Annex 1

Data Retention Policy

We will hold information about people for the following periods (for administrative purposes we allow a maximum of 2 months beyond the end of the specified period for data to be securely and permanently deleted):

Member:	Names will be held permanently. Contact information will be held for 6 months after they have ceased to be a member.
Non-Member:	Until 6 months after they have ceased attending the church.
Under 18s in our church, children or youth ministry	The child of a member will be treated for Data Protection purposes only as a member by association until their 18th birthday after which they will be treated as a Member or non-member depending on whether they apply for membership. The child of a Non-Member will be treated as a Non-Member until their 18th birthday.
Employee	The current and previous six years for most information. Parental Leave records are held for 18 years after the birth of the child, application and interview notes for unsuccessful applicants are held for one year. If safeguarding issues are raised then records are retained for 75 years.
Those hiring our buildings	The current and previous six years
Contractors	The current and previous six years
Safeguarding	Our policy matches the BU guidelines. In summary records are held for 75 years after last contact with the person or their death. Risk assessments etc where there were no incidents or concerns raised are held for three years.
Minutes of meetings	These are held permanently, although 10 years after the date of the meeting they will be held in archive.

Because we allow the use of private IT equipment by data controllers there is a possibility that backups of otherwise deleted data will exist beyond the times specified in the retention policy.

For a volunteer organisation the size of Ebenezer Baptist Church there is currently no practicable and cost-effective way of ensuring such information does not exist in private backups.

We therefore require individual data controllers to be aware of the risks, to delete old backups on a reasonable schedule (for instance always keep only the last 3 backups or some other fixed number), and to ensure that if they do restore from backup then they delete any restored data in accordance with our retention policy if necessary.

Data Acquisition Procedures

All personal information will be collected on official Ebenezer Baptist Church forms issued for that purpose and every form will be accompanied by an appropriate Privacy Notice - in the case of web forms then links to appropriate Privacy Notices must reside beside the web form.

In the case of photographs then an official Ebenezer Baptist Church form must have been completed by each identifiable person and an appropriate Privacy Notice issued (note, if somebody has given consent for their photograph to be used already in the current consent period then fresh consent is not required).

No person acting on behalf of the church will collect information that they are not entitled to.

All forms shall be forwarded to the GDPR Administrator for collation and dissemination to the appropriate persons as detailed in our Information Audit unless otherwise specified in the Privacy Notice.

Information about under-18s will always require the signature or counter-signature of a parent or guardian.

Procedure for when somebody changes roles

Every member of the church will, over time, slowly collect information about those within the church that they become friends with. However when somebody takes on a leadership or co-ordinating role they main gain access to additional information about those people or may gain information about other people. Both of those sets of additional information came to them as a result of their role and must be securely and permanently deleted when they cease to carry out that role. This procedure describes how we propose to address that issue.

For those who are carrying out such a role when our GDPR compliant Data Protection Policy was adopted by the church then we require that when they cease the role they go through all places where they store information and either (a) gain the permission of the data subjects to retain the information they have or (b) delete the information. Such information may only be basic name and address records or it may extend to more information such as emails, pastoral notes, etc.

For those who take on such a role after the policy was adopted then our procedures require that they keep their personal records and church records separate in such a way that they can clearly identify which is which, and thus delete church records securely and permanently when they cease to carry out the role. Care must be taken, in the case of electronic records, with backups and ensuring that church records can be removed from backups at the appropriate point in time.

Procedure for death in service

When a data controller, that is somebody who processes data on behalf of Ebenezer Baptist Church, dies whilst in possession of data then we will make appropriate and proportionate efforts to secure and ultimately regain possession of (or securely delete) that data taking into account the pastoral needs of the relatives of the deceased and the sensitivity of the data that was in their possession.

As a minimum our first action upon learning of the death will be to alert the relatives of the deceased and/or their executor of the existence or suspected existence of data and ask them to ensure that the data is retained securely and not accessed until a trustee (or a duly appointed representative) has had opportunity to examine the data and recover or delete it.

Unless the data is of a particularly sensitive nature such examination and subsequent recovery or deletion would normally be delayed until some time after the funeral of the deceased.

Procedure for when somebody attains the age of 18

On the 18th birthday of somebody attending Ebenezer Baptist Church events or services the GDPR Administrator shall issue them with an appropriate Privacy Notice and, where necessary, issue them with an appropriate form to capture their personal data.

Procedure for holding data

Master copies of all Ebenezer Baptist Church data will be held by our GDPR Administrator except for:

- Pastoral information which will be held by the Minister
- Financial information which will be held by the Treasurer
- Safeguarding information which will be held by the Safeguarding Trustee
- Group specific information will be held by the persons cited in the relevant privacy notice

When a data controller receives new or updated data for a data subject then they will immediately forward it to the person holding the Master copy of that data. The person holding the Master copy will then notify all other affected data controllers of the new or updated data. Each data controller is responsible for ensuring that they update all their records upon receipt of new or updated data.

Policy for use of personal devices by data controllers

The decision as to whether or not to use a personal device for processing Ebenezer Baptist Church data is a matter for each individual data controller. However if a data controller decides to use a personal device then they must abide by the following as a minimum:

- Up to date antivirus software must be installed and enabled at all times where such software is available
- All data must be password protected by a password known only to the data controller (this includes backups which must also be password protected)
- The data must be held in a way where it is easily separated from personal data such that it can be easily identified, and be able to be securely and permanently deleted (including from backups)

If a data controller is allowed by their employer to use an employer supplied device for Ebenezer Baptist Church data then the data controller must ensure that the foregoing are abided by, particularly considering employer backups and maintenance by the employer's IT provider.

Policy for use of email

All data controllers must only send and receive email using an @rockofhelp.org.uk email address. Email must be stored in separate folders from personal email to ensure that it can be easily identified and if necessary securely and permanently deleted.

Sharing information verbally

When data controllers share information verbally, for instance prayer requests, they must consider the physical environment in which they are sharing that information and the possibility of somebody overhearing their conversation. This includes in church. It is the responsibility of each data controller to ensure that they do not reveal data to unauthorised persons.

Prayer chain

Ebenezer Baptist Church operates a "Prayer Chain" which allows people to ask a group of designated church members (prayer chain team) to pray for them or others. The Prayer Chain operates by contacting the Prayer Chain Co-ordinator with a prayer request and the Prayer Chain Co-ordinator will propagate that prayer request to the prayer chain team.

The Prayer Chain Co-ordinator is responsible for ensuring that all propagated prayer requests have the explicit consent of all identifiable persons in the request (such consent can be gained verbally and the person submitting the prayer request will be trusted to pass on consent from third-parties that they have named).

All prayer chain team members will keep prayer requests confidential, and will delete them once they have determined that they will no longer be praying for them.