

# Data Protection Policy

## 1. Data Protection Policy statement

Maidstone Road Baptist Church holds and processes personal data about people (data subjects) for the purpose of general church administration and communication. The data may come directly from the person it is about, or from other sources such as previous employers and other churches. Personal data may be held in electronic and paper form, all personal data is subject to data protection law.

Maidstone Road Baptist Church is committed to protecting personal data and respecting the rights of our data subjects; the people whose personal data we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all relevant laws, and adopting good practice.

We process personal data to help us:

- a) maintain our list of church members and regular attendees
- b) provide pastoral support for members and others connected with our church
- c) safeguard children, young people and adults at risk
- d) recruit, support and manage staff and volunteers
- e) maintain our accounts and records
- f) promote our services
- g) respond effectively to enquirers and handle any complaints

This policy has been approved by the church's Charity Trustees who are responsible for ensuring that we comply with all our legal obligations and by the church members.

## 2. Why this policy is important

This policy sets out the measures we are committed to taking as an organisation to protect, keep safe and ensure accuracy of personal data and what each of us should do to ensure we comply with the relevant legislation.

We will make sure that all personal data is processed in line with the Data Protection Principles which in summary form state that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner
- b) processed for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes
- c) adequate, relevant and limited to what is necessary for the purposes for which it is being processed
- d) accurate and, where necessary, up to date
- e) not kept longer than necessary for the purposes for which it is being processed
- f) processed in a secure manner, by using appropriate technical and organisational means
- g) processed in keeping with the rights of data subjects regarding their personal data

# **Maidstone Road Baptist Church, Felixstowe Data Protection Policy and Practice**

## **3. How this policy applies to different roles in the church & what you need to know**

### **3.1 As an employee, trustee or volunteer**

As an employee, trustee or volunteer processing personal information on behalf of the church, you are required to comply with this policy. If you think that you have accidentally breached the policy it is important that you contact our Data Protection Trustee immediately so that we can take swift action to try and limit the impact of the breach.

Anyone who breaches the Data Protection Policy and Practice may be subject to disciplinary action, and where that individual has breached the policy intentionally, recklessly, or for personal benefit they may also be liable to prosecution or to regulatory action.

Before you collect or handle any personal data as part of your work (paid or otherwise) for Maidstone Road Baptist Church, it is important that you take the time to read this policy and practice carefully and understand what is required of you, as well as the organisation's responsibilities when we process data.

If you are unsure about whether anything you plan to do, or are currently doing, might breach this policy and practice you must first speak to the Data Protection Trustee

### **3.2 As a leader of a group**

As a leader of a group (e.g. CKers) you are required to make sure that any procedures that involve personal data, that you are responsible for in your group, follow the rules set out in this Data Protection Policy and Practice.

### **3.3 As an attendee/contact of the church**

As a data subject of Maidstone Road Baptist Church we will handle your personal information in line with this policy and practice.

### **3.4 As the Data Protection Trustee**

Our Data Protection Trustee is responsible for advising Maidstone Road Baptist Church and its staff and members about their legal obligations under data protection law, monitoring compliance with data protection law, dealing with data security breaches and with the development of this policy and practice.

## **4. Training and guidance**

We will provide general training at least annually for all people processing personal information on behalf of the church to raise awareness of their obligations and our responsibilities.

## **5. What personal information do we process?**

There are two categories of information that the church processes.

### **5.1 Personal data**

Personal data is information relating to a living individual who can be identified from that data. Personal data can be factual such as name, address or date of birth, or it can be opinion such as

## Maidstone Road Baptist Church, Felixstowe Data Protection Policy and Practice

performance appraisal. It includes images of individuals provided the image is clear enough for particular individuals to be identified.

### 5.2 Sensitive Personal Data

Sensitive personal data includes information about a person's: racial or ethnic origin; political opinions; religious or similar (e.g. philosophical) beliefs; trade union membership; health (including physical and mental health, and the provision of health care services); genetic data; biometric data; sexual life and sexual orientation.

## 6. How we follow the data protection principles

### 6.1 Personal data is processed lawfully, fairly and in a transparent manner

Processing of personal data must meet a legal condition and must be performed transparently i.e. we provide people with an explanation of how and why we process their personal data at the point we collect data from them, as well as when we collect data about them from other sources.

Processing of personal data is only lawful if at least one of these legal conditions is met:

- a) the processing is necessary for a contract with the data subject;
- b) the processing is necessary for us to comply with a legal obligation;
- c) the processing is necessary to protect someone's life (this is called "vital interests");
- d) the processing is necessary for us to perform a task in the public interest, and the task has a clear basis in law;
- e) the processing is necessary for the legitimate interests pursued by Maidstone Road Baptist Church, unless these are overridden by the interests, rights and freedoms of the data subject.
- f) If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their clear consent.

