

# ST CUTHBERT'S – ALLENDALE DATA PROTECTION POLICY



*First Issued : March 2017      Last Reviewed      : July 2017*

## Contents

Introduction to Data Protection.....	3
Definition of Terms.....	3
Data Protection Policy .....	4
Satisfaction of Principles .....	4
Data Protection Monitor .....	5
Status of the Policy .....	5
Subject Access to Information .....	5
Information we need not provide.....	6
Keeping Other People’s Information Confidential .....	6
Rights in Relation to Records .....	6
Incumbent, Church Warden or PCC members Rights in Relation to Their Records .....	6
Incumbent, Church Wardens and PCC Members Responsibilities .....	7
Data Security.....	7
Working from Home.....	7
Monitoring of Projects .....	8
Rights to Access Information.....	8
Publication of Information.....	8
Retention of Data .....	9
Compliance .....	9
Supporting Material .....	9
Useful Links.....	9

## Introduction to Data Protection

St Cuthbert's is required to maintain personal data about living individuals for the purposes of satisfying operational and legal obligations. We recognise the importance of correct and lawful treatment of personal data; it maintains confidence in the organisation and provides for successful operations.

Personal data that we require includes information about:

- Current, past and prospective church members.
- Users of our church.
- Suppliers.
- Others with whom we communicate.

This personal data whether held on paper, computers or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998.

We fully endorse and adhere to the principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. The incumbent, church wardens, PCC members and any others who obtain, handle, process, transport and store personal data for our organisation must adhere to these principles.

## Definition of Terms

### **'Other Data Subjects' and 'Third Parties'**

These terms may include contractors, suppliers, contacts, referees, friends or family members.

### **Personal Data**

Personal data is data which relates to a living individual who can be identified;

- From that data.
- From that data and other information which is in the possession of, or is likely to come into the possession of the holder of the data.

Sensitive personal data concerns the subject's race, ethnicity, politics, religion, trade union status, health, sex life or criminal record.

### **Processing**

Processing refers to any action involving personal data including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying.

### **Unlawful Obtaining of Personal Data**

This term refers to the offence committed when people use unlawful means such as hacking, theft and impersonation to obtain unauthorised access to personal data.

### **Information Commissioner's Office (ICO) Register of Data Controllers**

The Information Commissioner's Office maintains a public register of people that are responsible for complying with and overseeing data protection in an organisation. These people are known as data controllers. Each register entry includes the name and address of the data controller and details about the types of personal information they process.

The Data Protection Act 1998 requires every data controller who is processing personal information in an automated form to register and thereby notify the ICO, unless they are exempt. Failure to notify is a criminal offence and register entries have to be renewed annually.

## Data Protection Policy

### Principles of the Data Protection Act 1998

The principles require that personal data shall:

1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. Be adequate, relevant and not excessive for those purposes.
4. Be accurate and where necessary, kept up to date.
5. Not be kept for longer than is necessary for its purpose.
6. Be processed in accordance with the data subject's rights.
7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures.
8. Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

### Satisfaction of Principles

In order to meet the requirements of the principles we will:

1. Adopt a Data Protection policy (this document is our policy.)
2. Observe fully the conditions regarding the fair collection and use of personal data.
3. Meet our obligations to specify the purposes for which personal data is used.
4. Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements.
5. Ensure the quality of personal data used.
6. Apply strict checks to determine the length of time personal data is held.
7. Ensure that the rights of individuals about whom personal data is held, can be fully exercised under the Act.
8. Take the appropriate technical and organisational security measures to safeguard personal data.

9. Put in place controls on access to information (password protection on files and IT equipment capable of accessing personal data).
10. Take measures to control physical security (personal data should be kept in a locked filing cabinet).
11. Train the incumbent, church wardens, PCC members and any others on security systems and procedures.
12. Detect and investigate breaches of security to the best of our ability should they occur.
13. Ensure that personal data is not transferred abroad without suitable safeguards.
14. Establish a continuity/disaster recovery plan.

## Data Protection Monitor

Everyone within our organisation has a responsibility to be aware of Data Protection issues. However, it is important to have one person on the PCC who has agreed to monitor Data Protection. This person is responsible for ensuring;

- That the policies are up to date.
- That incumbent, church wardens, PCC members and any others are aware of the policy and have read and understood it.

The Data Protection Monitor is:

Mr Chris Welch

PCC Treasurer

Chriswelch1@btinternet.com

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Monitor.

## Status of the Policy

This policy has been approved by our PCC and any breach will be taken seriously and may result in formal action. Any incumbent, church wardens, PCC members and any others who consider that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Protection Monitor in the first instance.

## Subject Access to Information

All individuals who are the subject of personal data held by our organisation are entitled to:

- Ask what information the organisation holds about them and why.
- Ask how to gain access to that information.
- Be informed on how to keep it up to date.
- Be informed of what the organisation is doing to comply with its obligations under the Data Protection Act 1998.

## Information we need not provide

Individuals who are the subject of personal data held by our organisation are not entitled to request under subject access requests;

- Information held for management planning, (example. plans to invite someone to become a member of the church/PCC etc)
- Information as to the organisations intentions in respect of negotiations with the requester.
- References the organisation has given about the worker in confidence.
- Information about the prevention or detection of a crime, or the arrest or prosecution of offenders.
- Information that may identify someone else including the identity of a confidential complainant against the subject.

Personal data which is normally held for less than 40 days may be legitimately denied in subject access requests. This is due to the time limit data controllers must meet in making their response. If the data has been deleted by the normal procedures of the organisation by the time the data controller responds to a request, that data cannot be supplied.

