St. Michael and All Angels' Church, Sandhurst

Data Protection Policy

The protection of personal data is enshrined in UK law, but it is also a moral responsibility that St. Michael and All Angels' Church, Sandhurst takes seriously. Embedding data protection within the organisation benefits St. Michael and All Angels' Church, Sandhurst and all individuals who interact with us, by enabling a uniform and consistent decision making, building a culture of awareness and responsibility, making personal data management and infrastructure more resilient; and, through transparency and accountability, instilling trust and confidence in individuals when they provide us with their data, and ensuring their rights and freedoms are upheld.

Data refers to all information where a person is identifiable and this includes images.

The purpose of this policy is to describe the steps that St. Michael and All Angels' Church, Sandhurst are taking to comply with data protection legislation, to ensure that our compliance with the relevant legislation is clear and demonstrable. We also have a specific page on our website summarising this and it is found here http://www.stmichaels-sandhurst.org.uk/data-protection.html

This policy is also intended to provide us with measures for ensuring that risks to individuals through misuse of personal data are minimised, such as:

- personal data being used by unauthorised individuals through poor security or inappropriate disclosure;
- individuals being harmed by decisions made using inaccurate or insufficient data;
- individuals being uninformed by lack of transparency leading to unlawful practice;
- the invasion of privacy due to over-collection or over-retention of data.

1) Definitions
    a. **Data Subject** - The individual to whom the data being processed relates.
    b. **Data Controller** - A body or organisation that makes decisions on how personal data is being processed. Data Controllers almost always also process data.
    c. **Data breach** - any occasion when personal data is: accidentally or unlawfully lost, destroyed, corrupted or disclosed; accessed or passed on without proper authorisation; or made unavailable (through being hacked or by accidental loss/destruction.
    d. Data Processor
    e. **Personal data** is any information about a living individual, which is capable of identifying that individual:
        i. on paper *as well as* digital/electronic
        ii. images *as well as* text (e.g. photos, CCTV)
        iii. don't forget *indirect*
    f. **Sensitive Personal data** is any information relating to an individual's
        i. Racial or ethnic origin
        ii. Sexual orientation
        iii. **Religious**, political or trade union affiliation
        iv. Genetic or biometric data
        Known as '**special category**' data.
        NB Christian religious affiliation can be *inferred* for church members.

2) Principles of Data Protection
    a. Data processing must be **lawful**, **fair** and **transparent**
    b. For explicit legitimate **limited purposes** only
    c. Hold no more data than necessary for the purpose (**data minimisation**)
    d. Data must be kept **accurate** and up to date
    e. Keep data for no longer than necessary (**storage limitation**), after which destroy, delete or return it

f. Keep data secure: protect against accidental loss, damage, disclosure (**integrity and confidentiality**)
g. Data controllers are **accountable** for compliance and must be able to demonstrate compliance

3) Rights of Individuals
   - **Right to be Informed;** Informed about the collection and use of their personal data (transparency)
   - **Right of Access** (a.k.a. Subject Access Request) may be made verbally or in writing. One month to respond. No fee.
   - **Right to rectification** Correcting inaccurate data
   - **Right to erasure** (right to be forgotten)
   - **Right to restrict/suppress processing** In certain circumstances: store data but not use it.
   - **Right to Data Portability** Ease of movement between IT environments
   - **Right to Object** Absolute right with regard to direct marketing
   - **Rights in relation to automated decision-making and profiling**

4) Lawful reasons for collecting and holding data
   The examples in this section are samples only and not an exhaustive list.
   a. **Legitimate interest** – needed for performance of main business, and 'balance of interests'
      i. E.g. rota distribution list
   b. Necessary to fulfil **contractual obligation**
      i. E.g. hirers of Pastoral Centre
   c. **Legal obligation** of the data controller
      i. E.g. gift aid records, registers (baptisms, marriages, funerals)
   d. Data subject has given **consent**
      i. E.g. Next of kin for funerals so they can receive memorial service invites.
   e. Needed to protect **vital interests** (i.e. someone's life) of the data subject
      i. E.g. Safeguarding
   f. **Public task**

5) Safeguarding
   On occasions safeguarding may come into conflict with data protection. As safeguarding is of paramount importance the need to safeguard will always override data protection matters. The Safeguarding policy of St. Michael and All Angels church covers images of children and vulnerable adults.

6) Age Consent
   Under GDPR legislation the age of consent for people to provide consent for their personal data to be used is 13 (thirteen); however at St. Michael and All Angels, all people under 16, parental consent will be obtained.

