Detailed Practice Guidance on Data Protection (Revised January 2017)

1 Collecting personal information from individuals

When you collect personal information from an individual you should explain what you are going to do with the information, who we (EMBA) may give it to, and what they will do with it. This information is summarised in our Privacy Statement which is available on the EMBA website. (www.embaptists.co.uk/privacy)

Normally we will seek the implied consent of individuals to our privacy statement. Any form used to collect personal information should include a statement along these lines:

> *Unless you tell us otherwise we will use the personal information that you have provided to us, in accordance with our Data Protection Policy and our Privacy Statement. If we are unable to use your information it may affect our ability to work with you.*

If the personal information includes (or could include) sensitive personal information, you should normally seek the individual's explicit consent to processing this. You will need to obtain an indication from them that they agree to the following:

> *You agree that we will use the personal information that you have provided to us, in accordance with our Data Protection Policy and our Privacy Statement. If we are unable to use your information it may affect our ability to work with you.*

Before taking any photographs of video footage of individuals which will be used to by us in any way – for example in printed media or on our website – permission must be obtained. Sample permission forms are attached to these guidelines and are also available from the Data Protection Officer.

2 Obtaining personal information from someone else

When we obtain personal information from a source other than the data subject, we will expect the source to be able to demonstrate they have the authority to disclose that information.

3 Opinions and pastoral issues

When making written file notes or sending any internal communication that contains opinions about any person, make sure it is written in such a way that you would not be embarrassed if the person saw it. Opinions about a person constitute their personal data and they are entitled to see it on request. For more delicate situations consider whether a verbal conversation is more appropriate.

When dealing with pastoral complaints/issues that are not formal complaints, consider what third party details to include in your records. It may be appropriate to keep the record impersonal. Where the issues become recurrent or escalate and there is a need to be specific and rely on documentary evidence you should consider whether the purpose of the data processing is truly pastoral support (covered by the Privacy Statement) or part of conducting a formal Complaints Procedure.

4 Security

As an organisation we need to ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal information, and against the accidental loss of, or damage to, personal information. This applies from the point of collection to the point of destruction of the personal information.

Personal information may only be transferred to a third-party data processor if (s)he agrees to comply with those procedures and policies, or if (s)he also has adequate measures in place.

Maintaining information security means ensuring the confidentiality, integrity and controlled availability of the personal information, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal information should be accurate and suitable for the purpose for which it is processed.

Availability means that as appropriate we will restrict access to personal information held by us.

We will apply security procedures as a priority. In this Document they are marked *.

5 Premises entry controls *

We are aware that our premises must be kept reasonably secure to prevent unauthorised entry. As access to our premises is normally controlled and subject to permission, staff should ensure that security doors are kept shut at all times. Any stranger seen in the entry-controlled areas of our building should be signed in and wear a 'visitor' badge. If and when the security system is not working then staff must be extra vigilant about keeping personal information secure.

6 Secure lockable desks and cupboards *

Wherever possible (and particularly out of office hours) desks should be kept clear from personal information. Where such information is kept in areas that are not entry-controlled or outside of the office it should be kept on the person, in locked desks or cupboards or otherwise appropriately secured.

7 Information access controls *

We will restrict access to personal information so that only authorised data users who need access can access the information.

8 IT system access controls *

We will restrict access to our IT system as follows:

- All computers will be password protected.
- Personal information may not be stored on mobile devices unless the device is kept about your person or under lock and key at all times and the device is password or PIN protected. Laptops must be encrypted before confidential personal information is processed on them. Smart phones and other mobile devices must be equipped with a remote data destruction facility.

9 Remote working, home workers, travelling *

All portable devices (computers, mobile phones and memory sticks) and particularly paper files, paper documents and unencrypted devices must be kept secure at all times. So far as possible they must be kept about your person or in a bag which you attend at all times. Where you need to leave personal information unattended it must be kept under lock and key. If any such device is stolen or lost you must remotely wipe the data as soon as possible. Working from home must ensure the computer they are using has current firewall and anti-virus protection.

