**Policy on the use of**

**Surveillance Technology**

|  |  |
| --- | --- |
| **Document Type:** | Policy |
| **Version:**  | 1.0 |
| **Date of Issue:** | February 2021 |
| Renewal by:  | February 2023 |
| Author: | Information Governance Business Partner-Primary Care  |
| Distribution to: | All staff within Oswald Medical Centre |

|  |
| --- |
| **VERSION CONTROL SHEET** |
| **Date****dd/mm/yy** | **Version** | **Author** | **Version/Reason for changes** |
| **03/02/2021** | **0.1** | **Liz Griffiths** | **Initial production of policy** |
| **08/02/2021** | **0.2** |  | **Updates and amendments** |
| **16/02/2021** | **1.0** | **Liz Griffiths** | **Final and approved version** |

###### Contents:

|  |  |  |
| --- | --- | --- |
| **Heading Number** | Heading  | **Page Number(s)** |
| **1** | **Introduction / Purpose** | **3** |
| **2** | **Surveillance Technology including Closed Circuit Television (CCTV)** | **4-8** |
| **3** | **Associated Documents and Legislation** | **8** |
| **4** | **Duties**  | **9** |
| **5** | **Implementation** | **9** |
| **6** | Training and record keeping | **9** |
| **7** | Monitoring and review | **9-10** |
| **8** | References / Bibliography | **10-11** |

**1 Introduction / Purpose**

Surveillance technology includes Closed Circuit Television (CCTV), cameras and microphones and is used for surveillance in public areas where monitoring may be required e.g., banks, airports, hospitals, General Practices etc. The Information Commissioner’s Office (ICO) CCTV Code of Practice sets out the measures which must be adopted to comply with the Data Protection Act2018 (DPA18) which supplements the UK General Data Protection Regulations (UK GDPR). This Code of Practice has the dual purpose of assisting operators of surveillance technology to understand their legal obligations while also reassuring the public and our patients about the safeguards that should be in place.

The aim of this policy is to ensure that Oswald Medical Centre operates its CCTV system in accordance with the DPA18 and UK GDPR in respect of the use of surveillance technology. We also ensure we adhere to other key legislation, as listed in the Bibliography in section 10 of this document. The Care Quality Commission (CQC) and the ICO both regulate activities in relation to surveillance. The CQC ensure any practice or healthcare setting that uses surveillance to help keep people safe or monitor their wellbeing would use this as a method of care, and as such must meet the regulations as stipulated under the Health and Social Care Act (2012). The ICO regulate information collected about people so the practice recordings of anybody entering and using the services of our practice must meet the regulations as stipulated by the ICO.

This policy also reflects the wider regulatory environment. When using, or intending to use surveillance systems, the Practice also considers their obligations in relation to the Freedom of Information Act 2000 (FOIA), the Protection of Freedoms Act 2012 (POFA), the Human Rights Act 1998 (HRA) and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act (POFA code). Aside of considering compliance with the principles of the DPA and UK GDPR, the practice when using surveillance technology, will ensure they pre-determine two issues:

1. The type of personal data being processed as the DPA18/UK GDPR make it permissible for **Special categories of personal data** to be processed.

Personal data which falls within the definition of “Special Category” as defined by Chapter 2 Article 9 of GDPR must meet the following precept:

“*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited. This, however, shall not apply in the following cases:*

* Data subject has given explicit consent.
* Specific circumstances related to employment and social security.
* Protecting the rights of the subject or other person when subject is incapable of giving consent.
* Processing data manifestly made public by the subject.
* In defence of a legal claim when courts are acting in their judicial capacity.
* Substantial public interest provided this is proportionate to the aim pursued.
* Processing for the purposes of preventative or occupational medicine, subject to set safeguards.
* Public interest in the area of public health
* Research purposes in accordance with article 89(1), which is proportionate to the aim pursued.

2. The **purpose(s)** for which both personal and sensitive personal data is being processed. The data must be:

* Fairly and lawfully processed.
* Collected for a specified, explicit, and legitimate Purpose.
* Adequate, relevant, and limited to what is necessary.
* Accurate and where necessary, kept up to date.
* Not kept for longer than is necessary.
* Kept in a form which permits identification of data subjects for no longer than is necessary.
* Processed in a manner that ensures appropriate security of the personal data.