## Keeping Other People's Information Confidential

When providing data we must make sure that we don't violate anyone else's data protection rights. For example, if we receive a complaint about an incumbent, church warden or PCC member and that incumbent, church warden or PCC member then requests access to their file, this could lead to the complainant being identified.

To avoid this we will obscure the name of the complainant in the original document before copying it and handing the copy over. In some cases the contents of a document may still identify the writer so it may be necessary to obscure other parts of the document or withhold it altogether.

## Rights in Relation to Records

Individuals who are the subject of personal data held by the organisation are entitled to:

- View the data we hold on them, for a small fee, known as 'subject access fee.
- Have inaccurate personal data corrected.
- Compensation for damage suffered as a result of a breach of the Data Protection Act 1998.
- Prevent processing likely to cause substantial damage or substantial distress.
- Request that their data is not used for marketing purposes.
- Request that their data is not transferred to any third party.

## Incumbent, Church Warden or PCC Members' Rights in Relation to Their Records

The Incumbent, church wardens or PCC members are entitled to know the logic behind any automated decisions taken about them. Some fully automated decisions are exempt from these provisions. These are where the decision is;

- Taken in relation to entering or carrying out a contract.
- Authorised or required by an Act of Parliament.
- The result of a granting of a request the incumbent, church wardens and PCC members has made.

If an employee ( eg Cleaner) has reasonable grounds to believe the organisation has not paid them the National Minimum Wage, they have the right to see their pay records. To do this they must make a written request, on receipt we will produce the records within 14 days.

## Incumbent, Church Wardens and PCC Members' Responsibilities

All incumbent, church wardens PCC members and employees are responsible for:

1. Checking that any personal data they provide to the organisation is accurate and up to date.
2. Informing the organisation of any changes to information which they have provided, for example change of address.
3. Checking any information that we may send out and informing the organisation of any errors or where appropriate, procedures for up-dating entries.
4. Notifying all data subjects of the types of data held and the reasons why they are processed.

When incumbent, church wardens, PCC members supervise volunteers to undertake work which involves the processing of personal data, they must ensure that those volunteers are aware of the Data Protection Principles, in particular, the requirement to obtain the data subject's consent where appropriate.

If, as part of their responsibilities, incumbent, church wardens and PCC members collect information about other people they must comply with the Policy and with the Data Protection Procedures which are contained in the Data Protection Act 1998.

## Data Security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All incumbent, church wardens, PCC members are responsible for ensuring that;

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

## Working from Home

The organisation recognises that work is done at home by the incumbent, church wardens, PCC members. Everyone that works from home should;

- Attempt to keep information located at home up to date.
- Remove information from home computers when it's no longer needed at home.
- Ensure laptops or home computers have adequate and up to date anti-virus and security protection.
- Do their best to keep work taken home secure and to return all work related material upon completion.
- Inform the organization if information has been compromised.

## Monitoring of Projects

Project monitoring often requires incumbent, church wardens, PCC members and any others to request and hold personal data. In this case we will;

- Ask permission to utilise a person's data before collecting.
- Not keep more personal data than monitoring the project requires.
- Gain permission before publishing volunteer or beneficiaries details.
- Keep personal data only as long as necessary under monitoring and funding requirements.

## Rights to Access Information

Incumbent, church wardens and PCC members and other subjects of personal data held by St Cuthbert's have the right to access any personal data that is being kept about them on computer and to access paper-based data held in certain manual filing systems. This right is subject to certain exemptions which are set out in the Data Protection Act 1998. Any person who wishes to exercise this right should make the request in writing to the Data Protection Monitor.

We reserve the right to charge the maximum fee payable for each subject access request. This fee is reached by calculating the cost of assembling the information to the organisation. We reserve the right to ask for evidence in order to prove the requesters identity and for information we may need to find the requested data. If personal details are inaccurate, they can be amended upon request.

We aim to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a completed written request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

## Publication of Information

Information that is already published in the public domain is exempt from the Data Protection 1998 Act. This would include for example, information on incumbent, church wardens, PCC members and any others contained within externally circulated publications such as Diocesan reports and websites etc. Any individual who has good reason for wishing details in such publications to remain confidential should contact the Data Protection Monitor.



## Retention of Data

We will keep some forms of information for longer than others. All incumbent, church wardens, PCC members are responsible for ensuring that information is not kept for longer than necessary.

## Compliance

Compliance with the Data Protection Act 1998 is the responsibility of all incumbent, church wardens, and PCC members. Any deliberate or reckless breach of this policy may lead to disciplinary action and where appropriate, legal proceedings. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Monitor.

## Supporting Material

The Data Protection Act 1998 supports this policy. This document can be obtained free of charge from [Legislation.gov.uk](http://Legislation.gov.uk).

## Useful Links

### **Information Commissioner's Office**

Tel: 0303 123 1113

The Information Commissioner's Office's mission is to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

[www.ico.gov.uk](http://www.ico.gov.uk)

### **Direct Gov**

This website provides advice regarding collecting and protecting personal data.

[www.direct.gov.uk](http://www.direct.gov.uk)

### **Legislation Gov**

This site allows the public to view and download copies of all legislation in one central place. It also gives information on upcoming changes to individual pieces of legislation.

[www.legislation.gov.uk](http://www.legislation.gov.uk)

**Policy Adopted on Behalf of St Cuthbert's at PCC Meeting on 10<sup>th</sup> July 2017**