



Closed Circuit Television (CCTV) Monitoring Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
1.1	11/01/24	ZV	RLC	Updated CCTV locations following installations of new cameras

Table of contents

1	Introduction	2
1.1	Policy statement	2
1.2	Status	2
2	Legislation	2
2.1	Data Protection Act 2018	2
2.2	GDPR	3
2.3	Surveillance Camera Code of Practice 2013	3
3	Use of CCTV	5
3.1	Purpose	5
3.2	Data Protection Impact Assessment (DPIA)	5
3.3	Location	6
3.4	Retention of images and information	7
3.5	Accessing retained images and information	7
3.6	Third party requests for access to images and information	8
3.7	Disposal of images and information	8
3.8	Complaints	8
3.9	Access register	Error! Bookmark not defined.
3.10	Audit	9
4	Summary	9



1 Introduction

1.1 Policy statement

The safety and security of staff, patients, contractors and visitors at Ystwyth Medical Group 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](#) including Chapter 2 titled 'The GDPR'
- [Surveillance Camera Code of Practice 2013](#)

This document has been produced to provide all staff at Ystwyth Medical Group with the necessary level of information regarding the rationale for the use of CCTV systems in general practice and how to respond to patients who make enquires as to the use of such systems whilst also explaining how to respond to access requests for data generated by CCTV systems.

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 that 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This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time.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. Other individuals performing functions in relation to the organisation, such as agency workers, locums and contractors, are encouraged to use it.

2 Legislation

2.1 Data Protection Act 2018



GDPR gives member states limited opportunities to make provisions for how it applies in their country. Following Brexit, GDPR became UK GDPR and was incorporated as Chapter 2 of DPA 2018.

It is therefore important that the GDPR and the DPA 2018 are read side-by-side.

2.2 GDPR

Ystwyth Medical Group has a legal requirement to 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 which 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

Further reading can be found in the [UK GDPR Policy](#).

2.3 Surveillance Camera Code of Practice 2013

The [code](#) was released in June 2013 and then updated in both November 2021 and March 2022. It continues to detail 12 guiding principles which strike a balance between protecting the public and upholding civil liberties.

These are:



-
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 consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
 3. There must be as much transparency regarding 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 images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system and such images and information 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 regarding 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 purposes.
 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 legal requirements, policies and standards are compiled within the organisation with regular reports being published.
 11. When the use of a surveillance camera system is 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 aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

3 Use of CCTV

3.1 Purpose

The purpose of CCTV at Ystwyth Medical Group 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

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

3.2 Data Protection Impact Assessment (DPIA)

Specifically, under Article 30 of the UK GDPR, organisations are required to maintain a record of the processing activities taking place. This applies to both controllers and processors using surveillance systems. The records the organisation keeps should cover areas such as the purpose(s) for the lawful use of surveillance, any data sharing agreements that are in place and the retention periods of any personal data.

For surveillance systems, the organisation must take a data protection by design and default approach and perform a Data Protection Impact Assessment (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 in the circumstances. As part of the assessment, the organisation should consider the



reasonable expectations of the individuals whose personal data is processed and the potential impact on their rights and freedoms. Ystwyth Medical Group should record its considerations and mitigations in a DPIA prior to any deployment 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](#).

3.3 Location

CCTV cameras are positioned in the following locations:

- In the building
 - In the waiting room
- Outside the building
 - Facing the front door
 - Facing the rear fire exit
 - Facing the side fire exit
 - Facing the bins
 - Facing the car park

Cameras are all overtly positioned and do not impede upon any clinical areas within the organisation. Appropriate signage is positioned throughout the organisation in the following locations:

- In the building
 - In the waiting room
- Outside the building
 - On the building wall, facing the entrance to the car park
 - On the entrance to the waiting room

In accordance with Article 13 of the UK GDPR, it is important to ensure that the areas of surveillance are identified. The signs should 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.

It is also important to ensure that the organisation informs people other than workers, such as visitors who may inadvertently be caught by monitoring, aware of its operation and why the organisation is carrying this out.



3.4 Retention 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.

The retention period for different surveillance camera systems will vary due to the purpose for the system and how long images and other information need to be retained to serve its intended purpose. It is not, therefore, possible to be prescriptive about maximum or minimum periods. Initial retention periods should be reviewed by Rhianon Copeland Practice Manager and reset in the light of experience. 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 where a law enforcement body is investigating a crime to give them the opportunity to view the images as part of an active investigation.

3.5 Accessing retained images and information

Principle 7 of the [Surveillance Camera Code of Practice](#) advises that access to retained images is restricted. At Ystwyth Medical Group this is the data controller who is Dr Gail Davies, Senior Partner. In their absence, Rhianon Copeland Practice Manager and Daniel Webb Administrator, are authorised to access the retained images and information.

There may be, on occasion, requests by data subjects (individuals) to access images and information that are held about them. In accordance with the GDPR, all data subjects have a right to access their data and any supplementary information held by Ystwyth Medical Group.

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 subject access request form, available



from the practice website, or via reception. 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](#).

Whilst an unusual route to obtain CCTV images, information may also be made under the [Freedom of Information Act 2000](#). Further reading on FOI requests can be sought within the [Freedom of Information Policy](#).

3.6 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 where 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.

3.7 Disposal of images and information

As stated in [Section 3.4](#), the images and information are stored for the minimum time period necessary to fulfil the purpose and therefore, at Ystwyth Medical Group they will be routinely deleted after 6 months in an automated process.

3.8 Complaints

Should a patient, visitor or contractor have cause to complain about the organisation's CCTV system, the data controller should be contacted.

Patients, visitors and contractors are to be advised that complaints will be processed in accordance with complaints policy.

- [Complaints Procedure \(Wales\)](#)



**Grŵp Meddygol
Ystwyth
Medical Group**

www.ystwythmedicalgroup.co.uk

Parc y Llyn
Aberystwyth
Ceredigion
SY23 3TL

Tel: 01970 613500
Fax: 01970 613505

Audit

The template at [Annex C](#) is to be used to audit the CCTV system at Ystwyth Medical Group.

4 Summary

CCTV systems are valuable tools that enhance the safety, security and wellbeing of services, staff and patients at Ystwyth Medical Group and are an increasingly common sight in GP practices.

In line with the relevant legislation and code of practice referenced in this policy, it is essential that the use of such systems and the staff who use them are compliant and that all guidelines and processes are complied with.

Annex C – CCTV system audit

Ystwyth Medical Group	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:	