The ICO will consider the extent to which ${PracticeName} has used surveillance technology in relation to compliance with the CCTV Code of Practice when determining whether the practice has fulfilled its legal obligations when exercising their powers of enforcement.

It is the policy of ${PracticeName} that no one will be discriminated against on grounds of age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, or sexual orientation. ${PracticeName} will provide interpretation services or documentation in other mediums as requested and necessary to ensure natural justice and equality of access.

**2 Surveillance Technology including Closed Circuit Television (CCTV)**

Oswald Medical Centre has notified the ICO that we intend to use surveillance technology on site for the purposes of:

* Prevention or detection of crime or disorder
* Apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings)
* Interest of public and employee Health and Safety
* Protection of public health

Responsibility for the control of the images obtained from the surveillance technology and how they can be used lies with the Practice Manager (or equivalent).

**2.1 Initial Assessment Procedures**

Prior to any surveillance technology installation, the Practice Manager will ensure that it is to be used in accordance with Oswald Medical Centre’s registration with the ICO, as mentioned in section 2 and complies with the DPA18/UKGDPR and CCTV Code of Practice.

The process for approval for surveillance technology is:

* Need for surveillance technology identified.
* Area assessed by the Practice Manager and any other relevant personnel with practice to ensure surveillance is appropriate.
* The Practice Manager ensures a Risk Assessment is completed
* Siting of surveillance technology approved by the Practice Manager.

It is essential that a Data Protection Impact Assessment (DPIA) is completed to ensure the risks are clearly identified due to the high-risk nature of processing using surveillance technology, as advocated by the ICO, and legally mandated by the DPA18. The completed document must be signed by the Practice Caldicott Guardian, SIRO (or the Information Governance Lead if applicable) and the Practice Data Protection Officer. The fully compliant signed copies must be stored in practice and made available for release via the practice website.

**2.2 Selecting the Cameras and Quality of Image**

It is essential that the technical specification of the equipment is carefully considered, to ensure that the images captured are of an appropriate quality for the purposes for which they are being obtained and follow the DPA18/UK GDPR.

The surveillance technology will need to produce images of sufficient size, resolution, and clarity for its registered use, to ensure that the images produced are as clear as possible and effective for the purpose(s) for which they are intended (as listed in section 2). For example, if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose. To judge the quality of the image necessary for the purpose of its use, the Home Office Scientific Development Branch recommends the use of the following criteria:

* **Monitoring –** to watch the movement of people (or traffic) where it is not required to pick out individual figures.
* **Detecting –** to detect the presence of a person without the need to see their face.
* **Recognising –** to recognise someone you know or determine that someone is not known to you.
* **Identifying –** to record high quality facial images which can be used in court to prove someone’s identity beyond reasonable doubt.

Further consideration needs to be given to the suitability of the location where the camera is required e.g., light levels and size of the area to be viewed by the camera.

The cameras located within ${PracticeName} will only be installed by approved security companies who undertake camera installations and service contracts, and the cameras are to be serviced every year, with full maintenance logs and relevant certification retained by the practice.

Upon installation all equipment is tested to ensure that only the designated areas are monitored, and high-quality pictures are available in live and play-back mode.

The surveillance technology record continuously on each system and are referenced by camera location, date and time and camera number.

**2.3 Using the equipment.**

It is important that the surveillance technology used produces images of a suitable quality for the purpose for which the system was installed. The cameras installed at ${PracticeName} are used for the purposes described in section 2 and are accessed by authorised personnel only.

The compression rate for the system is based on the ‘weight’ of cameras per recording server. The cameras are serviced by the contractor every year and a record of the service is retained by the practice with logs stored in line with the NHS Records Management Code of Practice 2020.

**2.4 Siting the Surveillance Technology/CCTV Cameras.**

Appropriate and industry specification signage must be erected at entrance points to ${PracticeName} and throughout the site, to ensure staff, patients and visitors to the practice are aware that they are entering an area which is covered by CCTV surveillance equipment. The signs must include details of the:

* Name of the practice
* Purpose of the surveillance
* Contact details of the appropriate person if there are any queries.

