



Closed Circuit Television (CCTV) Monitoring Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
2.0	October 2025	Helen Kingdon		Updated policy adopted Oct 2024

Table of contents

1	Introduction	2
1.1	Policy statement	2
1.2	Status	2
2	Use of CCTV	2
2.1	Purpose	2
2.2	Data Protection Impact Assessment (DPIA)	3
2.3	Location	3
2.4	Retention and deletion of images and information	4
2.5	Accessing retained images and information	4
2.6	Third party requests for access to images and information	5
2.7	Complaints	5
2.8	Access register	5
2.9	Audit	6
	Annex A – Application for access to personal/CCTV records (SAR)	7
	Annex B – Access register	10
	Annex C – CCTV system audit	11



1 Introduction

1.1 Policy statement

The safety and security of staff, patients, contractors and visitors at St Leonard's Practice is of paramount importance. To support the management team in maintaining a safe and secure environment, a closed-circuit television (CCTV) system is used within the organisation.

This system has been installed and is used in accordance with extant legislation:

- [Data Protection Act 2018](#)
- [Surveillance Camera Code of Practice 2013](#)

This document has been produced to provide all staff with the necessary information regarding the use of CCTV and how to respond to patients who make enquires relating to the CCTV system, while explaining how to respond to access requests for data generated by CCTV systems.

This policy is to be read in conjunction with the organisation's [UK GDPR policy](#).

1.2 Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the [Equality Act 2010](#). Consideration has been given to the impact this policy might have regarding the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment. Furthermore, this document applies to all employees of the organisation and other individuals performing functions in relation to the organisation such as agency workers, locums and contractors.

2 Use of CCTV

2.1 Purpose

The purpose of CCTV at this organisation is to:

- Protect the safety, security and wellbeing of staff, patients, visitors and contractors



- Prevent and detect crime within the organisation and may be used to support the prosecution of offenders
- Facilitate learning through reflection because of incidents occurring within the monitored areas
- Monitor the movements and activities of staff and visitors whilst on the premises.
- Form part of staff counselling or disciplinary procedures, as appropriate.
- Assist with complaint resolution.

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

2.2 Data Protection Impact Assessment (DPIA)

For surveillance systems, the organisation must take a data protection by design and default approach and perform a DPIA for any processing that is likely to result in a high risk to individuals. This includes:

- Processing special category data
- Monitoring publicly accessible places on a large scale
- Monitoring individuals at a workplace

The organisation should assess whether the use of surveillance is appropriate and, as part of the assessment, should consider the reasonable expectations of the individuals whose personal data is processed and the potential impact on their rights and freedoms. This organisation will record its considerations and mitigations in a DPIA prior to the use of a surveillance system that is likely to result in a high risk to individuals.

If high risks cannot be mitigated, prior consultation with the Information Commissioners Office (ICO) is required and the organisation cannot proceed with the processing until guidance has been received from the ICO. An example DPIA can be found in the [UK GDPR Policy](#).

2.3 Location

At this organisation, all cameras are overtly positioned and do not impede upon any clinical areas. Appropriate signage is prominently displayed in all areas covered by the CCTV system.

The [ICO](#) explains that signs must be placed prominently before the entrance to the system's field of vision and reinforced with further signs within the area. They should be positioned at a reasonable distance from the places monitored and in such a way



that individuals can easily recognise the circumstances of the surveillance before entering the monitored area.

A poster to identify that this organisation has CCTV cameras can be found [here](#).

CCTV cameras are positioned in the following locations:

- Externally – beside the front entrance doors
- Internally – in the patient waiting area

2.4 Retention and deletion of images and information

Principle 6 of the [Surveillance Camera Code of Practice](#) states that images and information obtained from a surveillance camera system should not be retained for longer than necessary to fulfil the purpose for which they were obtained in the first place. A proportionate approach should always be used to inform retention periods and these should not be based upon infrequent exceptional cases.

Although images and other information should not be kept for longer than necessary to meet the purposes for recording them, on occasions a system operator may need to retain images for a longer period, for example when a law enforcement body is investigating a crime to give them the opportunity to view the images as part of an active investigation.

Images are currently retained for one month.

At the end of the retention period, all images are deleted appropriately.

2.5 Accessing retained images and information

To conform with Principle 7 of the [Surveillance Camera Code of Practice](#) access to retained images is restricted to the data controller. In their absence, a nominated individual is authorised to access the retained images and information.

In accordance with the UK GDPR, all data subjects have a right to access their data and any supplementary information held by this organisation. 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 data subjects access 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 advised to complete the organisation's CCTV subject access request form as



detailed in [Annex A](#). Providing an individual with a transcript of the visual information contained in the footage is not enough to comply in most circumstances.

Data controllers must respond to all data subject access requests as per the [Access to Medical Records Policy](#).

