

# ST ANDREW'S HAUGHTON LE SKERNE

## GDPR POLICY

### Purpose

The purpose of the Policy is to explain how we maintain the security of personal data that the church collects and uses in the course of its normal business. The document is part of a suite of GDPR documents listed at the end of this document.

### Special Category Data

The PCC is aware that as well as general personal data, there is Special Category Data that requires particular attention. This is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.
- Criminal Offence Data

### Procedures for Ensuring Compliance with the Principles of GDPR

#### **Accountability**

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of the PCC as our Data Controller
- Collecting the minimum personal data required
- Maintaining documentation of our processing activities
- Implementing appropriate security measures in relation to the personal data we process
- Carrying out data protection impact assessments for our processing

We regularly review our accountability measures and update or amend them when required.

#### **Lawfulness, Fairness and Transparency**

Processing personal data must be lawful, fair and transparent.

The legal basis for collecting and processing personal data is

- consent;

- contract;
- legal obligation;
- vital interests;
- public task; and
- legitimate interests.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, and this policy document.

Our processing for the purposes of employment relates to our obligations as an employer.

### **Purpose Limitation**

We process personal data for purposes given in the Privacy Notice.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

### **Data Minimisation**

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

### **Accuracy**

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

### **Storage Limitation**

All personal data including special category data processed by us for the purpose of employment, other legal requirements or our business needs is retained for the periods set out in our Data Retention Policy. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our Data Retention Policy is reviewed regularly and updated when necessary.

### **integrity and Confidentiality (security)**

Our electronic systems and physical storage have appropriate access controls applied.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

### **Third Party Processing of Data**

At times we will use third-party data processors as part of our business. An example of this is processing DBS checks.

When we use third-party data processors as part of our business, in order to comply with the Regulations, we must ensure that specific direction about data processing is given in the contract along with minimum set of terms to ensure data security. Guidance on this can be found at [What needs to be included in the contract? | ICO](#)

If we are 'calling off' services on a contract to which we are not a party, we must ensure that the contract fulfil the requirements of the Regulations. This will usually be achieved by obtaining a copy of the contract.

### **Retention and Erasure Policies**

Our retention and erasure practices are set out in our Data Retention Policy

### **GDPR Policy Review Date**

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed every three years, subject to any regulatory or legislative updates

### **Related Policies and Documents**

- Privacy Policy
- GDPR Data Retention Policy
- GDPR Data Breach Policy
- GDPR Subject Access Request Policy
- GDPR Complaints Policy
- GDPR Data Audit
- GDPR Data Impact Assessment – Risk Assessment