[INSERT CHURCH NAME]

CCTV Policy

**{March 2025: This template is intended as a ‘best practice’ document and does not constitute legal advice. We have made it clear where churches should tailor this document to their specific needs. Please be aware that if you make changes outside of these areas, it may mean the policy is no longer best practice and FIEC cannot be held responsible for your amendments. When customising this document for your own church’s use, please edit all the text in [square brackets] and delete the brackets. Please also delete the instructions in {curly brackets} once you have followed them – including this paragraph – as they should not form part of the final document.}**

## Church details

Charity number:

Church address:

Church contact:

Email:

Phone:

This policy first adopted / last reviewed: [INSERT DATE]

This policy should be reviewed at least every 2 years. The next review is due on: [INSERT DATE]

## Introduction

The safety and security of staff, volunteers and visitors at [CHURCH NAME] is of paramount importance. To support the church in maintaining a safe and secure environment, a Closed-Circuit Television system (CCTV) is used within and around the building. This system has been installed and is used in accordance with the legislation referenced throughout this policy.

This document has been produced to provide everyone at [CHURCH NAME] with the necessary level of information regarding the rationale for the use of a CCTV system and how to respond to anyone who make enquiries as to the use of such systems, whilst also explaining how to respond to access requests for data generated by CCTV systems.

## Definition of terms

CCTV (also referred to as a “surveillance camera system”) is a system used for the recording and viewing of visual images for surveillance purposes.

Undirected surveillance is the gathering of images and information which is not targeted at any one individual.

General Data Protection Regulation (GDPR) and the Data Protection Act 2018 is the legal framework that sets guidelines for the collection and processing of personal information of individuals.

The Surveillance Camera Code of Practice 2022 ([www.gov.uk/government/publications/update-to-surveillance-camera-code](http://www.gov.uk/government/publications/update-to-surveillance-camera-code)) details twelve guiding principles, which strike a balance between protecting the public and upholding civil liberties, as follows:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more information and images should be stored than are strictly necessary for the stated purpose of a surveillance camera system, and such information and images should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement reasons.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose, and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure that legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When a surveillance camera system is used in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the objective of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which is compared against a reference database for matching purposes should be accurate and kept up to date.

## Complying with GDPR

[CHURCH NAME] will ensure compliance with the GDPR and that personal data will be:

* Processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”)
* Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
* Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
* Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
* Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
* Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

In accordance with the requirements of the Information Commissioner’s Office for organisations who operate a CCTV system [CHURCH NAME] is registered with the Commission and has paid the appropriate fee.

## Use of CCTV

The purpose of CCTV at [CHURCH NAME] is to:

* Protect the safety, security and well-being of staff, volunteers and visitors
* Prevent and detect crime and may be used to support the prosecution of offenders
* Facilitate learning through reflection as a result of incidents occurring within the monitored areas

CCTV will not be used for any purpose other than those specified above.

### Location

CCTV cameras are positioned in the following locations:

* [INSERT LOCATION(S) OF CAMERA(S)]

All cameras are overtly positioned and appropriate signage is positioned around the property.

### Retention of images and information

A proportionate approach is used to inform retention periods; however, images and information acquired from the surveillance system at [CHURCH NAME] will not be kept for longer than is necessary. There may, however, be occasions where it is necessary to retain images for a longer period, i.e. when a crime is being investigated.

The agreed retention period for CCTV images at [CHURCH NAME] is [INSERT TIME PERIOD]. All images are saved [LOCATION] {specify where images are saved and how they will be deleted after retention period, e.g. “on the hard drive of the CCTV and they are automatically deleted after 14 days”}.

### Accessing retained images and information

Access to retained images is restricted to the data protection lead at [CHURCH NAME], who is [INSERT NAME OF DATA PROTECTION LEAD].

There may be, on occasion, requests by data subjects (individuals) to access images and information that is held about them. In accordance with the GDPR, all data subjects have a right to access their data and any supplementary information held by [CHURCH NAME]. Data subjects have a right to receive:

* Confirmation that their data is being processed
* Access to their personal data
* Access to any other supplementary information held about them

The purpose for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them.

When a request to access images and information is received, the data subject is to be asked to provide as much detail as possible. All access requests must be made in line with the church’s data protection policies and response must be within the timeframes specified therein.

### Third-party requests for access to images and information

Requests may be received from third parties to access images and information. The data controller must be able to satisfy themselves that the person requesting the data has the authority of the data subject or the legal right to request information.

### Complaints

Should a visitor have cause to complain about the CCTV system, the data controller should be contacted. Visitors are to be advised that complaints will be processed in accordance with [CHURCH NAME]’s complaints policy.