Processing of sensitive personal data is only lawful when, in addition to the conditions above, one of these extra conditions is met:

- a) the processing is necessary for carrying out our obligations under employment and social security and social protection law;
- b) the processing is necessary for safeguarding the vital interests (in emergency, life or death situations) of an individual and the data subject is incapable of giving consent;
- c) the processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes;
- d) the processing is necessary for pursuing legal claims.
- e) If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent.

The advice we have been given is that we should obtain written consent for any personal information we publish e.g. Church Directory.

The advice we have been given about groups and others within the church sharing contact details with each other is that communications within house groups or internal church groups do not involve sharing information with the church/Trustees as the Data Controller, so would not require privacy statements or require consent.

## **Maidstone Road Baptist Church, Felixstowe Data Protection Policy and Practice**

When personal data is collected directly from the individual, we will inform them in writing about; our identity/contact details and those of the Data Protection Trustee, the reasons for processing, and the legal bases, explaining our legitimate interests, and where relevant, the consequences of not providing data needed for a contract or statutory requirement; who we will share the data with; if we plan to send the data outside of the European Union; how long the data will be stored and the data subjects' rights. This information is provided in a 'Privacy Notice' and will be given at the time when the personal data is collected.

If data is collected from another source, rather than directly from the data subject, we will provide the data subject with the information described above as well as: the categories of the data concerned; and the source of the data. It will be provided to the individual in writing and no later than within 1 month after we receive the data, unless a legal exemption under the GDPR applies. If we use the data to communicate with the data subject, we will at the latest give them this information at the time of the first communication.

If we plan to pass the data onto someone else outside of Maidstone Road Baptist Church, we will give the data subject this information before we pass on the data.

### **6.2 Personal data shall be processed for specified purposes**

We will only process personal data for the specific purposes explained in our privacy notices (as described above) or for other purposes specifically permitted by law. We will explain those other purposes to data subjects, unless there are lawful reasons for not doing so.

### **6.3 Personal data shall be adequate, relevant and not excessive**

We will only collect and use personal data that is needed for the purposes described in Section 1 above. We will not collect more than is needed to achieve those purposes.

### **6.4 Personal data shall be accurate**

We will make sure that personal data held is accurate and, where appropriate, kept up to date.

### **6.5 Personal data shall not be kept longer than necessary**

We will not keep personal data longer than is necessary for the purposes that it was collected for. We will comply with official guidance about retention periods for specific records. Information about how long we keep records for can be found in the Data Retention Schedule in our practice.

### **6.6 Personal data shall be processed in a secure manner**

We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing.

### **6.7 Personal data shall be processed in keeping with the rights of data subjects**

We will process personal data in line with data subjects' rights, including their right to:

## **Maidstone Road Baptist Church, Felixstowe Data Protection Policy and Practice**

- a) request access to any of their personal data held by us (known as a Subject Access Request)
- b) ask to have inaccurate personal data changed
- c) restrict processing, in certain circumstances
- d) object to processing, in certain circumstances, including preventing the use of their data for direct marketing
- e) data portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation
- f) not be subject to automated decisions, in certain circumstances
- g) withdraw consent when we are relying on consent to process their data.

### **7. Direct marketing**

We will comply with the rules set out in the GDPR, the Privacy and Electronic Communications Regulations (PECR) and any laws which may amend or replace the regulations around direct marketing. This includes, but is not limited to, when we make contact with data subjects by post, email, text message, social media messaging, telephone (both live and recorded calls) and fax.

### **8. Sharing information with other organisations**

We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice), unless legal exemptions apply to informing data subjects about the sharing.

We will follow the ICO's statutory [Data Sharing Code of Practice](#) (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

### **9. Data processors**

We don't use external companies or organisations to process personal data on our behalf.

### **10. Transferring personal data outside the European Union (EU)**

Personal data cannot be transferred (or stored) outside of the European Union unless this is permitted by the GDPR. This includes storage on a "cloud" based service where the servers are located outside the EU.

We will only transfer data outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR

### **11. Data protection impact assessments**

When we are planning to carry out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment (DPIA).

DPIAs will be conducted in accordance with the ICO's Code of Practice '[Conducting privacy impact assessments](#)'.

**Policy adopted by Trustees and Church Members at church meeting held on  
8<sup>th</sup> May 2018                      Signed:**

# Data Protection Practice

## 1. Church's Data Protection Trustee

The Trustees will appoint one of their number to act as the Church's Data Protection Trustee. All questions and concerns in relation to this policy should be addressed to them. As at April 2017 this person is Steve Lineham and they can be contacted via the church administrator.

## 2. Collecting and processing personal data

We collect personal information for the following purposes, there is a privacy notice and information collection form for each purpose. Please use the correct privacy notice/information collection form, if you need to collect personal information for a purpose not covered here then please contact the Data Protection Trustee. We must obtain consent for any instance when we publish personal information.

