The Parish Church of St. John the Evangelist and Clayton Brook Community Church in the Church of England Diocese of Blackburn

Data Protection Policy

September 2018

1. Introduction

The PCC of St Johns and Clayton Brook recognises the importance of the correct and lawful treatment of personal data. All personal data, however held, will be subject to the appropriate legal safeguards as specified in the **General Data Protection Regulations (GDPR) (May 2018)** which supersedes the Data Protection Act. The key changes made strengthen the rights of individuals and increase the obligations on organisations for the protection of personal information and data. St Johns and Clayton Brook retains personal data about individuals, living, and recently departed, within the Parish for the purpose of pastoral care and communication.

2. Scope

This policy covers all living members and recently departed. within the Parish, all clergy, staff, members, organisations and individuals hiring church premises and anyone visiting the churches.

3. Roles and Responsibilities

- The Parochial Church Council (PCC) has overall responsibility for policy implementation
- Day to day responsibility for implementing this policy is delegated to the clergy, Church Wardens and PCC Secretary.

4. Policy Statement

St Johns and Clayton Brook churches fully endorse and adhere to the eight principles of GDPR. These are:

- Lawfulness, fairness and transparency
- Purpose limitation – information collected and held will only be for the purpose specified
- Data minimisation – only data required for the purpose specified will be collected
- Accuracy – data held will be kept up to date
- Storage limitation – information will only be kept as long as is necessary
- Integrity and confidentiality – information will be kept safe and secure and
- Accountability - the PCC will ensure compliance with the above principles

The PCC will continue to follow 8 key steps

1. **Review all personal data held.**
   The PCC will keep under review what information is collected, why, how it is stored and who has access to it.
2. **Agree a policy for the length of retention for information**
   Personal data will be erased when it is no longer required, if the data subject (individual whose information is stored) withdraws consent or there is no longer a legal reason foe holding the information.
   There may be legal exceptions for non-compliance with a removal request e.g. safeguarding concerns.
3. **Agree a policy for the security of information and data stored**
   All data held on computers must be password protected and if shared with other PCC members preferably encrypted. Paper records should be stored in a safe or lockable drawer.
4. **Understand legitimate interest**
   Personal information and data can be processed without consent if the PCC believes it has a genuine and legitimate reason for doing so unless outweighed by the potential harm to the individuals rights and interests. An assessment as to whether a legitimate interest can be relied upon will be carried out on a case by case basis.

Legitimate interest may include:

- For the performance of a contract
- In compliance with a legal obligation
- To protect the interest of the data subject or another individual
- For the purpose of legitimate interests the PCC is pursuing

The PCC recognise the eight rights of an individual in drafting this policy viz:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object and
- Rights in relation to automated decision making and profiling

5. **Consent**
   When we hold a person's individual details, protecting those details is of paramount importance and the consent form will make it clear what the data will be used for, how it will be stored and for how long it will be held. The consent form will be clear as to how information collected will be used. If there are changes a further consent form will be required.

6. **Third Party Risk**
   If any data or information is shared with individuals or organisations outside the PCC written confirmation will be required from those individuals/organisations that they comply with GDPR.

7. **Subject Access Requests (SAR)**
   If an SAR is valid and permissible the information held on that individual will be supplied within one month from the receipt of the request. A charge may be made for processing the request.

8. **What to do if a breach is identified**
   "A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data transmitted, stored or otherwise processed."

   If data is breached and we believe the information could cause material or emotional harm to an individual the PCC will report the breach to the Information Commissioner within 72 hours of the breach becoming known. We will also inform the data subject of the breach unless we are restricted from doing so by legal requirements.

   Note: If the data breached is encrypted the PCC may decide not to declare the breach.

5. Policy Guidance

This policy should be read in conjunction with the Parish Safeguarding Policy

6. Review of this Policy

The policy will be reviewed every three years unless there is a subsequent change in the law or regulations pertaining to data protection.

7. Contacts

Rev Philip Venables
Lyndom Wright – Church Warden
Gill Menhennet - Church Warden
David Barlow - PCC Secretary

8. Authorised

Signed:

Rev. P Venables (Incumbent) …….

L Wright (Churchwarden) …….

G Menhennet (Churchwarden)……#

September 2018