UK GDPR and DATA PROTECTION POLICY

The CHURCH OF ENGLAND

The Diocese of Peterborough

Whitefriars Church,
Boughton Drive,
Rushden, NN10 9HX

THIS POLICY was first produced in March 2023.

This policy will be reviewed every three years (unless there is a change to the law). It will be reviewed again in March 2026.

Signed: *MDHunter*

Office: PCC Secretary

Whitefriars Church and PCC are committed to protecting all information that we handle about people we support and work with, and to respecting people's rights around how their information is handled. This policy explains our responsibilities and how we meet them.

Contents:

UK GDPR and DATA PROTECTION POLICY

The Purpose of This Policy

Policy Statement

Whitefriars Church (the church) is committed to protecting personal data and respecting the rights of our church members (data subjects) and the people whose personal data we collect and use.

The church processes personal data to help:

a) maintain a list of church members
b) maintain lists of the groups within the church to which members belong or have a connection
c) provide pastoral support for members and others with connection to the church
d) provide a vehicle for regular and appropriate contact
e) respond effectively to enquirers and handle complaints

Why is this Policy important?

We are committed to ensuring that personal data are protected from misuse, being wrongfully accessed through poor security and being inaccurate, as we are aware that people can be upset or harmed if any of these things happen.

This policy sets out the processes of the church to ensure we comply with the relevant legislation

In particular, we make sure that personal data are:

a) processed lawfully, fairly and in a transparent manner
b) processed for specified, explicit and legitimate purposes and not in any way that is incompatible with those purposes
c) adequate, relevant and limited to what is necessary for the workings of the church
d) accurate and up-to-date
e) not kept longer than is necessary for the purposes for which it is processed
f) processed in a secure manner
g) processed in keeping with the rights of the data subjects

How does this Policy apply to you and what do you need to know?

Whatever your position with the church (leader, employee, trustee, group leader, member, etc.), you are required to ensure that any processes that involve personal data are carried out in compliance with this policy.

If you think that you have accidentally breached the policy, it is important that you contact the Data Protection Officer of the church immediately (and within 72 hours maximum) so that the impact of the breach can be limited as far as possible.

The church has undertaken to use ChurchSuite (data processor/controller) to process the personal data of members of the church. They guarantee to do this in a secure manner, having in place technical and organisational measures to ensure this security. By using this facility, church members, by invitation, upload to their area of ChurchSuite a minimum of their name and email address, along with any other personal details that they wish to include, and they can choose what additional information is visible to others. No-one else can see your personal information apart from your name unless you choose to make this visible.

The church has a Data Protection Officer (DPO) who is responsible for advising the staff and PCC about their legal obligations under data protection law, monitoring compliance and dealing with data breaches. The DPO is Melvyn Hunter who can be contacted in writing at c/o Whitefriars Church, Boughton Drive, Rushden, NN10 9HX or by email on melvyndhunter@gmail.com: there are also more details on the church web-site at https://www.whitefriarschurch.org.uk/safeguarding

The only personal data that will be requested and retained by the church in paper format is for those who are employed by the church. Such information will be required in line with safer recruiting guidelines and in relation to the position applied for. Such information will be kept secure in a locked cabinet while it is 'live' and will be destroyed by cross-shredding once it has expired.

Training and Guidance

Training for all staff and trustees is provided (annually) to raise awareness of their responsibilities and obligations. Annual updates will be included with safeguarding training.

The Data Protection Responsibilities of the Church and PCC

What personal data do we process?

For church members, sufficient personal information is requested to enable communication with members about services and upcoming events. Links to church groups can also be added to individuals so that they can receive details specific to those groups. Church members are at liberty to include any other personal details they wish.

For employees of the church, additional personal information is required, firstly to process their job application, and so possibly including education, previous employment, work references, other relevant details and possibly photographs. Such information will be kept securely and will be shared only with those who are immediately involved in the job interview panel. All paperwork relating to unsuccessful candidates will be destroyed by cross-shredding. Paperwork for employees is retained securely by the church.

In some cases, it is necessary for the church to store 'Special Categories' of information. The only special categories that are retained by the church at present relate to safeguarding issues. Such information is available only to the incumbent and the parish safeguarding team and is processed under Article 6 (i) (f) UK GDPR or under Schedule 1 Part 2 Data Protection Act 2018 conditions 10, 11, 12, 18 and 19. At present, no special categories relating to ethnic origin, political inclination, philosophical beliefs, trade union membership, health, sexual orientation, genetic data or criminal proceedings (except where there is a clear lawful basis to process this) are stored. Any processing of information relating to criminal conviction will be carried out with advice from the Diocesan Safeguarding Advisor and team.

Many church members contribute financially to the church. Management of this has been placed with the Parish Giving Scheme, and it is responsible for the secure keeping and processing of bank details.

How do we ensure this processing is lawful and fair?

Processing of personal data is lawful and fair when the purpose for the processing meets a legal basis and the processing is transparent. Church members are able to request an explanation as to how and why their personal data are processed as well as how and when such data are obtained.

Processing personal data is only lawful if at least one of the following legal conditions is met (see Article 6 UK GDPR):

a) processing is necessary for a contract with the person (such contract is made when church members subscribe to ChurchSuite: employees of the church have separate paper contracts)
b) processing is required for the church to comply with a legal obligation
c) processing is required to protect the vital interests of the individual
d) processing is required for the church to perform a task in the public interest and there is a clear interest in law for this

e) the processing is necessary for the legitimate interests pursued by the church unless these are overridden by the interests, rights and freedoms of the individual

For any other legal condition, consent must be obtained for processing to be lawful.

If processing of 'Special Categories' of information is necessary, the church must refer to Article 9 UK GDPR for guidelines of how this must be done to be lawful. It may be that legal advice should also be sought.

ChurchSuite provides church members with how their personal data are managed and processed.

The church also has a Privacy Notice (available on the church web-site).

If any processing of personal data is required that is not contained within the privacy notice, then written consent must be obtained before such processing is carried out.

Church members must also be informed if personal data relating to them has been obtained from another source (the usual reason for this is the obtaining of references for those applying to work for the church, or references for those seeking a DBS clearance with the church).

How and when do we need consent to process this data?

Subscribing to ChurchSuite includes the giving of consent for the church to process personal data in line with the normal day-to-day working of the church. Consent for any other form of processing must be obtained in writing. Such consent can be withdrawn again by the individual and any processing relating to that consent must stop at that point.

Processing for specific purposes

All processing purposes are explained in the Privacy Notice available on the church web-site.

Ensuring that data are adequate, relevant and not excessive

The church will collect only personal data that is needed for the specific purposed of the running of the church. This normally includes just the name and email address of the church member. Any additional information provided through ChurchSuite is at the behest of the individual.

Ensuring accuracy of data stored

Only individual members can access their personal data on ChurchSuite, though permission may be given by the individual to a ChurchSuite manager to do this. Individual members are, therefore, able to maintain the accuracy of the data stored about them.

Keeping data and destroying data

Personal data are not kept for longer than is required. Individual members can, at any time, make their details 'invisible' on ChurchSuite and can request that their information be removed. This will usually be done within five working days of such a request.

For those whose data are stored in paper format (i.e. employees), such data will be destroyed by cross-shredding once employment has ended. Minimal details may be retained so that relevant information can be passed on to future employers. Employees will be notified as to what data are retained.

Security of data

ChurchSuite guarantees the security of personal data stored by them and that such data cannot be accessed unlawfully. The measures in place include:

a) technical systems security
b) restriction of access to data
c) measures to ensure that data remain available and can be easily restored in the case of incident
d) physical security of premises
e) organisational measures
f) regular testing and evaluating of effectiveness of security systems

Paper format personal data are stored securely in a manner that protects against unlawful access and/or processing, accidental loss or theft, destruction or damage.

Keeping records of our data processing

Individual members who have subscribed to ChurchSuite can see within their area of ChurchSuite what communications have been made. Data managers can also see a list of all the changes that have been made as a time-line.

Working with people about whom we process data (Data Subjects)

Data subjects' rights

Much of what follows refers primarily to employees of the church. This is because individual members can access their data on ChurchSuite and make changes themselves.

The data subject has the right to:

a) make a Subject Access Request (SAR) (i.e. ask for access to their own personal data held by the church)
b) ask for inaccurate data to be corrected
c) restrict processing in certain circumstances
d) object to processing in certain circumstances including preventing direct marketing
e) data portability (i.e. receive their data or some of their data in a format that can easily be used by someone else)
f) not be subject to automated decisions in certain circumstances
g) withdraw consent where consent to data processing is required

Any request for personal information from a data subject that relates to their data protection must be forwarded to the DPO (link on the church web-site).

Any valid SAR will be acted upon as quickly as possible and certainly within one calendar month of the request unless there is a lawful reason for extending this timescale.

There should be no charge for any SAR, though, if this is to be provided in paper format and a large quantity of paper is required, a charge may be made for this: the data subject must be informed of this in advance and advised of other methods of transfer.

Direct marketing

The church will not use data processing for any form of direct marketing.

The church will not share personal data with any other organisation for the purposes of direct marketing.

Working with other organisations and transferring data

Sharing information with other organisations

The church will only share personal data with other organisations or people when there is a legal basis to do so and after the data subject has been informed (unless legal exemptions apply). Only authorised individuals are allowed to do this.

A detailed record will be kept of every occasion on which personal data has been shared with a third party: this must include any legal exemptions that may have applied and will be in line with the Data Sharing Code Of Practice from the Information Commissioners Office (ICO).

Data processors

ChurchSuite is the main data processor for the church. The privacy notice and terms and conditions are available on their web-site.

Transferring personal data outside the UK

Personal data cannot be transferred outside of the UK unless this is permitted within UK GDPR. This includes storage of personal data of others on a ‘cloud’-based service.

Managing change and risks

Data protection impact assessments

A Data Protection Impact Assessment (DPIA) is required if any data processing may result in a risk of data breach such as moving personal data to a new server or data processor, or transferring personal data abroad. If a decision is made not to apply a DPIA, this must be minuted by the PCC and may also need to be reported to the ICO.

Dealing with data protection breaches

If anyone thinks they may have accidentally caused a data breach, this must immediately be reported to the DPO in order to limit damage to the data subject(s) involved. The DPO, depending upon the level of data breach, may also have to inform the ICO: this will happen if the data breach could result in harm to the data subject.

All data breaches must be recorded even if they are not reported to the ICO

Appendix A – definitions

Data controller	this is the person, company, authority or other body that determines the means for processing personal data and the purposes for which it is processed.
Data processor	this is the individual or organisation which processes the personal data on behalf of the instructions of the data controller.
Data subject	this includes everyone about whom personal data are stored and, from a church point-of-view, will include employees and church members, and may include people we care for, other people and/or organisations with whom we work, volunteers, complainants, supports, enquirers, advisory agencies.
ICO	the Information Commissioners Office: this is the regulatory body in the UK responsible for ensuring compliance with our legal duties. The ICO produces guidance on implementing data protection law and can take legal action where a breach occurs: such legal action can lead to a fine.
Personal data	this is any information relating to a person that can identify that person. Such information is factual, and includes such details as name, address, date of birth, etc.
Privacy notice	the information given to data subjects that explains how we process their data and for what reasons.