Purpose	Privacy notice/information collection form	Consent required?	Legal basis
Church member/attendee contact information	Member/attendee information	No	Legitimate interest
Publishing member/attendee contact details in the church directory and birthdays in weekly sheet	Member/attendee information	Yes	Consent
Information for claiming Gift Aid refund	Gift aid	Yes – info sent to HMRC	Legitimate interest
Contact information for carers of children who come to CKers and SMOG and images	Children and youth	Yes for images	Legitimate interest/ consent
Outside groups and organisations using the building	Use of buildings	No	Legitimate interest
Information relating to paid staff e.g. references	Paid staff information	No	Contract with data subject
References and records of volunteers working with children, young adults, and vulnerable adults	Volunteers information	No	Legitimate interest

Requests to withdraw consent by a data subject for the information provided should be passed to the Data Protection Trustee immediately.

Photographs and videos of individuals, in which individuals can be recognised, will not be published without following the following practice:

1. Adults - adults will be informed when photographs are to be taken or video recorded and how they will be used; adults will be told how to opt out of having themselves in any material published

## **Maidstone Road Baptist Church, Felixstowe Data Protection Policy and Practice**

2. Children and young people - explicit and informed consent from their parents will be obtained. We will never publish the names of children and young people alongside their photographs.

DBS checks do not require us to collect personal information. Our DBS administrator confirms a person's identity but does not access or store the information the person has entered. The DBS administrator receives and files a copy of the result of the DBS check.

### **3. Data subjects' rights to access information**

Individuals whose personal information is held by Maidstone Road Baptist Church have the right to access that information. This right is subject to certain exemptions outlined in the Data Protection Act.

Any person who wishes to exercise this right should make the request in writing to the Church Administrator. The request will be forwarded to our Data Protection Trustee immediately. We will act on all valid requests as soon as possible, and at the latest within one calendar month, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances.

If personal details are inaccurate, they can be amended upon request to the Church Administrator. All data subjects' rights are provided free of charge. Any information provided to data subjects will be concise and transparent, using clear and plain language.

When we receive a request we will search all appropriate documents to find any references to the person making the request – where necessary we will redact and/or anonymise information that identifies other parties.

A copy of this policy and practice will be on our church website

### **4. Direct marketing - contacting contacts with information about events.**

Any direct marketing material that we send will identify Maidstone Road Baptist Church as the sender and should say that people can object to receiving similar communications in the future by contacting the Church Administrator. The Church Administrator will record that request and stop the direct marketing as soon as possible.

### **5. Sharing information with other organisations**

Only authorised and properly instructed staff/Trustees are allowed to share personal data with an outside organisation. We will keep records of information shared with a third party.

### **6. Dealing with data protection breaches**

Where staff or volunteers, think that this policy has not been followed, or data might have been breached or lost, this should be reported immediately to the Data Protection Trustee.

The Data Protection Trustee will keep records of data breaches, even if we do not report them to the ICO.

We will report all data breaches which are likely to result in a risk to any person, to the ICO. Reports will be made to the ICO within 72 hours from when someone in the church becomes aware of the

## Maidstone Road Baptist Church, Felixstowe Data Protection Policy and Practice

breach. In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay.

### **7. Data retention**

We will ensure that personal information is not kept for longer than it is needed. We will delete a person's personal information once they no longer attend the church.

### **8. Personal information processed securely**

All personal information held by staff and volunteers on behalf of Maidstone Road Baptist 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:

- We will store paper-based information in secure, lockable cupboards – the paper copies of leadership and church meetings are the master copies
- We will use password protections and/or encryption of particularly sensitive electronic documents
- When sensitive personal matters are discussed in a meeting, such matters will be minuted separately. Such a separate minute won't be circulated with the minutes of the meeting, a paper copy will be stored with the paper copy of the relevant meeting minutes.
- The master copy of electronic versions of meeting minutes and other administrative documents will be stored securely with a GDPR compliant Cloud provider.
- We will restrict access to both paper and electronic personal data to those who need to process
- We will ensure that personal information is transmitted securely in a way that cannot be intercepted by unintended recipients

### **9. Registering with the ICO**

We won't register with the ICO as we understand that we are an exempt organisation. The wording in the GDPR which we believe we meet and which provides the exemption is as follows:

*Are you a not-for-profit organisation that qualifies for an exemption?*

*Answer 'Yes' if your organisation was established for not-for-profit making purposes and does not make a profit. Also answer 'yes' if your organisation makes a profit for its own purposes, as long as the profit is not used to enrich others. You must:*

- *only process information necessary to establish or maintain membership or support;*
- *only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;*
- *only share the information with people and organisations necessary to carry out the organisation's activities. Important - if individuals give you permission to share their information, this is OK (you can still answer 'yes'); and*
- *only keep the information while the individual is a member or supporter or as long as necessary for member/supporter administration.*