St Michael's Clinic CCTV Policy

Document Control

1. Confidentiality Notice

This document and the information contained therein is the property of St Michael's Clinic. This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from St Michael's Clinic.

2. Document Details

Organisation:	BUPA – St Michael's Clinic
Current Version Number:	V1.2
Current Document Approved By:	Mark Norfolk
Date Approved:	September 2022
Next Review Date:	May 2026 (or before if required)

3. Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1.1	April 2024	Helen Carter	Mark Norfolk	Reviewed, minor amendments made
1.2	May 2025	P Haycox J Darlington	Graham White	Reviewed no amendments made
	June 2026			Organisation change

CCTV Policy

1. Policy Objective

The purpose of this policy is to regulate the management and use of the closed-circuit television (CCTV) system at St Michael's Clinic.

2. Relevant CQC Fundamental Standard / H+SC Act Regulation (2014)

- Regulation 10: Dignity and respect
- Regulation 13: Safeguarding

3. Policy

3.1 The purpose of using CCTV is to ensure that St Michael's Clinic's Patients, staff members, visitors and healthcare professionals are afforded the best possible security and safety whilst visiting or being treated by St Michael's Clinic.

3.2 The CCTV system is a digital system; it is an entirely closed system with no wireless capability. The system does not make audio recordings.

3.3 It is policy that all CCTV cameras are situated in communal areas only; there are no cameras in private areas such as changing rooms, WCs, etc.

3.4 Information about use of CCTV will be made available e.g., warning signs, as required by the Code of Practice of the Information Commissioner will be placed at all access routes to areas.

3.5 CCTV is never used as a substitute for trained and well supported staff members; instead it is used as an extra layer of security.

3.6 It is policy that St Michael's Clinic will meet at all times the ICO 'A Data Protection Code of Practice for Surveillance Cameras And Personal Information', ICO 'Conducting Privacy Impact Assessments' CQC 'Using Surveillance' and St Michael's Clinic Information Governance Policy & Procedure and St Michael's Clinic CCTV Code of Practice, the Data Protection Act 1998, The Human Rights Act 1998, and the Health & Social Care Act 2008.

3.7 The Home Office Code of Conduct will be followed at all times (see Annex 1)

3.8 Materials or knowledge secured as a result of CCTV will not be released to the media, or used for any commercial purpose, or for the purpose of entertainment. Recordings will only be released under the written authority from the Police, or in respect of a subject access request.

3.9 The CCTV system will be in operation 24 hours a day, for every day of the year.

3.10 The CQC Registered Manager or nominee will check on a weekly basis that the system is operating effectively and in particular that the equipment is properly recording and that cameras are functional. The system will be regularly serviced and maintained. Defects will be reported to the servicing company at the earliest convenient opportunity.

3.11 All persons viewing CCTV material will be authorised and have a business- need-to-know to do so.

3.12 All staff involved in the operation of the CCTV system will, by training and access to this policy, be made aware of the sensitivity of handling CCTV images and recordings.

3.13 Information about the existence of the CCTV systems will be made available to patients, staff and others using the facility, and appropriate consents obtained as applicable.

4 Control of Software and Access To The System

Access to the CCTV software will be strictly limited to authorised operators.

4.1 Camera surveillance may be maintained at all times

4.2 Monitors will be located in secure areas offices.

4.3 Live and recorded materials may be viewed by authorised operators in investigating an incident and recorded material may be downloaded from the system in line with the objectives of the scheme.

4.4 A record will be maintained of the release of images to the Police or other authorised applicants. A register will be available for this purpose.

4.5 Images (stills and footage) may be viewed by the Police for the detection of crime. Viewing of images by the Police must be recorded in writing and in the logbook. Requests by the Police can be allowable under section 29 of the Data Protection Act (DPA) 1998

4.6 Should images be required as evidence, a digital copy may be released to the Police. St Michael's Clinic retains the right to refuse permission for the Police to pass the images to any other person.

4.7 The Police may require St Michael's Clinic to retain images for possible use as evidence in the future. Such images will be securely stored until they are needed by the Police

4.8 Applications received from outside bodies (e.g., solicitors) to view or release images will be referred to the Directors, in these circumstances, images will normally be

released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.

4.9 Retention: Images will be retained only for as long as these are required. The system will automatically delete all recordings held on the main control unit.
None of the systems enable storage after a maximum of 60 days.