7) Privacy Policy
   Individuals have the right to be informed about the collection and use of their personal data and St. Michael and All Angels' Church, Sandhurst will be open and transparent about our use of personal data in line with this Policy. Our current privacy notice is attached to this policy as Appendix 1 and can also be found on our website.

8) Cookie Policy
   A "cookie" is a small text file which collects data about the websites you visit. St. Michael and All Angels' doesn't directly collect cookies, however our website provider does. Our cookie policy is attached to this policy as Appendix 2 and can also be found on our website.

9) Data Breach Process

Under GDPR legislation we are required to have a process for dealing with breaches in data protection. This is outlined in our Data protection Process which is attached to this policy as Appendix 3 and also available on our website.

10) Subject Access Request Process

Under the legislation people are entitled to ask to review the information we hold about them. This is known as a "Subject access Request". Our process for dealing with Subject Access Requests are outlined in the process in the attached Appendix 3 and is also on our website.

11) Best Practices for Handling Data

All staff and volunteers handling data will be requested to comply with the best practices for handling personal data set out below.

a) Email correspondence: A new email per subject to ensuring that all relevant information is included. Using BCC to send out emails to groups.
b) Not re-using old lists / information unless permission has been obtained.
c) To ensure that data stored is up-to-date and that once an event has passed to ensure the data is confidentially shredded/destroyed.
d) Not to pass personal contact details onto other people unless they have provided their permission.
e) Only using the personal data for the reason it was collected for. For example, churchyard helpers can only be contacted about matters relating to the churchyard.
f) Ensuring that where photos are taken at church events, people in those photos are aware that their photo may be used in church publications, social media and on the web.

12) Renewal of Policy

Data Protection will be a regular item on Parochial Church Council meeting agendas to ensure that data protection is regularly reviewed in light of the activities we undertake and this policy, along with all appendices will be renewed every two years.

The following appendices are an integral part of this Data Protection Policy

Appendix 1: Data Privacy Notice
Appendix 2: Cookie Policy
Appendix 3: Data Breach Process
Appendix 4: Subject Access Request Process

February 2020

DATA PRIVACY NOTICE

The Parochial Church Council (PCC) of St Michael and All Angels', Sandhurst

1. Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

2. Who are we?

The PCC of St. Michael and All Angels', Sandhurst is the data controller (contact details below). This means it decides how your personal data is processed and for what purposes. This includes the different groups of St. Michael's, (for example choir).

3. How do we process your personal data?

The PCC of St. Michael and All Angels', Sandhurst complies with its obligations under the "GDPR" by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

We use your personal data for the following purposes: -

- To provide support to the NHS Test and Trace for COVID-19 and any other Public Health requirements
- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area;
- To administer membership records;
- To fundraise and promote the interests of St. Michael and All Angels Church;
- To manage our employees and volunteers;
- To maintain our own accounts and records (including the processing of gift aid applications);
- To inform you of news, events, activities and services running at St. Michael and All Angels' Church.
- To run specific activities connected to St. Michael and All Angels' Church.
- Our processing also includes the use of CCTV systems for the detection and prevention of crime
- To process Gift Aid donations/applications
- To contact individuals via surveys to conduct research about their opinions of current services or of potential new services that may be offered.

4. What is the legal basis for processing your personal data?

- Explicit consent of the data subject for public health purposes as outlined in NHS Test and Trace[1]
- Explicit consent of the data subject so that we can keep you informed about news, events, activities and services and keep you informed about parish events.
- Processing is necessary for carrying out legal obligations in relation to Gift Aid or under employment, social security or social protection law, or a collective agreement;
- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided: -

[1] For more information about Test and Trace, and how they will use your personal details, please see the Government guidance website: https://www.gov.uk/guidance/nhs-test-and-trace-how-it-works

- the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and
- there is no disclosure to a third party without consent.

5. Sharing your personal data
Your personal data will be treated as strictly confidential and will only be shared with other members of the church in order to carry out purposes connected with the church including the running of the church and the groups within the church, as applicable. We will only share your data with third parties outside of the parish with your consent (for example, to recover tax on Gift Aid donations). Your personal data may be stored on "cloud" servers which may or may not be in the EU. In the event of a crime or a possible crime being committed, images from CCTV may be passed to the police without your consent.
Data collected for NHS Test and Trace support will be passed to NHS Test and Trace if requested by public health authorities.

