



ALL SAINTS' CHURCH, BANSTEAD

DATA PROTECTION POLICY & PRACTICE

Overview

All Saints' Church, Banstead, recognises the importance of the correct and lawful treatment of personal data. All personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the General Data Protection Regulation in effect from May 2018.

All Saints' Church uses personal data about living individuals solely to facilitate:

- Normal church administration - including employee data, safeguarding, rotas, financial records of giving for tax purposes;
- Church committees, groups and activities organised by All Saints' Church;
- Pastoral care, including calls and visits;
- The Church's Electoral Roll;
- Communications regarding church activities;
- The production of a church directory (confidential to clergy, churchwardens and administrator) for pastoral purposes.

The PCC is also responsible for the Churchyard and for the Church Institute and may use personal data for

- Lettings (paid or unpaid) of parts of the premises;
- Upkeep and maintenance.

The lawful basis for processing¹ personal data is explained in our Privacy Notice, obtainable from the Parish Office and our website www.bansteadallsaints.com. The PCC accepts responsibility for ensuring that all staff and volunteers of All Saints' Church are conversant with good practice on Data Protection.

Categories of Data

Data is information which is recorded as part of a relevant filing system, whether manual or computerised. There are two basic categories of data:

- Personal Data is information relating to a living individual who can be identified from the data, e.g. name and address details;
- Sensitive Personal Data is information relating to any of the following:
 - Racial or ethnic origins of the person;
 - Political opinions;
 - Religious beliefs;
 - Trade union membership
 - Physical or mental health;
 - Sexual life;

¹ Processing is anything done with/to personal data, including storing it.

- The commission or alleged commission of any offence, and any proceeding in relation to such commission or alleged commission

In order to process both these types of data, consent from the individual must be obtained. When consent is given for 'sensitive personal data' (which will apply to much of the personal data processed for Church purposes because it relates to or implies 'religious belief'), such consent must be explicit, freely given, informed, unambiguous, and able to be withdrawn.

All Saints' Church fully endorses and adheres to the following underlying principles of Data Protection.

The Principles

The principles require that personal data shall:

1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
3. Be adequate, relevant and limited to what is necessary
4. Be accurate and, where necessary, kept up to date
5. Not to be kept for longer than is necessary for that purpose
6. Be processed in accordance with the data subject's rights
7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures
8. And not 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.

Maintaining Confidentiality

All personal data is to be treated as private and confidential information and is not to be disclosed to anyone other than those who need access to the personal data solely in order to facilitate pastoral care and staff administration in dealing with the day-to-day ministry of the Church.

There are four exceptional circumstances to the above permitted by law:

- Where we are legally compelled to do so;
- Where there is a duty to the public to disclose;
- Where disclosure is required to protect your interest;
- Where disclosure is made at your request or with your consent.

Storage and Retention

Data is distributed among a number of computers (both Church and privately owned) and in paper format by those who have a need to either maintain, process or use the data.

All personal information held by staff (clerical and lay) and volunteers on behalf of All Saints' Church will be held and processed in a sufficiently secure manner (whether in paper or electronic form) to prevent unauthorised access (whether by unauthorised church staff or third parties). This means those responsible for data storage undertake to:

- Store paper-based information in secure lockable cupboards or filing cabinets;
- Use password protection for electronic documents;

- Adequately protect devices used for electronic storage with the latest updates to the operating system, antivirus, firewall and any other technical measures which are necessary;
- Restrict access to both paper and electronic personal data to those who need to process it for one of the above uses;
- Ensure that when personal information is transmitted this is done securely in a way that cannot be intercepted by unintended recipients.

Generally, when data is no longer required, electronically held data should be erased, ensuring that temporary files and backups are also erased, and paper records should be shredded. Some data (e.g. marriage and burial registers) must be retained: see the guidance in https://www.churchofengland.org/sites/default/files/2017-11/care_of_parish_records_keep_or_bin_-_2009_edition.pdf

Right to Access Information

Employees and other subjects of personal data held by All Saints' Church have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. This right is subject to certain exemptions, e.g. personal information may be withheld if information relating to another individual is included.

All individuals who are the subject of personal data held by All Saints' are entitled to:

- Ask what information All Saints' holds about them and why;
- Ask how to gain access to it;
- Be informed how to keep it up to date;
- Be informed what All Saints' Church is doing to comply with its obligations under the General Data Protection Regulation.

Any person who wishes to exercise this right should make the request in writing to the Churchwardens. A response shall be provided within one calendar month.

What if there is a Breach?

A personal data breach is one that leads to the accidental or unlawful loss, alteration, unauthorised disclosure of or access to personal data. If a breach is detected which might result in a high risk to an individual (e.g. of identity theft) All Saints' will inform the affected individual and the Information Commissioner's Office within 72 hours, and report on the potential scope of the breach, its cause and the mitigation actions the PCC will undertake. Advice will be sought from the Diocesan Registrar where necessary.

Data Protection Controller

The Data Protection Controller for most data held by All Saints' Church for purposes of administration and pastoral care is the PCC.

As a separate legal entity the Vicar is a Data Protection Controller for personal data held in her role as incumbent.

Queries should be addressed to the Churchwardens - churchwarden@bansteadallsaints.com or via the Parish Office (01737 379289).