

Hook Norton Baptist Church Data Protection Policy

1. Definitions

Personal Data: Information about a living individual which is capable of identifying that individual e.g. names, email addresses, photos.

Processing: Anything done with or to the personal data including storing it.

Data Subject: The person about whom the personal data is processed.

Data Controller: The person or organisation who determines the how and what of data processing at Hook Norton Baptist Church. This is the Trustees and Leadership Team. The Data Controller delegates day to day administration of GDPR obligations to the Church Secretary acting as **Data Protection Officer**, currently this is Nigel Whitehead.

2. Background & Scope

Background

The General Data Protection Regulation (GDPR) came into force on 25th May 2018, replacing the Data Protection Act 1998 and provides individuals with greater rights and protection regarding how their personal data is used by organisations.

Churches must comply with its requirements.

Scope

Hook Norton Baptist Church recognises the importance of correct and lawful treatment of personal information its processes and holds whether on paper, on computer or any other media. The church fully recognises, endorses and adheres to the fundamental principles of GDPR although at this stage does not consider registration with the Information Commissioner's Office necessary due to the limited nature of the church's legitimate data processing interest.

3. Underlying Principles of GDPR as applied to Hook Norton Baptist Church

All personal data shall:

- Be processed fairly, lawfully and transparently based on the legitimate interest of the church in the efficient administration of its general membership, activity groups, associated rotas and those linked to the church through its various services, events and activities.
- Be obtained for the lawful specified purpose above and not processed in any manner incompatible with that purpose.

- Be relevant, adequate and not excessive in relation to the purposes.
- Be accurate and where necessary kept up to date and maintained only for as long as is necessary.
- Be kept secure from unauthorised and unlawful processing protected against accidental loss, destruction or damage.
- Be processed in accordance with the data subject's rights, specified below.

4. Rights of the Individual Data Subjects.

The rights of individuals under GDPR are as follows;

- The right to be informed that personal information will be processed fairly and in accordance with the specified purpose and legitimate interest of the church. This right will be expressed in a Privacy Notice made available in the Church Office.
- The right to have access to a data subject's personal information which is held by the church in order to verify the lawfulness of use and its accuracy. Such access to be made available within 28 days of any such request to the Data Controller.
- The right to have their personal data corrected or rectified if it is inaccurate or incomplete. Any third parties to whom the data has been given must be informed of the correction. Data subjects must also be informed of third parties to whom the personal information has been supplied (if any).
- The right to request the deletion or removal of personal data where there is no compelling reason for its continued processing or retention by the church.
- The right to restrict the processing of personal data in circumstances where they may consider the processing to be unlawful or the data to be inaccurate.
- The right to move, copy or transfer personal data easily from one IT system to another. This right is unlikely to impact the way in which the church holds and processes an individual's personal data.
- The right to object to processing data in circumstances where the individual is not happy that the church has the right to process that data.
- The right to be protected against the risk that data is processed automatically resulting personal profiling by a third party agency.
- Personal data relating to children under the age of 13 must be subject to parental or guardian consent.

5. Complaint by a Data Subject

Where a data subject believes that their rights under GDPR have been infringed by the church, they should in the first instance notify the Data Controller within 28 days of becoming aware of the potential infringement.

Notification should be in writing to the Church Secretary (as Data Controller) who will bring the matter to the attention of the Data Controller at the next available meeting.

A response to the complainant will be made in writing on behalf of the Data Controller within 14 days of the meeting.

Should the complainant be unsatisfied with the response of the Data Controller, they have the right to notify the Information Commissioner's Office within a further 14 days.

6. Data Protection Impact Assessments.

In the event that the church proposes to embark on a project which will require the processing of sensitive personal data on a large scale (e.g. fund raising for a legitimate purpose) a data protection impact assessment (DPIA) should be carried out by the Data Controller.

The DPIA will include:

- A description of the project
- A Description of the processing activities and their purpose
- An assessment of the need for the processing and its proportionality
- Any risks which may arise from the processing and steps to be taken to mitigate the risks.

7. Data Breach

A personal data breach is one which results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. Under GDPR notification of a breach is mandatory.

All such breaches should be notified by the Data Controller to the Information Commissioner's Office within 72 hours of identifying the breach

8. Policy Review

This policy and its implementation will be reviewed annually and a report produced for the church Annual General Meeting.

January 2019