Version 7
Ludlow St. Laurence Parish Church

Revisions:
V1 Dec 2016 using material from Ely, Liverpool, York & new content
V1.2 Jan 7th 2017, following initial review by A. Keyser
V2 17th Jan 2017, approved by Standing Com
V2.1 With amendments following further review by A. Keyser
V3 23rd Jan 2017 Considered by PCC on 27th February 2017.
V4 and 5 Updated 1st March 2017
V6 updated Feb 2021
V7 Final – Mar 2021

CCTV POLICY

The purpose of this policy is to ensure:

1. That the use of CCTV adheres to the principles of the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 and Code of Practice 2017 covering GDPR.
2. That the CCTV system is not abused or misused.
3. That CCTV is correctly and efficiently installed and operated.
4. That all personnel can be assured of the safeguards in place.

1. Introduction

A level of surveillance is carried out visually by staff at all times. This is unregulated, but the actions in the case of an irregularity being observed need to be defined:

CCTV is not used for recording church services or in areas of private prayer. St. Laurence's Church uses closed circuit television (CCTV) images to provide a safe and secure environment for employees, volunteers and to protect Parochial Church Council (PCC) assets and property. The SLL CCTV facility records images. There is no audio recording and therefore conversations are not recorded on CCTV (but see the section on covert recording below).

2. Purposes of CCTV

The purposes of the PCC installing and using CCTV systems include:

- assisting in the prevention or detection of crime or equivalent malpractice
- assisting in the identification and prosecution of offenders
- monitoring the security of the Church building and environs
- monitoring tills, cash handling and safes within the church
- assisting with the assurance of safeguarding procedures
- assisting with the identification of unauthorised actions or unsafe working practices that might result in disciplinary proceedings being instituted against employees and to help in providing relevant evidence
- monitoring the building by remote when the alarm is activated

3. Permission to operate the scheme

The PCC shall satisfy itself that:

a) the actions to be taken when starting the use of the scheme have been properly complied with (See Appendix C),
b) there are procedures (including those in this Policy) in place regarding the operation of the system (See Appendix D) and
c) that there is a procedure in place for an annual audit of the system operation (See Appendix E) before giving its consent to the operation of the scheme.

4. Location of cameras

Cameras are located at strategic points throughout the church including:

1. Nave
2. Chancel
3. Shop
4. Shop Till
5. Outer vestry Cash counting table
6. Inner vestry safes
7. Outer vestry safes

All cameras (with the exception of any that may be temporarily set up for covert recording) are clearly visible. A sign is prominently and clearly displayed at the entrance so that employees, volunteers, and visitors are aware that they are entering an area covered by CCTV.

5. Administrators/Operators of the CCTV system:

The system may only be used by the Church Operations Manager and the Rector. Each has an individual password and can access the system remotely.

6. Live viewing

The CCTV system records images in real time. The system can be live viewed by the Operator for the purposes described below. Note that live images will still be recorded and retained and are thus subsequently managed under this Policy.

Live viewing is authorised only in the event that an alarm is triggered. In such an event the Administrator and/or the Operator may undertake live viewing. In the absence of the Administrator and the Operator, a Church Warden may undertake live viewing. As a result of live viewing the Police may be called. A record must be kept of any such viewing and stored at the Parish Office.

7. Recording and retention of images

Images are produced by the CCTV equipment are as clear as possible so that they are effective for the purposes for which they are intended. Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly and that high quality images are being produced. Images are recorded in constant real-time (24 hours a day throughout the year). The recording system records digital images which are stored on the hard drive of a PC or server. CCTV images that are held are deleted

and overwritten on a recycling basis and, in any event, are not normally held for more than 28 days. When a hard drive has reached the end of its use it will be rendered unreadable prior to disposal. Images that are stored on, or transferred to, removable media such as CDs are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be after a period of one month. The Administrator will ensure that records of each copy, its contents, current user/location and destruction are recorded. Where a law enforcement agency is investigating a crime, images may need to be retained for a longer period and destroyed as soon as practicable at the conclusion of any investigation or proceedings.

8. Access to and disclosure of images

Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are protected. Images can only be disclosed in accordance with the purposes for which they were originally collected. The images are recorded centrally and held in a secure location. Access to recorded images is restricted to the Administrator and Operator, and on occasions the Church Wardens. When viewing of recorded images is taking place, two persons must be present and would normally be the Church Operations Manager and the Rector , if one or both of them are unavailable, then one or both Church Wardens will be present. They are authorised to view recorded images in accordance with the purposes of the system. Viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing is taking place. Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and limited to:

- the police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness
- prosecution agencies, such as the Crown Prosecution Service
- relevant legal representatives with appropriate permissions/authority
- supervisors involved with SLL's disciplinary processes
- individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

The PCC are the only persons permitted to authorise disclosure of information to external third parties such as law enforcement agencies. All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded. See Appendix A.

9. Intruder detection

The CCTV system may be used in conjunction with the building intruder detection system from time to time. In this case, images will be relayed to the Administrator and Operator mobile telephone/tablet as part of the security procedures. The Administrator will keep a record of such authorised mobile telephone numbers, the telephone user and the date(s)/time(s) of use. Images will not be retained on these devices for longer than required for the immediate security purpose, as the image is also stored within the CCTV system.

10. Individuals' access rights

Under the Data Protection Act 1998, individuals have the right on request to receive a copy of the personal data that the PCC holds about them, including CCTV images if they are recognisable from the image.

