EMBA DATA PROTECTION POLICY

We use people's personal details throughout our organisation, in electronic and paper form. In some cases it is very sensitive and confidential information. We also have a large volume of mundane information such as names and contact details of ministers, church trustees, other church members, and church contacts and current, past and prospective staff. We may also receive other personal information from other sources. This policy sets out how we will handle personal details in our organisation.

Purpose of this policy

Laws apply to our use of anyone's personal details. Everyone has rights regarding how their personal information is handled. The purpose of this policy is to set out what measures we are committed to taking, as an organisation and as individual members of staff, to ensure we comply with the law.

Our Policy

East Midland Baptist Association is committed to

a) Complying with data protection law and data subjects' rights under it, in relation to their personal information, whilst it is under our control. The data subject is the person that the personal information identifies or relates to.

b) Complying with the eight principles of data protection as set out below.

c) Handling and processing personal information in line with our Privacy Statement.

Our commitment applies to our handling of personal information throughout its time under our control. It applies to our obtaining, collection, storage, processing and destruction of personal information, and when we transmit it or make it available to third parties.

Summary of the Data Protection Principles (1998 Data Protection Act)

Personal information must be:

(1) Processed fairly and lawfully.

(2) Processed for clearly defined purposes which the data subject is aware of, and which are lawful.

(3) Adequate, relevant and not excessive for the purposes.

(4) Accurate.

(5) Not kept longer than necessary for the purposes.

(6) Processed in line with data subjects' rights.

(7) Secure.

(8) Not transferred to people or organisations outside the European Economic Area, and particularly to countries which lack adequate protection for personal information.

Detailed practice guidance

We have produced a set of 'Good Practice Guidelines' which set out how in practice we will meet our commitment to the above policy. The implications of the eight data protection principles for our work are wide-ranging. These Guidelines are likely to change as our processes of monitoring and review identify issues where policy or guidance is needed, or help us to refine our policy and guidance statements.

If you need any further information about these please contact our Data Protection Officer.

How this policy applies to you

This policy does not form part of your employment contract. However, you are required to comply with this policy and a breach of these rules will be taken seriously and could lead to disciplinary action or dismissal. If you are unsure about whether anything you propose to do might breach our policy speak to the Data Protection Officer for advice first.

From time to time we may need to make changes to this policy or guidance in line with current operational practices and/or legislation. We will tell you of the changes.

Training and guidance

For you to comply with this policy you need a reasonable understanding of the eight principles of data protection (see page 1) and how they apply to your work. We will provide general training for all staff as part of their induction programme. In addition we will provide regular ongoing training to maintain awareness and good practice across our organisations. We may also issue further guidance or instructions from time to time.

How we manage this policy

This policy has been approved by the Board of Trustees, which has appointed the Data Protection Officer to:

- oversee our compliance with the policy, and
- provide or arrange training and guidance for staff and oversee each team's programme of training, awareness and initiatives, and
- act as our nominated contact with the Information Commissioner's Office.

Currently the Data Protection Officer is EMBA Company Secretary Melvyn Gilmour. The EMBA Regional Team Leader is responsible for overseeing compliance with this policy with support from the Data Protection Officer.

Development of this policy

Any questions, ideas or concerns about the operation of this policy or recommendations for additions or amendments should be referred in the first instance to the Data Protection Officer.

Breach of this policy or the law

If you consider that the policy has not been followed in respect of personal information about any person you should report this promptly to your line manager. If they are not available then contact the Data Protection Officer. Line Managers should report breaches to the Data Protection Officer as appropriate.

The Data Protection Officer will keep a record of such reports, and will investigate in appropriate detail. If a breach of the law is found, the Data Protection Officer must consider guidance issued by the Information Commissioner's Office, and all of the following:

- Do we need to change our policy or issue guidance?
- Does any member of staff require training or guidance?
- Is it appropriate to refer the matter to the Moderator of the Staffing Group under our disciplinary policy?
- Should we report the matter to the data subject? Factors to consider include the seriousness of the breach, and whether or not the data subject will be able to do anything to prevent or lessen distress or damage
- Should the matter be reported to the Information Commissioner's Office?

Exceptions and qualifications to the scope of this policy

We may receive, consider or disclose personal information for the purposes of the prevention or detection of crime, or as required by our regulators or by order of the Courts, or for other legitimate purposes.

The specific terms of this policy also do not apply to disclosure of financial or other information to our accountants or for audit purposes, although we will ensure such processing is in line with the Data Protection Act 1998.

Finally, certain key personnel have specific authorisation to hold staff personal information or have access to that information for the purposes of emergencies or other critical functions.

Glossary of terms used in this policy

Control of personal information means that we have received the information (normally direct from the data subject) on the basis that, subject to our policy and the law and any privacy statement accepted by the data subject, we can process their personal information as we decide and without further reference to the data subject.

Data is information which is stored electronically or in our paper-based filing systems.

Data subjects include all living individuals about whom we hold personal information. A data subject need not be a UK national or resident.

Personal information means data relating to a living individual who can be identified from that data (or from that data plus other information in our possession). Personal information can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal) or a statement of intention.

Data controllers are the people or organisations which control and determine, subject to the permission given to them by the data subject or the law, how and why any personal information is processed.

Data users include all our staff whose work involves using personal information. Data users have to follow our data protection and security policies at all times.

Data processors include any person who processes personal information on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include volunteers or partners or suppliers who handle personal information on our behalf.

Privacy Statement means the document entitled 'Privacy Statement' which is available on our website at www. embaptists.co.uk/privacy

Processing is any activity that involves use of personal information. It includes obtaining, recording or holding the information, using it in any way such as organising, amending, retrieving, disclosing, erasing or destroying it. Processing also includes transferring personal information to third parties.

Sensitive personal information includes information about a person's nationality, racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. We will also treat financial information and payment card details as sensitive personal information. Sensitive personal information can only be processed under strict conditions.

We/us means the East Midlands Baptist Association, Registered Charity 1094457, a Company Limited By Guarantee, Registered in England and Wales 4302466 and East Midlands Baptist Trust Company Limited

You means each and every employee and other member of staff of East Midlands Baptist Association and East Midlands Baptist Trust Company Limited

July 2016