6. How long do we keep your personal data[2]?
We keep your personal data in accordance with the guidance set out in the guidance from the Church of England, which is available from the Church of England website [see footnote for link], where multiple documents exist the latest available will be used.

Specifically, we retain electoral roll data while it is still current (it is renewed every 6 years); gift aid declarations and associated paperwork for up to 6 years after the calendar year to which they relate; and parish registers (baptisms, marriages, funerals, burials) permanently.

For data collected for the NHS Test and Trace your data will be kept for 21days and will not be used for any other purposes.

7. Your rights and your personal data
Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- The right to request a copy of your personal data which the PCC of St. Michael and All Angels' Church. holds about you;
- The right to request that the PCC St. Michael and All Angels' Church corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for the PCC St. Michael and All Angels' Church to retain such data;
- The right to withdraw your consent to the processing at any time
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable)
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable)
- The right to lodge a complaint with the Information Commissioners Office.

8. Further processing
If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing. In the event that there is a conflict between our data privacy notice and safeguarding policy, then safeguarding policy takes precedence.

---

[2] Details about retention periods can currently be found in the Record Management Guides located on the Church of England website at: - https://www.churchofengland.org/more/libraries-and-archives/records-management-guides

9. Contact Details

To exercise all relevant rights, queries or complaints please in the first instance contact the Parish Office at St. Michael and All Angels' Church, Lower Church Road, Sandhurst, Berkshire, GU47 8HN; 01252 873030; office@stmichaels-sandhurst.org.uk

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

Appendix 2

St. Michael and All Angels' Church, Sandhurst

Cookie Policy

In accordance with European law on cookies and data protection, when people visit our website (www.stmichaels-sandhurst.org.uk) people are asked if they accept cookies or not.

The St Michaels Church website does not collect any personal data, and we do not directly save or use any data in cookies.

However the website is created and hosted by Weebly, who automatically insert cookie handling for their own purposes. This is outside our control, and the detail is the responsibility of Weebly. On first visit to the site, users are invited to opt-in to the use of cookies, and to the best of our knowledge this complies with the relevant GDPR requirement.

Approved by PCC 8May2019

Appendix 3

Data Protection Breach

St. Michael and All Angels' Church takes its responsibility under the data protection legislation (GDPR) legislation seriously and is committed to ensuring that all personal data which is held is done so in a secure manner and that only authorised individuals have access to the data.

A personal data breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Anyone can report a breach to the Rector and Churchwardens.

Breach Process

The following process will be followed:

1) A breach is identified
2) Rector and Churchwardens are informed
3) Record the breach on the log which will ensure that appropriate corrective actions are implemented.
4) Within 7 days, Rector and Churchwardens assess the severity of the breach and identify the root cause of breach. The items assessed be the likelihood and severity of the resulting risk to people's rights and freedom (section 85 of GDPR). This includes
    a. Result in physical, material or non-material damage include but not limited to,
        i. Loss of control over their personal data
        ii. Limitation of their rights
        iii. Discrimination,
        iv. identity theft or fraud
        v. Financial loss
        vi. Damage to reputation
5) Identify the people affected by the breach.
6) Review the policies, procedures and training.
7) The Churchwardens/Rector will notify the Diocesan Secretary, the Diocesan registrar and if advised the Information Commissioner within 72 hours (GDPR mandatory timeline)
8) If applicable, inform the individuals affected about the breach.

Failure to report a breach to the ICO (if required) can result in a significant fine up to 2% of our turnover.

Sample Data Breach Log

Date	Details of Breach	Person Reporting	Severity	Corrective Actions

Approved by PCC 8-May-2019

Appendix 4

Subject Access Request Process for
St. Michael and all Angels Church, Sandhurst

St. Michael and All Angels Church, Sandhurst acknowledge that under Data Protection legislation, one of the rights of individuals is to request what information we hold on them.

Anyone is entitled to make a subject access request on behalf of themselves and they should make this in writing (either handwritten or email) to the Rector and Churchwardens who can be contacted via the Parish Office.

The Rector and Churchwardens will then respond to the enquirer within 1 calendar month of the request being made. If for some reason there would need to be a delay in responding to the request (for example of the Christmas and Easter periods) then we will inform the person as soon as possible and advise them when the response will be made by.

In accordance with the data protection legislation, there will be no charge for this request or for responding.

If any data is found to be inaccurate then St. Michael and All Angels will take all reasonable steps to correct this data wherever possible, the exception for correcting personal data will be where the entries are the registers.

July 2019