11. Covert recording

The PCC will only undertake covert recording (in real time or delayed) with authorisation of the PCC and Rector where there is good cause to suspect that criminal activity such as theft is taking, or is about to take, place and where informing the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection. Covert monitoring may include both video and audio recording. Covert monitoring will only take place for a limited and reasonable amount of time consistent with the objective of assisting in the prevention and detection of the particular suspected criminal activity or equivalent malpractice. Once the specific investigation has been completed, covert monitoring will cease. Information obtained through covert monitoring will only be used for the prevention or detection of criminal activity or equivalent malpractice. All other information collected in the course of covert monitoring will be deleted or destroyed unless it reveals information which the PCC cannot reasonably be expected to ignore.

12. Staff training

The PCC will ensure that all employees handling CCTV images or recordings are trained in the operation and administration of the CCTV system and on the impact of the Data Protection Act 1998 with regard to that system.

13. Implementation

The Administrator is responsible for the implementation of and compliance with this policy and the operation of the CCTV system. He/she will conduct an annual review of the use of CCTV. Any complaints or enquiries about the operation of the CCTV system should be addressed to him/her. The Administrator is responsible for the safe keeping and retention of all records relating to permissions, viewing and destruction of CCTV data as set out in this Policy for a period of not less than 7 years from the date of the activity

Appendix A

Image Provision to Third Party

Date of Incident		Description	Outcome
Time of Incident			
Operator			

Original to be provided, copy to be retained Yes/No		Copy to be provided, original to be retained Yes/No
Reason for Provision		Legal Proceedings/Subject Access/Other
Date of Creation	Time of Creation	Operator
Crime/Incident no/ Reason for Access		
Police Officer/3rd Party Name		
Police Station/3rd Party Address		
Telephone Number	Date of Handover	
Signature		
Date of destruction/return	Method of Destruction	Operator

Appendix B

Viewing of CCTV Images (*FROM RECORDING or *LIVE) (delete as applicable)

Date of viewing	Time	Location	Operator
Reason for viewing			
Outcome if any			
Name(s) of Persons viewing		**Organisation Details**	

Appendix C – Check list when starting the CCTV scheme

- Who has responsibility for control of the information and making decisions on how it can be used? If more than one body is involved have responsibilities been agreed and does each know its responsibilities?
- Has the body (or have the bodies) responsible notified the ICO that they are the data controller? Does the notification cover the purposes for which the information is used, the disclosures that are made and other relevant details?
- If someone outside your organisation provides you with any processing services, for example editing information (such as CCTV images), is a written contract in place with clearly defined responsibilities? This should ensure that information is only processed in accordance with your instructions. The contract should also include guarantees about security, such as storage and the use of properly trained staff.
- Have you identified clearly defined and specific purposes for the use of information and have these been communicated to those who operate the system?
- Are there clearly documented procedures, based on this code, for how information should be handled in practice? This could include guidance on disclosures and how to keep a record of these. Have these been given to the appropriate people?
- Has responsibility for ensuring that procedures are followed been allocated to an appropriate named individual? They should ensure that standards are set, procedures are put in place to meet these standards, and that the system complies with this code and legal obligations such as an individual's right of access.
- Are proactive checks or audits carried out on a regular basis to ensure that procedures are being complied with? This can be either by you as the system operator, or a third party.

Appendix D – Governance checklist

Once you have followed the guidance in this code and set up the surveillance system you need to ensure that it continues to comply with the DPA and the code's requirements in practice. You should:

- tell people how they can make a subject access request, who it should be sent to and what information needs to be supplied with their request;
- give them a copy of this code or details of the ICO website; and
- tell them how to complain about either the operation of the system or failure to comply with the requirements of this code.

Staff using the surveillance system or information should be trained to ensure they comply with this code. In particular, do they know:

- What the organisation's policies are for recording and retaining information?
- How to handle the information securely?
- What to do if they receive a request for information, for example, from the police?
- How to recognise a subject access request and what to do if they receive one?

All information must be sufficiently protected to ensure that it does not fall into the wrong hands. This should include technical, organisational and physical security. For example:

- Are sufficient safeguards in place to protect wireless transmission systems from interception?
- Is the ability to make copies of information restricted to appropriate staff?
- Are there sufficient controls and safeguards in place if the system is connected to, or made available across, a computer, eg an intranet?
- Where information is disclosed, how is it safely delivered to the intended recipient?
- Are control rooms and rooms where information is stored secure?
- Are staff trained in security procedures and are there sanctions against staff who misuse surveillance system information?
- Are staff aware that they could be committing a criminal offence if they misuse surveillance system information?

Any documented procedures that you produce following on from this code should be regularly reviewed, either by a designated individual within the organisation or by a third party. This is to ensure the standards established during the setup of the system are

maintained.

Similarly, there should be a periodic review, at least annually, of the system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, it should be stopped or modified.

- Is it addressing the needs and delivering the benefits that justified its use?
- Is information available to help deal with queries about the operation of the system and how individuals may make access requests?
- Does the information include your commitment to the recommendations in this code and include details of the ICO if individuals have data protection compliance concerns? Is a system of regular compliance reviews in place, including compliance with the provisions of this code, continued operational effectiveness and whether the system continues to meet its purposes and remains justified?
- Are the results of the review recorded, and are its conclusions acted upon?

Appendix E - Checklist for users of limited CCTV systems monitoring small retail and business premises

This CCTV system and the images produced by it are controlled by …….. who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998).

Activity	Checked (date)	Checked by	Date of next check
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
The problem we are trying to address has been clearly defined and installing cameras is the best solution.			
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.			

The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

*****END*****