



Holy Trinity Church Old Hill Data Protection Policy

Document History

Version	Purpose / Amendments	Originated	Checked	Approved	Date
I	First version for approval	June 24	June 24	PCC	1/7/24

Contents

SECTION A: INTRODUCTION	3
Policy Statement	3
Key Definitions	3
Scope	3
Data Protection Principles	4
Roles and Responsibilities	4
SECTION B: PROCESSING OF PERSONAL DATA	5
Data Processing	5
Privacy Notice	5
When we need consent to process data	6
Accurate Data	6
Data Retention	6
Security of personal data	6
SECTION C: INDIVIDUAL RIGHTS	7
Data Subjects Rights	7
Direct Marketing	8
SECTION D: SHARING OF DATA	8
SECTION E: MANAGING CHANGE & RISKS	8
Data Protection Impact Assessment	8
Data Breach	8
REVIEW OF POLICY	9
ICO REGISTRATION	9

Section A: Introduction

Policy Statement

The Parochial Church Council (PCC) and Vicar of Holy Trinity Church Old Hill (“Holy Trinity”) are committed to protecting personal data and respecting the rights of the people whose personal data we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all relevant laws, and adopting good practice. Holy Trinity has a responsibility under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) to ensure that the personal data we collect is accurate, necessary and proportionate for our purposes, is accessed only by those who need to, is retained securely and for only as long as required. This policy sets out the measures Holy Trinity takes to meet its commitments and responsibilities under law.

Key Definitions

- *Personal Data* – any information relating to a living individual who is identified or identifiable directly from that information or who can be indirectly identified from that information in combination with other information. Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.
- *Data Subject* - the identifiable living individual about whom Holy Trinity holds personal data.
- *Processing* – Anything that is ‘done’ to personal data, including the collection, access of, retention and updating of that data.

Scope

At Holy Trinity, we process personal data to help us:

- Maintain our list of church members.
- Provide pastoral support for members and other connected with the church.
- Provide services to the community, such as Open Door, Food for the Soul etc.
- Safeguard children, young people and adults at risk.
- Recruit, support and manage staff and volunteers.
- Provide services for life events, including weddings and funerals.
- Maintain our accounts and records.
- Promote our services and activities.
- Maintain the security of the church building.
- Respond effectively to any enquires.

In the course of our work, we may collect and process information (personal data) about many different people (data subjects). This includes data we receive straight from the person it is about, for example, where they complete forms or contact us. We may also receive information about data subjects from other sources including, for example, previous employers and personal referees.

Data subjects that we are likely to hold personal data about include:

- the people we care for and support;
- our employees (and former employees);
- consultants/individuals who are our contractors or employees working for them;
- volunteers;
- trustees;

- complainants;
- supporters;
- enquirers;
- friends and family;
- advisers and representatives of other organisations.

We process personal data in both electronic and paper form and where this data is held electronically or in a paper filing system all this data is protected under data protection law. The personal data we process can include information such as names and contact details, education or employment details, and visual images of people.

This policy applies to all employees of Holy Trinity, individuals and organisations that work on behalf of the church.

Data Protection Principles

In compliance with the seven Data Protection Principles laid out by the GDPR and the DPA, Holy Trinity will make sure that all personal data is:

- Processed lawfully, fairly and in a transparent manner.
- Processed for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary for the purposes for which it is being processed.
- Accurate and, where necessary, up to date.
- Not kept longer than necessary for the purposes for which it is being processed.
- Processed in a secure manner, by using appropriate technical and organisational means.
- Processed in keeping with the rights of data subjects regarding their personal data.

Roles and Responsibilities

- *Data Protection Officer (DPO)* – is responsible for advising Holy Trinity clergy, staff and trustees about their legal obligations under data protection law, monitoring compliance with data protection law, dealing with data security breaches and with the development of this policy. The DPO is also the primary liaison between the church and the Information Commissioner's Office (ICO). This role will be assumed by the Administrator. Any questions about this policy or any concerns that the policy has not been followed should be referred to mail@holytrinity.org.uk
- *Data Controller* – is responsible for determining the purposes for which personal data is processed and the way in which it is processed. Holy Trinity PCC, as an organisation, is the data controller.
- This policy has been approved by the Parochial Church Council who are responsible for ensuring that we comply with our legal obligations.