When siting a camera, it is important to consider:

* Location
* Height
* Light
* Size of area requiring monitoring.
* It is secure and protected from vandalism.
* If a camera is positioned outside, that is it not obscured by the growth of foliage in spring/summer.
* The camera is appropriate for the type of image required.

Oswald Medical Centre has the following types of cameras installed.

* CCTV

A plan of the camera sites within Oswald Medical Centre is available from the Practice Manager.

**2.5 Storing/processing of images.**

All images are securely recorded on the system within the Practice for a period of 31 days. Once this period expires the image will be re-recorded over. Any hard drives which require disposal are done in line with the Practice IT Security policy as advised and governed by the Practice IT supplier. The Practice will also maintain an operating logbook for all surveillance technology used which will include all aspects of the operations process. This will be retained in practice and be subject to regular audits and monitoring to maintain efficient protocols.

**2.5.1 Retention of images**

Images, which are not required for the purpose(s) for which the equipment is being used, will not be retained for longer than is necessary. While images are retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the DPA and UKGDPR.

CCTV surveillance footage recorded on alternative media should be stored in a way that maintains the integrity of the images and where a limited number of authorised staff have access to it. The viewing and disclosure of these recordings is strictly monitored as per sections 2.5 and 2.6.

Where the images are required for evidential purposes in legal or Oswald Medical Centre disciplinary proceedings, the image is archived within the PC or recorded onto a CD (or equivalent media source) and stored securely by the Practice Manager. Viewing of images within Oswald Medical Centre Office is controlled by the Practice Manager.

**2.6 Access to viewing.**

Viewing of live images on monitors should be restricted to the operator unless the monitor displays a scene in the location of the monitor. If a request to view an image is received this is should be done in the designated secure office. Access to this office must be restricted to authorised personnel only. Prior to the viewing a formal request should be made to the Practice Manager.

**2.6.1 Disclosure of images to third parties**

The purpose of the surveillance technology within Oswald Medical Centre is primarily the detection and prevention of crime, health and safety of staff, patients, and visitors to the practice, therefore it may be appropriate to disclose images to law enforcement agencies in the event a crime needs to be investigated. Prior to any images being disclosed to any third-party, a formal request should be made to the Practice Manager.

It is important that access to, and disclosure of, the images recorded by surveillance technology is restricted and carefully controlled. This will 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 for example in a Police enquiry or an investigation being undertaken Police are required to demonstrate that the images they seek are necessary for the prevention or detection of crime and/or the apprehension or prosecution of offenders, and that if the images are not made available, these activities would be prejudiced. Police officers have access to a standard form as detailed under Schedule 2 Part 1 Paragraph 2 (or 5) of the DPA18, which can be used when asking for personal information, including CCTV images. A log of who accessed, deleted, or copied any data for audit purposes will be created and retained for audit purposes. Where copies of the images are to be removed for use in criminal proceedings, the requesting officer must supply a standard police section form, fully completed, and authorised by a more senior officer than the requesting officer, no lower than Inspector level. This form will be retained for audit purposes.

Access to the medium on which the images are displayed and recorded is restricted to practice staff and any authorised third parties.

Access and disclosure to images is permitted only if it supports the purpose of the registration.

**2.6.2 Subject Access Requests/Access to images by individuals**

Individuals whose images are recorded have a right under the DPA18 to request access to view CCTV images of themselves and to be provided with a copy of the images. Care should be taken in processing such a request if other people who may be seen in such footage cannot be edited out. It must be accepted that such a request may be refused if it puts any on-going criminal investigation at risk. Following a request, a written response will be made to the individual, giving the decision (and if the request has been refused, giving reasons). Following such a request the CCTV owner (in this case the practice) must provide this within one calendar month as per the conditions of any Subject Access Request. The CCTV owner (the practice) may also invite a requestor to view any such requested footage in cases where this might not be provided, and the applicant agrees with this arrangement.

If images of third parties are shown in the images requested, identifiable information must be redacted from the image prior to release by ${PracticeManager}. This should be done if providing these images would involve an unfair intrusion into the privacy of the third party or would cause them unwarranted harm or distress.

Redaction (including obscuring of individuals) of images is performed by the Practice Manager or nominated personnel working within Oswald Medical Centre.

