



# ALLSAINTS

## WOODFORD WELLS

<b>Title</b>	CCTV Policy
<b>Owner</b>	Operations Manager
<b>Issue Date</b>	January 2025
<b>Reviewed By</b>	Bob Darby
<b>Approved By</b>	PCC
<b>Approved Date</b>	March 2015 March 2017 March 2019 March 2024 January 2025 March 2026
<b>Next Review Due</b>	March 2027

# All Saints' with St Andrew's CCTV Policy

## Introduction

All Saints' Woodford Wells operates a CCTV scheme within the entire church and site premises. The CCTV cameras monitor the interior and exterior of the building continuously. The system was upgraded in January 2025.

The PCC is ultimately responsible for this policy. Authority to manage the CCTV system is delegated to the Operations Manager.

## Policy Principles

1. CCTV shall be provisioned to provide a safer and more secure environment for the benefit of all users of the site and in particular:
  - To deter burglary, vandalism, misuse of church property and misuse of visitors' property.
  - To deter inappropriate access to activities going on, such as children's work and the pre-school.
  - To substantiate facts in the event of an accident or claim.
2. CCTV shall be implemented to deliver these benefits ensuring:
  - Camera locations are appropriate (and won't be obscured).
  - Cameras are operational 24/7
  - Camera image quality is sufficient to achieve the purpose – including when prints are produced from the recordings. The level of compression is appropriate.
  - Cameras are secure and protected from vandalism as far as practicable.
  - Cameras have not been sited in areas where privacy can be expected (toilets/changing rooms, counselling room).
3. Notices shall be permanently displayed at key locations to indicate that a CCTV monitoring system is in place. All new staff members will be informed of the CCTV operation during their induction.
4. The CCTV will not be used to record sound.

## CCTV Procedures

5. **Access** – The CCTV recording equipment is kept securely in a locked cupboard. Access to the cupboard is authorised by the Operations Manager. Access to images is controlled with secure passwords, and is available to operational staff, via a display screen in the church office, and to other staff via a web-based app as approved by the Operations Manager. Access to recordings is controlled with secure passwords and is available to staff as approved by the Operations Manager.
6. **Retention/destruction of images** - Images are stored on the hard drive in the cupboard. Images will normally be kept for 30 days and permanently deleted/overwritten after that time. Where there has been an incident which may involve damage/injury or where (in the view of the Operations Manager) suspicious activity has been recorded, relevant images may be preserved until such time as it is apparent that they are no longer likely to be relevant. If there

is a requirement to save images these are stored in a secure and restricted access location on the ASWW file server. A review of any retained images will be carried out annually and, in each case, it will be determined whether the images still need to be retained.

7. **Releasing images to third parties** – This will only be done with the approval of the churchwardens or the Operations Manager and only in circumstances where:

Either:

- The PCC is obliged by law to disclose the images, or
- The police have requested the images as part of a criminal investigation, or
- Social services or another public body have requested the images in order to assist them in fulfilling their legitimate duties, or
- Images are relevant or have been requested for the purposes of an insurance claim or court proceedings and failure to release them could result in an injustice, or
- The images are relevant in the context of court proceedings in which the parish or a member of staff/volunteer is involved, or
- An individual has requested copies of images of themselves or their possessions. (In this case copies will be provided as soon as possible and in any event within one month.)<sup>1</sup>

and

- It is made clear that the images are released on the express condition that they are not to be passed on any further,

and

- Clear records are kept of what images have been released, to whom, on what date and with what justification.

8. **Review and maintenance** – The Operations Manager will be responsible for monitoring compliance with this policy and for carrying out regular checks and audits.

- There will be an annual checks/maintenance of equipment – including a check that the date and time stamp remain correct.
- There will be a annual review of this policy
- There will be an annual audit of compliance with procedures and policy.

<sup>1</sup> In the case of a subject access request, care will be taken to ensure that images of other people are obscured before the images are handed over. If it is necessary to appoint a contractor to do this a written contract will be put in place providing explicit security guarantees. The subject will be asked to specify precisely that dates and times in respect of which their request is made.