4.10 In the event of a serious incident, data will be downloaded from the system and stored securely pending any external investigation. This will not be retained for longer than 60 days unless this has been deemed necessary by an external body in relation to their own investigations. As soon as it is reasonably practical, the data will be deleted following any external investigation.

5. Breaches of the Policy & Procedure/Code of Practice

Any breach of the CCTV Code of Practice by staff members at St Michael's Clinic will be investigated by the CQC Registered Manager or nominee in order for them to take any appropriate disciplinary action.

6. External Requests for Access to CCTV Recording

6.1 Requests by persons outside of the company for viewing or copying of disks or obtaining digital recordings will be assessed on a case-by-case basis.

6.2 Requests from the police will arise in a number of ways, including:

- requests for a review of recordings in order to trace incidents that have been reported
- immediate action relating to live incidents, e.g., immediate pursuit
- for major incidents that occur when images may have been recorded continuously
- individual police officers seeking to review recorded images on the monitor

6.3 All requests for disclosures will be forwarded to the CQC Registered Manager or nominee.

6.4 Requests for access to recorded images from persons other than the police or the data subject (that is, the person whose image has been captured by the CCTV system) will be considered on a case-by-case basis. Access to recorded images in these circumstances will only be granted where it is consistent with the obligations placed on St Michael's Clinic by the Data Protection Act 1998 (DPA) and, in particular, with the purposes set out in Section 1 of the DPA.

6.5 It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for

evidential purposes. Users of CCTV will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images. These aspects of the policy reflect the Second and Seventh Data Protection Principles of the Data Protection Act 1998.

6.6 All staff should be aware of the restrictions set out in this policy in relation to access to, and disclosure of, recorded images.

6.7 Access to recorded images will be restricted to staff who need to have access in order to achieve the purposes of using the equipment.

6.8 All access to the disks on which the images are recorded will be documented.

6.9 Disclosure of the recorded images to third parties will be made only in the following limited and prescribed circumstances and to the extent required or permitted by law:

- law enforcement agencies where the images recorded would assist in a specific criminal inquiry
- prosecution agencies
- relevant legal representatives
- people whose images have been recorded and retained and disclosure is required by virtue of the Data Protection Act 1998

6.10 All requests for access or disclosure will be recorded. The management will make decisions on access to recorded images by persons other than police officers. Requests by the police for access to images will not normally be denied and can be made without the above authority, provided they are accompanied by a written request signed by a police officer who must indicate that the images are required for the purposes of a specific crime enquiry.

6.11 If access or disclosure is denied, the reasons will be documented.

6.12 If access to or disclosure of the images is allowed then the following will be documented:

- the date and time at which access was allowed or the date on which disclosure was made
- the reason for allowing access or disclosure
- the extent of the information to which access was allowed

7. Photographs

Photographs and hard copy prints taken from digital images are subject to the same controls and principles of Data Protection as other data collected. They will be treated in the same way as digital images.

At the end of their useful life all computer disks, still photographs and hard copy prints will be disposed of as confidential waste. This code of practice will be reviewed annually to assess its implementation and effectiveness and it will be promoted and implemented throughout our company

8. Privacy Impact Assessment

A privacy impact assessment will be conducted by St Michael's Clinic when necessary to enable us to consider risks and how these can be mitigated.

All actions to reduce risks will be implemented by St Michael's Clinic following completion of the assessment.

9. Complaints

Complaints about St Michael's Clinic CCTV system should be handled under St Michael's Clinic Complaints Policy & Procedure.

10 Consent

Consents from patients will be obtained when necessary, e.g. when video or audio recordings are to be released to third-parties.

APPENDIX 1

Home Office CCTV Code of Practice

In line with the Home Office 12-point code of conduct the use of the system will:

- always be for the purpose specified which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
- consider its effect on individuals and their privacy
- have as much transparency as possible, including a contact point for access to information and complaints
- have clear responsibility and accountability for all surveillance activities including images and information collected, held and used
- have clear rules, policies, and procedures in place and these must be communicated to all who need to comply with them

- have no more images and information stored than that which is strictly required
- restrict access to retained images and information with clear rules on who can gain access
- consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
- be subject to appropriate security measures to safeguard against unauthorised access and use
- have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with 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, when used in pursuit of a legitimate aim
- be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes

The primary purpose of the system is to:

- help maintain an environment for patients, staff, and others, which supports their safety and welfare
- deter crime against persons, and against the company buildings and company assets
- assist in the identification and prosecution of persons having committed an offence