While an unusual route to obtain CCTV images, information may also be made under the [Freedom of Information Act 2000](#). For further detailed information, see the organisation's [Freedom of Information Policy](#).

This organisation is not permitted to charge a fee for processing such requests.

2.6 Third party requests for access to images and information

Requests may be received from third parties to access images and information. Such instances may include requests from solicitors to support either a claimant or defendant when a crime has been alleged or, for example, a person's property has been damaged within the car park.

The data controller must be able to satisfy themselves that the person requesting the data has the authority of the data subject. The responsibility for providing the required authority rests with the third party and is usually in the form of a written statement or consent form, signed by the data subject. It should be noted that such requests for images or information should be approached with care and in accordance with the data protection legislation as a wide disclosure may be an unfair intrusion into the privacy of the individuals concerned.

2.7 Complaints

Should a patient, visitor or contractor have cause to complain about the organisation's CCTV system, the data controller should be contacted. Complaints will be processed in accordance with organisation's complaints procedure.

- [Complaints Procedure \(England\)](#)
- [Complaints Procedure \(Scotland\)](#)
- [Complaints Procedure \(Wales\)](#)
- [Complaints Procedure \(Northern Ireland\)](#)

2.8 Access register

The template at [Annex B](#) is to be used to record all access to the CCTV system.



2.9 Audit

The template at [Annex C](#) is to be used to audit the CCTV system at St Leonard's Practice.

Annex A – Application for access to personal/CCTV records (SAR)

APPLICATION FOR ACCESS TO PERSONAL/ CCTV RECORDS (SAR)

In accordance with the Data Protection Act 2018

Section 1: Personal details

Surname		Title	
Forename		Date of birth	
Address			
Tel no.		Email:	

Section 2: Record(s) requested

Please tick the relevant box below. The more specific you can be, the easier it is for us to quickly provide you with the records requested.

I am applying for access to view my records only	☐
I am applying for an electronic copy of my records	☐
I am applying for a printed copy of my records	☐
I am applying for CCTV records	☐

Please specify what information you are requesting:

Records between specific dates only (please give dates below)	☐
Records with regard to a specific incident (please give details below)	☐
Other (please give details below)	☐

Declaration

I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the records referred to above under the terms of the UK [Data Protection Act 2018](#).



You are advised that the making of false or misleading statements to obtain personal information to which you are not entitled is a criminal offence which could lead to prosecution.

Signature		Date	
------------------	--	-------------	--

Section 3: Proof of identity

Under the [Data Protection Act 2018](#), you do not have to give a reason for applying for access to your records. You will however be asked to provide two forms of identification one of which must be photographic identification.

ADDITIONAL NOTES:

Before returning this form, please ensure that you have:

- Signed and dated the form
- Are able to provide proof of your identity
- Enclosed documentation to support your request (if applicable)

Incomplete applications will be returned; therefore, please ensure you have the correct documentation before returning the form.

For office use only:

Identification verification must be verified through two forms of ID one of which must contain a photo, e.g., passport or photo driving licence, and, for example, a bank statement.

Request received		Request refused	
Reviewed by		Request completed	
Fee		Date sent	
Comments			
Identity verified by		Date	
Method	☐ Photo ID or proof of residence – Type ☐ Photo ID or proof of residence – Type		



Annex B – Access register

[Insert organisation name]	Data controller: [insert name]
CCTV System Access Register	Date: [insert month]

Date	Time	Reason for access	Outcome	Individual
20 Jan 23	14.30	Deletion of images in accordance with organisation policy	All images deleted successfully	I N Pain (Practice manager)

Annex C – CCTV system audit

[Insert organisation name]		Data controller: [insert name]	
CCTV system audit		Date: [insert date]	
Requirement	Yes	No	
Is the appropriate signage displayed throughout the organisation advising individuals that CCTV surveillance is taking place?			
Do the signs include who is responsible for operating the system and who to contact for further information?			
Is the system fit for purpose, i.e., does it capture quality images?			
Are all clinical areas excluded from CCTV surveillance?			
Does the system require regular maintenance or calibration? If so, is there an appropriate contract in place to facilitate this?			
Are images stored using encryption?			
Is access restricted to the images and information which are collected?			
Is there a CCTV subject access request form available for individuals and third parties to use to request access to images and information?			
Who can access images and information? [State names and roles]			
What is the retention period? [Give details]			
What is the disposal process? [Give details]			

Does the organisation have a CCTV or surveillance policy?			
Does the policy reflect the GDPR?			
Is staff aware of the organisation policy and how to deal with requests and complaints? [Give details if necessary]			
Is the CCTV system included on the organisation asset register?			
Is there a log to record access and disposal?			
What training has staff received in relation to the use of the CCTV surveillance system? [Give details]			
Additional comments:			
Signed:		Name:	