

Closed Circuit Television (CCTV) images are used for the prevention, identification, and reduction of crime and to monitor buildings. It is used to provide a safe and secure environment for the public and to prevent the loss of or damage to property. It is a TV system primarily for surveillance and security purposes in which signals are not publicly distributed but are monitored, and where access to their content is limited by design only to those authorised to see it.

Available below is a GDPR compliant template policy document that will allow churches and cathedrals to govern the installation and operation of all CCTV cameras within their church or cathedral buildings or any separate building or land that are owned and controlled by them. This policy template will need to be tailored to the requirements of the buildings, but when finalised, will apply to all who use the building and must be followed by all staff including consultants and contractors.

Download

[CCTV Policy Template](#)

[CCTV Signage](#)



Pickpik

CCTV operators, those assigned to manage the CCTV systems, will need to be properly licensed by the [Security Industry Authority](#).

- A license is required where CCTV is used for wider security purposes, and the system is staffed by paid security staff.
- A minister who is listed as the CCTV operator, as a fixed entity/person, will be treated as an "employee" and will require a license.
- A license will not be needed if the person overseeing the CCTV is undertaking the work as a volunteer and receives no payment in kind or a reward for services.

If the person in charge of the CCTV system is a churchwarden, a license may not be needed. The PCC should consider who is best placed to hold the license (churchwarden or minister) to reduce disruption with changing personnel.

The use of any CCTV system must comply with the Information Commissioner's Office (ICO) CCTV [Code of Practice 2017](#) to ensure CCTV is used responsibly and safeguards both trust and confidence in its continued use. The [Surveillance Camera Code of Practice 2013](#) also provides statutory guidance on the appropriate and effective use of surveillance camera systems in accordance with Section 30 (1) (a) of the [Protection of Freedoms Act 2012](#) and should be considered as part of this guidance.

CCTV systems can only be used to observe the areas under surveillance to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed. Operation of the CCTV system must be conducted in a professional, ethical, and legal manner, and any diversion of the use of CCTV security technologies for other purposes is illegal.

Any camera used for CCTV recording must be sited, so it only captures images relevant to the purposes for which it is installed. Also, equipment must be carefully positioned to:

- cover the specific area to be monitored only;
- keep privacy intrusion to a minimum;
- provide recordings are fit for purpose and not in any way obstructed (e.g. by foliage);
- minimise the risk of damage or theft.

CCTV may **not** be used for streaming services or any other event held in a church or cathedral, and any interior CCTV **must not** record any areas set aside for private devotions where one would not expect to be filmed while praying. Similarly, in any churches where sacramental Confession or other ministries of individual pastoral support, such as healing, are practised, there should be no filming in the part, or parts of the church set aside for these purposes. Interior cameras covering areas of public worship **must** be **turned off** during any form of service, whether regular

worship or occasional offices. Exterior CCTV or cameras in areas not used for public worship should remain in operation during services.

Cameras should only be monitored in a secure and private location by the named operator. For churches where CCTV is added for security purposes, a fixed and secure lockbox/cabinet could be used for monitoring and viewing CCTV images. Additionally, the data can be accessed via a wireless device in a private room. If a private and secure area is not available, this secure lockbox may be discretely located in an open space, and the data broadcast over a private server and made available via a live stream to the operator.

Livestreaming via the use of a surveillance system, such as a webcam or even a mobile phone app that provides access to live streaming functions, is still subject to the requirements of the UK GDPR, as the recording still constitutes the processing of personal data if you can identify individuals directly or indirectly. Helpful guidance on Video Surveillance, and more specifically on Live Streaming, is [provided by the ICO](#) and includes relevant checklists that should be considered as part of any installation of CCTV system or use of live streaming devices.

Where Cloud-based storage is used, the church or cathedral will need to ensure that such storage is located in the European Economic Area (EEA) and that all relevant security and data protection measures are in place. The recorded material must be stored in a way that maintains the integrity of the image and information to ensure that metadata (e.g. time, date, and location) is recorded reliably, and compression of data does not reduce its usefulness.

If viewing on-site, any monitors should be password protected and switched off when not in use to prevent unauthorised use or viewing. The cameras installed must provide images that are of suitable quality for the specified purposes for which they are installed, and all cameras must be checked daily to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

For copyright purposes, any images recorded will remain the property and copyright of the church or cathedral.

The location of equipment must be carefully considered to ensure that images captured to comply with data protection requirements. Signs must be placed at all pedestrian and vehicular entrances in order to inform staff, church officers, visitors, and members of the public that CCTV is in operation. A template of this sign is available [here](#).

If installing any CCTV System within a church, permission will be required from the Archdeacon under B1.10 of the **Faculty Jurisdiction (Amendment) Rules 2019**. If in doubt, speak to your [Diocesan Advisory Committee secretary](#). For cathedrals, permission for the introduction of cameras must be sought from the [Cathedral's Fabric Advisory Committee](#). In some cases, depending on the location, prominence, or attachment requirements, permission may be necessary from the [Cathedrals Fabric Commission for England](#).

Unless required for evidentiary purposes, the investigation of an offence or as otherwise required by law, all CCTV images must be retained for

no longer than 31 calendar days from the date of recording. Where an image is required to be held in excess of this retention period, any recordings will need to be protected against loss or held separately from the surveillance system and retained for a period of 6 months following the date of the last action. Images held in excess of this retention period will be reviewed on a three-monthly basis, and if these are no longer required for evidentiary purposes, these should be deleted.

The full template CCTV policy is available [here](#), and where amendments are required, these are highlighted in yellow or marked via a comment.

Also of interest

[Audio visual and electrical wiring](#)

[How to keep all your electrical systems and equipment safe to use.](#)

[Connectivity](#)

[Find how more on how to get connected](#)

[Live Streaming](#)

[Review the legal and safety considerations for live streaming or sharing recordings from your church building](#)

[Applying for permission](#)

[Understand more about the faculty process and gaining permission for works to churches](#)

Source URL: <https://www.churchofengland.org/resources/churchcare/advice-and-guidance-church-buildings/cctv>