10 Eavesdropping *

Data users should ensure that when you are in public view your conversation, page or screen containing personal information does not show confidential information to passers-by. You must log off from your electronic devices and close and securely store paper documents when they are left unattended. If you are dealing with sensitive personal information please make sure your computer is locked when leaving your desk.

11 Transmission of personal information *

Personal information sent out by us must be transmitted by secure means. You should always take care to ensure the information is being sent to the correct address or email address.

When sending personal information by post or email you should carry out a risk-assessment of the potential harm to the data subject if the security of their information is breached. Informed by your risk assessment, you should consider the following options.

- Enclosing sensitive or confidential personal information in an attachment rather than in the body of an email
- Password-protecting any document containing confidential or sensitive personal information and communicate the password to the recipient(s) by other means. [Appendix 1 explains how to do this]
- Anonymising the personal information
- Using recorded delivery when sending information by post

We will encourage others from whom we receive personal information to adopt similar practices.

12 Personal use of information *

You may not use personal information that you obtain in the course of your work for any personal purposes unless you or we have the data subject's permission and can evidence it. You may not use any of your personal paper filing systems, other than those you have at our premises, to store or use anyone else's personal information. You may not use your personal email account to transmit personal information obtained in the course of your work.

13 Handling telephone calls *

13.1 Where appropriate, you should check a caller's identity to make sure that information is only given to a person who is entitled to it. If the caller's identity cannot be confirmed then you should ask them to put their request in writing. You must refer to the Data Protection Officer in difficult situations.

13.2 You should never leave a voicemail message which includes personal information. If you are unable to speak directly to the individual concerned leave a message asking them to return your call.

14 Methods of disposal *

Once personal information is no longer required for the purposes set out in our Privacy Statement it should be destroyed. Paper documents should be shredded. Floppy disks, CD-ROMs and other electronic storage media permanently cleaned of data or physically destroyed.

15 Accurate Information

We rely on individuals to keep us informed of changes in their information and our database should be updated promptly when we receive written notice of changes from individuals. Contact details should not normally be held separately from our main database. You must exercise caution before using information which is known to be old. You must mark information as out of date or not to be used if it is known to be incorrect.

16 Use of emails

All staff should take great care when using email communication. In particular:

- Emails sent to groups of people should normally be sent using BCC rather than CC. This is to ensure that individual email addresses are not being made available to the whole group.
- When forwarding an email, care should be taken that the person to whom the email is being forwarded has the right to see any personal information contained in any part of the email.
- When sending an email that contains opinions about any person, make sure that it is written in such a way that you would not be embarrassed if the person saw it. Opinions about a person constitute their personal data and they are entitled to see it on request.

17 Requests for personal information

A formal request from an individual (data subject) for their personal information that we hold about them must be made in writing. Before we comply with the request:

- A fee of £10 is payable by the individual for provision of this information.
- We must be satisfied that the person requesting the information is that individual or their lawfully and duly appointed representative with authority to receive the information.
- We will agree terms with the recipient regarding how the transmission of the personal information will be handled.

Personal information often includes references to people other than the data subject. When disclosing their personal information to the individual making the request we will not disclose, and will endeavour to conceal, the identities of other people and their personal information, unless we have their consent or some other lawful grounds to disclose. The same applies to confidential information, and to intellectual property which is owned by someone other than the data subject.

Any member of staff who receives a formal access request should inform the Data Protection Officer and/or their Team Leader immediately as we have to respond to such requests within forty days of their receipt.

18 When we may disclose information to someone else

Normally we will only disclose personal information to the individual to whom it relates.

We may disclose personal information to someone other than the data subject if all the following requirements are met:

- If our Privacy Statement says that we may disclose the information, or if the law permits or requires the information to be disclosed
- If we have followed the process for disclosure to someone other than the data subject (see section 19 below)

If you are unsure as to whether personal information can be disclosed in a specific case you should discuss this with your Team Leader and/or the Data Protection Officer.