Section B: Processing of Personal Data

Data Processing

Holy Trinity will ensure that at least one of the following lawful bases applies to the processing of personal data:

- The processing is necessary for a contract with the data subject.
- The processing is necessary for us to comply with a legal obligation.
- The processing is necessary to protect someone's life (this is called "vital interests").
- The processing is necessary for us to perform a task in the public interest, and the task has a clear basis in law.
- The processing is necessary for legitimate interests pursued by Holy Trinity or another organisation, unless these are overridden by the interests, rights and freedoms of the data subject.
- the processing will only be lawful if the data subject has given their clear consent.

In some cases, we may hold types of information that are called "special categories" of data in the GDPR. This personal data can only be processed under strict conditions. 'Special categories' of data, as set out in the GDPR, includes information about a person's: racial or ethnic origin; political opinions; religious or similar (e.g. philosophical) beliefs; trade union membership; health (including physical and mental health, and the provision of health care services); genetic data; biometric data; sexual life and sexual orientation.

Processing of 'special categories' of personal data is only lawful when, in addition to the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These conditions include where:

- The processing is necessary for carrying out our obligations under employment and social security and social protection law.
- The processing is necessary for safeguarding the vital interests (in emergency, life or death situations) of an individual and the data subject is incapable of giving consent.
- The processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes.
- The processing is necessary for pursuing legal claims.
- If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent.

We will not hold information relating to criminal proceedings or offences or allegations of offences unless there is a clear lawful basis to process this data such as where it fulfils one of the substantial public interest conditions in relation to the safeguarding of children and of individuals at risk or one of the additional conditions relating to criminal convictions set out in either Part 2 or Part 3 of Schedule 1 of the Data Protection Act 2018. Any such processing will be carried out on the advice of the Diocese of Worcester's Safeguarding Team.

To ensure that our processing of personal data will only be fair and lawful when the purpose for the processing meets a legal basis, as listed below, and when the processing is transparent. This means we will provide people with an explanation of how and why we process their personal data at the point we collect data from them, as well as when we collect data about them from other sources, unless an exemption under the DPA applies.

Privacy Notice

Holy Trinity's Privacy Notice will be made available to data subjects so that they can access full privacy information regarding the retention of their data; any sharing of that data; and their rights in relation to their personal data. Where personal data is collected from another source, this information will be provided to the data subject in writing and no later than within 1 month after we receive the data, unless a legal exemption under the GDPR applies. If we use the data to communicate with the data subject, we will at the latest give them this information at the time of the first communication.

When we need consent to process data

Where none of the other legal conditions apply to the processing, and we are required to get consent from the data subject, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

Consent can however be withdrawn at any time and if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

Accurate Data

We will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points thereafter. Data subjects have a responsibility to provide accurate data when requested by Holy Trinity.

Data Retention

Holy Trinity shall regularly, review the personal data which it holds and remove any data where retention is no longer justified. Such removal shall be made as soon as is reasonably practicable after retention of the data was identified as no longer justified.

Security of personal data

We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful access, or from accidental loss, destruction or damage.

We will implement measures which provide a level of security that is appropriate to the risks involved in the processing.

All laptops/PCs containing user identifiable data should –

- Have user accounts protected by a password that isn't used anywhere else, of at least 9 characters and include both upper & lowercase letters, at least one numeric and one symbol.
- Have their local drive(s) encrypted via BitLocker (Windows) or FileVault (MacOS). This will ensure that should any laptop/PC be stolen, the local drives cannot simply be removed and accessed via another device. For this reason, all laptops/PC owned by Holy Trinity must be running the Professional edition of Windows, not the Home version.

Where non-Holy Trinity owned devices are used –

- All user accounts (ie family members with their own logins) must be protected by a password. Non-trusted accounts (ie children) must not have accounts with Administrative access.
- If non-Holy Trinity devices are unable to run BitLocker or FileFault , any data that can be identified to an individual must either be stored on an external USB Drives that supports data encryption, and has data encryption enabled, or third party drive encryption software should be used.

