



St. Michael & All Angels

CHURCH IN THE PARK | LIVING, LOVING, SERVING

DATA PROTECTION AND PRIVACY POLICY

The following policy was agreed at the Parochial Church Council (PCC) meeting held on ...

1. **Purpose of this policy.** This policy sets the Church's understanding of data protection and the policies the PCC uses to ensure compliance with the Data Protection Act 2018, which encompassed the UK General Data Protection Regulation (GDPR).
2. **Why the PCC needs this policy.** The Data Protection Act 2018 places a responsibility on all organisations that handle personal data to protect that information. It also states that charities and other organisations must register with the Information Commissioner's Office under various circumstances, including if they use Closed Circuit Television (CCTV) for crime prevention. The specifics of the church's use of CCTV are covered in a separate policy.
3. **Why the PCC collects information.** The PCC may collect data on individuals for the following purposes:
 - a. Administration of financial accounts and records.
 - b. Advertising, marketing and public relations.
 - c. Officer holder, subcontractor and volunteer administration.
 - d. Administration of membership records, including the generation of the church's Electoral Roll.
 - e. Fundraising, including the generation of Gift Aid returns to HM Revenue & Customs.
 - f. Realising the objectives of a charitable organisation or voluntary body.

4. **How the PCC collects information.** The PCC may collect personal information when individuals contact with it, such as when they:

a. Visit **the church** website.

b. Register their details using a paper form or via an electronic form on our website.

c. Make a donation, by completion of offering envelopes or by electronic means.

d. Register for a course or other church event.

e. Communicate with the PCC, such as face-to-face or by email, letter and telephone.

f. Access social media platforms, such as Facebook.

5. **What the PCC does with collected information.** The PCC processes and stores information in the form of paper and computer records; its preferred method of storing personal information is in its computer database called ChurchSuite. Data security and privacy information about ChurchSuite can be found on the ChurchSuite website: <http://churchsuite.com>

Policy statements - how the PCC will handle and protect personal information

6. The PCC complies with all aspects of data protection legislation, adhering to the eight principles of the GDPR. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data.

7. The PCC will not pass personal data to third parties without the explicit consent of individuals, except when permitted by law under the following exceptional circumstances:

a. Where the PCC is legally compelled to do so.

b. Where there is a duty to the public to disclose.

c. Where disclosure is required to protect **an individual's** interest.

d. Where disclosure is made at an individual's own request or with their consent.

8. The PCC will use a standard statement whenever personal data is collected. Individuals submitting their information on a paper or electronic forms will be required to date the form (whether in writing or by electronic date stamp) to indicate they have given their consent. If individuals provide their personal data verbally, such as in person or over the telephone, the person receiving the information will read out the statement and record the date when the individual's consent was given. The statement for use is:

I consent that this information may be used to contact me about St Michael & All Angels Church activities, used for church administration purposes and stored in computerised or paper formats. I am aware that, in compliance with **UK data protection law**, the church will store my information securely and will never pass it to a third party without my explicit permission. I am aware that I can contact any of the church's officers or administrators at any time to withdraw this consent and to ask that any information held about me is permanently destroyed.

9. **Under UK law, children are able to give consent at age 13, which means that consent should come from the child rather than the parent/guardian from age 13 unless there are other reasons why the child does not have the capacity to consent.**

10. The PCC will permit access to **an individual's** own personal data upon request at no charge. Such requests should be made to the **Incumbent (the Vicar)**..

11. The PCC will update **an** individual's information when notified, typically through the My ChurchSuite tool.
12. The PCC will delete all paper and electronic records about an individual when that individual, or their empowered representative, asks the PCC to do so or when the PCC no longer has a need to retain that information. This will apply unless that information is a legal record, such as an entry in the church's registers, **or where the information is required to support an investigation.**
13. The PCC will do its best to ensure all **people acting on its behalf** are conversant with data protection legislation and practice. All people with access to personal data, other than data which individuals agree to share with the church community, will be **asked to read, understand** and comply with this policy. They will be **requested to do so again** every 3 years or whenever there is a material change to this policy.

Who will have access to personal data

14. Individuals **are** able to share as much, or as little, of their personal contact information with other church members as they would like, setting that level of access using their individual ChurchSuite login.
15. Individuals who are church officer holders or who hold voluntary roles within the church will be asked to confirm their consent before their contact information is published or displayed.
16. Where individuals provide their own contact information for publication (such as on a poster, for a notice in the pew newsletter or for an article in Outlook magazine), their consent for **that** particular publication will be implied.
17. Where individuals provide their bank account details, for the purposes of receiving reimbursement for expenses paid, their consent to share that information with the PCC's bank will be implied.
18. The PCC will control access to the main ChurchSuite database by:
 - a. Providing individual logins and requiring people to set their own, strong passwords.
 - b. Providing access to the various modules within the database on a "need to access" basis only; the modules containing Children's and Giving information will have additional password controls applied. Examples of people who may need access to the main database include the Ministry Team, the PCC Administrator, members of the PCC and rota coordinators.
 - c. Controlling access via a Data Controller and other specified administrators, who will be the only people who can access and set these security parameters.

Oversight of personal data

19. The PCC has appointed the Parish Administrator to be its Data Controller. Their role is to:
 - a. Maintain a record of who has access to which elements of personal data, including paper records.
 - b. Implement controlled access to personal data.
20. The PCC will appoint a Data Protection Officer whose role is to:
 - a. Review and update this policy as required, such as if the applicable data protection legislation is updated or at the direction of the PCC.
 - b. Handle and investigate any discovered, alleged or reported misuse or mishandling of personal data by the PCC.
 - c. Conduct an audit of the PCC's personal data handling policies, procedures and practices at least once every 2 years or sooner if requested by the PCC.

Additional guidance

This guidance expands on, but does not supersede, the statements set out in the main Data Protection and Privacy Policy

- All personal data held must be secured against unauthorised access and theft:
 - IT systems used to process information should be made as secure as possible from unauthorised access, including via the Internet, and should have anti-virus software installed that automatically installs updates as soon as they are available.
 - Church PCs should be password protected and are locked or logged off when individuals are away from their desk.
 - Paper records should be locked away when not in use.
- Information about any individual that enables that individual to be identified **must** not be given to any person outside the Church without the express permission of the individual concerned.
- **Churchsuite must be used as the primary means for storing and accessing personal information, for sending of messages to the church community, for signing-up people for events, activities or groups, or for arranging rotas.**
- If emails **must be sent and if they** are being sent to multiple addressees, blind copies (using the BCC line) should be used to avoid sharing individuals' email addresses.
- Consent **must** be obtained from individuals before their information is put on the website or in a publication. This can be implied if someone provides their contact details for a notice or Outlook article but, if that person provides another individual's contact information, the consent of that other individual should be checked.
- Personal data **must** be securely deleted or destroyed when it is no longer required. As a guideline, information about a person should be archived a maximum of 18 months after not having contact with an individual and deleted 1 year after archival (or sooner if the individual requests it).
- Personal data **must** not be accepted from another organisation without the consent of the individual concerned.
- **Should people performing roles for the church or PCC ignore or disregard this guidance or the Church's Data Protection and Privacy Policy, they may become personally liable for any harm or loss caused by the misuse or mishandling of personal data entrusted to them.**