Consents given in written declarations which also cover other matters must be clearly

distinguishable, and must be intelligible, easily accessible and in clear and plain language.

Consent is defined as any freely given, specific, informed and unambiguous indication of

the data subject’s wishes – either by a statement or by a clear affirmative action.

* **Legitimate interests**

This involves a balancing test between the controller (or a third party’s) legitimate interests

and the interests or fundamental rights of and freedoms of the data subject – in particular

where the data subject is a child. (Note: A child is defined as being under 13 years of age).

* **Contractual necessity**

Personal data may be processed if the processing is necessary in order to enter into or

perform a contract with the data subject (or to take steps prior to entering into a contract).

* **Compliance with legal obligation**

Personal data may be processed if the controller is legally required to perform such

processing (e.g. complying with the provisions of the Church Representation Rules;

reporting of race or ethnic origin or gender pay data).

* **Vital Interests**

Personal data may be processed to protect the ‘vital interests’ of the data subject (e.g. in a

life or death situation it is permissible to use a person’s medical or emergency contact

information without their consent).

* **Public Interest**

Personal data may be processed if the processing is necessary for the performance of tasks

carried out by a public authority or private organisation acting in the public interest.

1. **As religious belief is ‘sensitive’ data, in order to process such data at least one of the following criteria must also be met:**
* **Explicit consent of the data subject** has been obtained.
* **Employment Law** – if necessary for employment law or social security or social protection.
* **Vital Interests** – e.g. in a life or death situation where the data subject is incapable of

giving consent

* **Charities, religious organisations and not for profit organisations** – to further the interests of the organisation on behalf of members, former members or persons with whom it has regular contact such as donors. Note, however, that explicit consent is required for the personal data to be shared with a third party.
* **Data made public by the data subject** – the data must have been made public

‘manifestly’.

* **Legal Claims** – where necessary for the establishment, exercise or defence of legal

claims or for the courts acting in this judicial capacity.

* **Reasons of substantial public interest** – where proportionate to the aim pursued and the rights of individuals are protected.
* **Medical Diagnosis or treatment** – where necessary for medical treatment by health professionals including assessing work capacity or the management of health or

social care systems.

* **Public Health** – where necessary for reasons of public health e.g. safety of medical

products.

* **Historical, Statistical or scientific purposes** – where necessary for statistical purposes in the public interest for historical, scientific research or statistical purposes.

In an ecumenical partnership context, the most relevant lawful bases for processing under Special Category Data (sensitive data) are likely to be:

* Explicit consent from a person; or
* Where the processing is the legitimate activity of the organisation (ours being a

‘religious organisation’) and relates to either members or former members or to

individuals with whom there is regular contact, but is not disclosed to any third

parties without explicit consent.

1. **The Data Protection Principles in Practice**

**6.1** **Fair and lawful Processing**

The GDPR is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. For personal data to be processed lawfully, certain specific conditions have to be met. These include, among other things, requirements that the data subject has consented to the processing, or that the processing has a legitimate lawful basis. As religious data is classed as sensitive, additional conditions must be met. In most cases the data subject's explicit consent to the processing of such data will be required and processing will not be carried out until consent has been obtained.

When consent is relied on, the data subject must be told the purpose(s) for which the data is to be processed, and freely and explicitly consented to a specified purpose before any processing for that purpose takes place. Several different consent forms (or elements within a single form) are likely to be needed to cover different areas of data processing. Consents obtained must be stored.

We shall ensure that when personal data is collected, data subjects will be informed that the data will be held in accordance with the requirements of the GDPR and in compliance with this policy, a copy of which can be obtained from the Church Council Secretary.

**6.2 Processing for Limited Purposes**

Personal data may only be processed for the specific purposes that the person has consented to or for any other lawful purposes specifically permitted by the Act, such as complying with requests from the police or other authorities. We shall ensure that personal data is only collected for the legitimate purposes of St. Augustine of Canterbury, North Springfield and its Church Council. If it becomes necessary to change the purpose for which the data is processed, the data subject will be informed of the new purpose and consent sought and obtained before any processing occurs.

**6.3 Adequate, Relevant and Non-excessive processing**

Personal data should only be collected to the extent that it is required for the specific purposes that the data subject has consented to or for any other lawful purpose specifically permitted by the GDPR. We shall ensure that only necessary data is collected and that any data which later becomes irrelevant will be destroyed.

**6.4 Accurate Data**

Personal data must be accurate and kept up to date. We shall take steps to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed.

**6.5 Timely Processing**

Personal data should not be kept longer than is necessary for the purpose for which it was collected. We shall ensure that data is destroyed or erased from our systems when it is no longer required.

**6.6 Processing in line with Data subject’s rights**

Data must be processed in line with data subjects' rights. We shall ensure that data subjects have a right to the following:

* To request access to any data held about them (known as a subject access request)
* To prevent the processing of their data for direct-marketing purposes
* To have inaccurate data amended
* To prevent processing that is likely to cause damage or distress to themselves or anyone else
* To have their data deleted (i.e. to be ‘forgotten’)

**6.7 Security and Disclosure of Personal Data**

The GDPR requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We shall ensure that appropriate security measures are taken to prevent unlawful or unauthorised processing or disclosure of personal data and against the accidental loss of, or damage to, personal data.

In particular, we shall ensure that personal data is only disclosed in accordance with this policy.

**We shall also take the following steps to secure personal data:**

* Only those employees or volunteers who are authorised to use the data will be able to access it and process it
* Data administrators will only keep current records on their password-controlled secure computers, and always password protected
* Desks and cupboards will be kept locked if they hold personal data of any kind whether on computer or in a filing system
* When destroying personal data, paper documents will be shredded and CD-ROMs will be physically destroyed
* Data users will be required to ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC or lock their computer when it is left unattended

When receiving telephone or email enquiries, employees and volunteers will be required to be careful about disclosing any personal data held on our systems. In particular they will:

* Check the caller's identity to make sure that data is only given to a person who is entitled to it
* Suggest that the caller put their request in writing where the employee or volunteer is not sure about the caller's identity and where their identity cannot be checked
* Refer to the Data Protection Officer for assistance in difficult situations

If personal data is to be transferred to a third-party data processor (such as a supplier or IT consultant) under contract, the GDPR stipulates mandatory topics which must be included in the contract. If organisations fail to do this both controllers and processors can be fined. If third party organisations provide our partnership with services and they can access personal data then this applies to us.

Any such contract must include the following:

* Processor must process data only on the instructions of the data controller
* People authorised to access data are subject to confidentiality
* Ensure security of processing
* Assist the controller in complying with data subjects rights (where possible).
* Assist the controller with regard to security measures, breach reporting and DPIAs (Data Protection Impact Assessment).

Personal data will only be transferred to a third-party data processor under contract to the Church Council, if they comply with the GDPR requirements.

**6.8 Dealing with subject access requests**

A formal request from a data subject for information we hold about them must be made in writing or by email to the Data Protection Officer. There is no charge. Employees or volunteers who receive a subject access request will forward it to the Data Protection Officer immediately who will take appropriate action in accordance with the GDPR.

1. **The rights of individuals:**
* The right to be informed
* The right of access to their data
* The right to rectification (correction of any errors)
* The right to erasure (also known as the right to be forgotten)
* The right to restrict processing
* The right to data portability (i.e. data must be capable of being easily transferred from one IT system to another). It only applies in certain circumstances and is unlikely to affect parishes.
* The right to object in certain circumstances. E.g. If a parish has relied on ‘legitimate interest’ to process data without consent then an individual can object to this processing.
* The right not to be subject to automated decision making including profiling.

**8. Website**

Any website operated by the Church Council shall comply with this policy. A statement will appear on the website to give users information on how the Church Council collects and processes personal data

through use of the website, including any data users may provide through this website.

 **9. Registration with Information Commissioner’s Office**

With effect from 7 April 2022 the Church Council of St. Augustine of Canterbury, North Springfield is registered with the ICO for CCTV (for security and crime prevention) and for processing of all personal data including sensitive data which is required for its legitimate church purposes. This registration covers both the church and the car park.