Paper-based records (containing user identifiable data) should never be left lying about after use, and always out away after use.

In all cases, storage of data that can be identified to an individual should only be stored when absolutely necessary. Those with access to the full HTOH Directory and with Administrative access to our church database software need to be fully aware of entries that cannot be shared with others without prior permission. If in any doubt the best approach is always to get the details of the person requesting the contact details and then pass these directly to the person they are requesting the details for, and ask them to make contact.

In all cases a certain degree of common sense should be used as often there is an overlap of personal and Holy Trinity data, ie names and contact details of friends who are also members of Holy Trinity.

Measures will be reviewed on a continuous basis. Any additional or changes to existing measures will be assessed in consideration of the following:

- The quality of the security measure.
- The costs of implementation.
- The nature, scope, context and purpose of processing.
- The risk (of varying likelihood and severity) to the rights and freedoms of data subjects.
- The risk which could result from a data breach.

Holy Trinity will seek appropriate professional advice commensurate with its data protection requirement whenever the following might adversely compromise the church's legitimate processing of personal data covered by the GDPR:

- We are planning to make significant changes to the ways in which they process personal data.
- There is any national publicity about new risks (e.g. cyber-attacks).

Section C: Individual Rights

Data Subjects Rights

We will process personal data in line with data subjects' rights, including their right to:

- Request access to any of their personal data held by us (known as a Subject Access Request).
- Ask to have inaccurate personal data changed.
- Restrict processing, in certain circumstances.
- Object to processing, in certain circumstances, including preventing the use of their data for direct marketing.
- Data portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation.

- Not be subject to automated decisions, in certain circumstances.
- Withdraw consent when we are relying on consent to process their data.

We will act on all valid requests from data subjects that relates to their data protection rights as soon as possible, and at the latest within one calendar month, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances. All data subjects' rights are provided free of charge but data subjects are required to provide proof of identification in order for their Subject Access Request to be responded to

Direct Marketing

Direct marketing means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. "Marketing" does not need to be selling anything or be advertising a commercial product. It includes contact made by organisations to individuals for the purposes of promoting the organisation's aims.

Any direct marketing material that we send will identify Holy Trinity as the sender and will describe how people can object to receiving similar communications in the future. If a data subject exercises their right to object to direct marketing, we will stop the direct marketing as soon as possible.

Section D: Sharing of Data

We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice), unless legal exemptions apply to informing data subjects about the sharing. Only authorised and properly instructed clergy, staff and trustees are allowed to share personal data.

Before sharing personal data with an external body, Holy Trinity will take all reasonable steps to verify that the body is, itself, compliant with the provisions of the GDPR.

We will keep records of information shared with an external body, which will include recording any exemptions which have been applied, and why they have been applied. We will follow the Information Commissioner's Office (ICO) statutory Data Sharing Code of Practice (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

Section E: Managing Change & Risks

Data Protection Impact Assessment

When we are planning to carry out any data processing which is likely to result in a high risk, we will carry out a Data Protection Impact Assessment (DPIA). We may also conduct a DPIA in other cases when we consider it appropriate to do so. If we are unable to mitigate the identified risks such that a high risk remains, we will consult with the ICO.

DPIAs will be conducted in accordance with the ICO's Code of Practice, available [here](#).

Data Breach

Where clergy, staff, trustees or volunteers, (or contractors working for us), think that this policy has not been followed, or data might have been breached or lost, this will be reported immediately to the Data Protection Officer. A record of all personal data breaches will be kept by the Data

Protection Officer.

We will report all serious data breaches which are likely to result in a high risk to any person, to the ICO. Reports will be made to the ICO within 72 hours from when someone in the church becomes aware of the breach.

In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay.

Review of Policy

This policy will be reviewed by the Parochial Church Council annually.

ICO Registration

Data Controller: Holy Trinity Church Old Hill

Registration Number:

Date Registered:

Date Expires: