Chorley Parish Church of St. Laurence
in the Church of England Diocese of Blackburn

Data Protection Policy

Issue 2 July 2020

Address: *Parish Office St Laurence's Church, Union Street, Chorley, PR7 1EB*
Email: *office@stlaurencechorley.co.uk*
Phone: *01257 231360*
Registered Charity Number: *1175130*

1. Introduction

The Parish of St Laurence recognises the importance of the correct and lawful treatment of personal data. All personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the new **General Data Protection Regulation**, which supersedes the Data Protection Act on 25th May 2018. The key changes from the current law are to strengthen rights of individuals and place more obligations on organisations in looking after personal data. The Parish of St Laurence uses personal data about living individuals, 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, of Chorley Parish Church of St. Laurence, all Clergy, administrative staff, organisations/individuals hiring and/or anyone visiting the church premises.

3. Roles and responsibilities

Overall and final responsibility for policy implementation	*Chorley Parish Church of St. Laurence Parochial Church Council*
Day-to-day responsibility for ensuring this policy is put into practice is delegated to:	*The Parish Administrator, Sunday School Leader, The Rector and Church Wardens*

4. Policy Statement

St Laurence's Church fully endorses and adheres to the eight principles of GDPR These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for St Laurence's Church must adhere to these principals.

- **Lawfulness, fairness and transparency** – as with Data Protection
- **Purpose limitation** – only collect for specific purposes and then don't use it for other purposes
- **Data minimisation** – only collect the data you need for the purpose you are using it
- **Accuracy** – as now, keep it up to date!
- **Storage limitation** – don't keep it for longer than you need to fulfil the purpose
- **Integrity and confidentiality** – keep it safe and secure e.g. encrypted if on a laptop or mobile phone.

- **Accountability** – you must be able to prove you have complied with the above.

There are 8 key steps that need to be in place

1.Review all the personal data we hold

- What data do we hold?
- Why do we hold it?
- Who has access to the data?
- How is the data secured?

2. A clear policy for the retention of data is essential

- personal data must be erased, without delay when:
  - it is no longer necessary for purpose
  - the data subject withdraws consent
  - there is no longer any legal grounds to hold or process that data

- Data cannot be kept indefinitely and must be removed, when asked by the data subject.
- Exceptions to this removal request
  - For vital interests or public interest
  - Archiving in relation to public interest, scientific/historic and statistical research
  - Exercise of legal claims

Do the policies need to be amended to comply with GDPR?

3. Where data is held.

- All data stored on computers or in paper form is password encrypted or stored in lockable drawers or the safe.
- We will only collect the data we need and keep it only as long as needed in order to fulfil an agreed purpose and then delete it.

4. Understand Legitimate Interest

- We can process personal data without consent if we have a **genuine and legitimate** reason **unless this is outweighed** by the harm to the individual's rights and interest
- An assessment of whether legitimate interests conditions can be relied upon must be carried out on a **case by case** basis
- The legitimate interest condition is **necessity based**

We would have legitimate interest and be able to process personal data **without** consent where it is necessary:

- For the performance of a contract
- For compliance with a legal obligation
- To protect the vital interests of the data subject or another person
- In the exercise of official authority or in the public interest

  - For the purposes of legitimate interests you are undertaking

- ONLY if NONE of the above apply do you need consent.

5. Consent

- GDPR means that when we do hold individual's personal details, protecting these details is paramount and the consent form must make clear **what the data will be used** for and for **how long.**

PCCs cannot collect data from parishioners to inform them about services and then use that data to fundraise.

- PCCs cannot profile certain people to target for fundraising.
- If you wish to use the personal information to contact individuals on fundraising the wording on the consent form must make this clear.
- Information obtained from the Electoral Roll cannot be used to direct mail individuals about events taking place unless you have explained this is what the information will also be used for and have the individuals explicit consent to contact them.
- Personal data given for baptism, weddings and funerals cannot be used to mail individuals about services in the year unless the consent form makes it clear.

6. Third Party Risk

Is data shared with people/ organisations outside of your PCC

  - i.e. IT databases, IT systems.

We have obtained written confirmation that third party companies comply with the new GDPR rules.

7. Subject Access Requests (SAR)

If the SAR request is valid and permissible the data we hold on that individual has to be supplied within 30 days of the request. This will involve a charge.

8. What to do if we identify a breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- If data is breached and the data breached could cause material or emotional harm to the individual we have just 72 hours to declare it to the ICO (Information Commissioners Office)
- If severe then the breach must also be declared to the data subject.
- We need to do this from the point that you are aware.

Note: If the data is breached but is encrypted, i.e. it cannot be accessed by anyone and therefore will not cause harm we do NOT need to declare the breach.

Fines
The fines that can be imposed due to non-compliance depend on the severity of non-compliance.

There are eight rights of Data Subjects

(Data subject is the individual whose personal data is held).

- 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
- Rights in relation to automated decision making and profiling

5. Policy Guidance

This policy is to be read in conjunction with:

- *Chorley Parish Church of St Laurence safeguarding Policy*
- *Chorley Parish Church of St Laurence E Policy*

6. Emergency contacts

If there is an intruder or you are threatened dial 999, give the address of the Church:

St Laurence's Church, Union Street, Chorley, PR7 1EB

Contact the key holders as follows:

Warden:	Bernard Oakley	01254 831693
Rector:	Fr. Neil Kelley	01257 266037

7. Review and monitoring of this policy

This policy will be reviewed, monitored and revised every 18 months (or sooner if church activities change significantly or legislation changes) and will be approved by the PCC and adopted by the Church Meeting after such changes.

8. Further information

For further information please contact:

Rector:	Fr. Neil Kelley	01257 266037
Warden:	Bernard Oakley	01254 831693

9. Authorised

Signed:

Name: Fr. Neil Kelley **Date:**
Position: Rector

Signed:

Name: **Date:**
Position: Church Warden

Version History					
Version	**Date**	**Detail**	**Author**	**Approved**	**Date**
1.0	10/05/2018	New policy	K Chandler		
2.0	15/07/2020	Updated contact details	J Gemson		