19 Processes for disclosure to someone else

19.1 If the information is going to one of our agreed partners, in accordance with our Privacy Statement, then a Data Sharing Agreement needs to be in place before any sensitive information can be shared. The Data Protection Officer has a list of the partners where Data-Sharing agreements are in place.

19.2 Contact details of those people shown on our database as BUGB accredited ministers, BUGB accredited church workers or church secretaries can be given to church members and others who request this information. These should be on an individual basis. We do not provide lists or mailing labels for groups of such people other than the Church Directory which is issued to member churches.

19.3 If the information is going to someone who will process it on our instruction, for our purposes, a data processing agreement is required and a standard agreement document can be obtained from the Data Protection Officer. We will not disclose any personal information to a third-party data processor until the following requirements are met:

- We are reasonably satisfied that the recipient will hold the personal information we disclose to them in accordance with the law including the data protection principles, and to at least the standards set by our Data Protection Policy.
- We have agreed terms with the recipient regarding how the transmission of the personal information will be handled.

19.4 If the information is going to be sent to other organisations in relation to matters of accreditation or pastoral support, in accordance with our privacy statement, then only information that is clearly necessary for that purpose should be sent. Information should not be sent outside the European Economic Area without first obtaining the explicit consent of the individual to whom it relates.

19.5 If the information is to be shared with a minister (or one of the other Trustees) of a church, or with the Safeguarding Officer of another denomination, where there is deemed to be a risk of children, young people or vulnerable adults suffering significant harm, then this should only be done by the Safeguarding Officer who will have worked through the agreed procedures before making this disclosure.

19.6 Any request from a third party for personal information must be passed to your Team Leader or the Data Protection Officer as appropriate. This includes requests from a local authority, safeguarding board, regulators, government department or other public authority, police, fire service, health authority or medical practitioner in connection with crime prevention or detection, risk assessment, resolution of complaints or other issues,

19.7 Information about an individual should not be shared with someone who claims to represent them unless you are satisfied that the individual has appointed them to act on their behalf.

20 Responding to data subjects who exercise rights

Where we hold personal information of a data subject and have control of that information, if the data subject exercises any rights that are binding upon us in relation to the personal information we will respond reasonably promptly and in any case within the maximum time-limit that is set by law.

21 Complaints to the Information Commissioner's office

Any member of staff who becomes aware that an individual is intending to complain or has complained to the Information Commissioner's Office (ICO) about one of our organisations must inform their Team Leader and the Data Protection Officer as soon as possible

22 Revisions to Guidance Notes

From time to time the Data Protection Officer may issue revised Guidance Notes or supplements to these notes which staff should also comply with.

Appendix 1 – EMBA Data Processing Agreement

EAST MIDLANDS BAPTIST ASSOCIATION

Data Processor Agreement

(Name)	has been appointed by the Trustees/Directors of the above named organisation to act in the following role in a voluntary capacity

As part of this role they will need to process personal data for the sole purpose of

and therefore will need access to the National Baptist Database for the following reason(s)

Signed on behalf of the above named organisation

..... (Association Moderator or Regional Team Leader)

Date.....

1. The Data Processor agrees to ensure that any personal data given to them
   - will be held securely at all times and not made available to anyone else without the express permission of the Trustees/Directors
   - will be destroyed once it is no longer needed
   - will all be handed over to the Trustees/Directors on request.

2. The Data Processor acknowledges that they will process the data only according to the instructions provided by the Charity Trustees and that they must not process this data for their own purposes

3. The Data Processor agrees that they will only use the National Baptist Database for the purposes outlined above and not for any personal use and that they will not pass on their login details to anyone else.

4. The Data Processor understands that any electronic device used to store the personal data, or access the National Baptist Database, must be password or pin-protected and that appropriate firewall measures are in place

I agree to the above

Signed..... (Data Processor) Date.....