Individuals who request access to images must make a formal request, adhering to the practice Subject Access Request Policy to the Practice Manager. The circumstances under which such a request may be denied are made clear in 2.6.2 above.

**2.6.3 Freedom of Information (FOI)**

As Oswald Medical Centre is required by law to release information relating its NHS activities, requests made under The Freedom of Information Act 2000 (FOIA) must be complied with and within 20 working days from receipt of the request.

Section 40 of the FOIA contains two exceptions relating to information about individuals:

* If the images requested are of the requester then this is exempt from an FOI request and should be dealt with as a Subject Access Request under the Data Protection Act.
* If the images are of other individuals, they may only be disclosed if the images contained do not breach the DPA/UK GDPR.

If individuals can be identified from the images, this constitutes *personal information* which will not be disclosed under FOI as exempt under section 40. The rules under which personal information is managed under DPA18/UK GDPR must also be considered. This decision will be made by the practice as part of the established FOI process.

**2.7 Complaints**

Any complaints received are managed via the Practice Complaint Management Policy and will be handled by the Practice’s named complaints lead. As per the practice Complaints Policy all complaints must be received in writing.

**2.8 Enforcement**

The ICO has the power to issue Enforcement Notices where it is considered that there has been a breach of one or more of the Data Protection Principles. An Enforcement Notice[[1]](#endnote-1) would set out the remedial action that the ICO requires of ${PracticeName} to ensure future compliance with the requirements of the Act.

**2.9 Documentation**

Copies of all documentation and records relating to CCTV usage will be held securely in line with the Records Management Code of Practice for a period of 3 years.

**3 Associated Documents & Legislation**

* The Human Rights Act 1998
* The Data Protection Act 2018
* The Freedom of Information Act 2000
* Data Protection and Information Governance Policy
* Access to Health Records Policy
* Protection of Freedoms Act 2012, Section 29
* The Regulation of Investigatory Powers Act (RIPA) 2000
* The Mental Health Act 1983
* CCTV Code of Practice 2020
* CCTV Systems and the Data Protection Act revised guidance (2018)
* Association of Chief Police Officers (ACPO) Guidance 2011-The Use of CCTV in Criminal Investigations
* Section 16(4) of the Private and Voluntary Health Care Regulations 2001
* General Medical Council: Making and Using Visual and Audio Recordings of Patients Standards May 2002
* Surveillance Camera Code of Practice; June 2013
* POFA

**4** **Duties within the Practice - Practice Manager (or other suitably appointed member of the team)**

* Liaising with Security Specialists to ensure that CCTV systems are legally managed.
* Selection and management of CCTV systems
* Providing assurance to the Senior members of the Practice Team/Owners that CCTV systems are operated in a manner to provide statutory compliance.
* Reviewing this document every 2 years or when there is a change in legislation.
* Ensuring that this document is implemented and adhered to
* Ensuring that mandatory and refresher training is attended every 2 years or as required.
* The management of documents and systems to comply with statutory requirements.
* Ensuring that systems are operated in accordance with the Data Protection Act 2018, UK General Data Protection Regulations, and the CCTV Code of Practice
* Developing, maintaining, and delivering CCTV training within the practice
* The monitoring of practice CCTV systems against statutory requirements
* Ensuring that Business Continuity Plans relating to the CCTV service are in place.
* Instructing others working with the system
* Ensuring that CCTV systems provide appropriate security coverage on site.
* Liaising with the Data Protection Officer regarding ${PracticeName} Data Protection Act registration.
* Ensuring the security of recorded images.
* Controlling access to CCTV systems and images.

**5 Implementation**

This document will be available within the Practice internal policies for all staff and made available on the website for all staff, patients, and members of the public to access.

**6 Training and Record Keeping**

The Practice will keep records showing who is responsible for operating the surveillance system and how we protect and manage the information the surveillance system collects.

As a Practice we will make sure the only people with access to recorded information are people with a legitimate and lawful need. The CCTV monitors will be housed in a lockable office and you strong passwords will be used to protect the information. As a Practice we remain responsible for the security of the information we collect.

To protect people's information, as a Practice we will ensure:

* staff are properly trained in handling information gathered by surveillance.
* we have clear policies and procedures for when people ask for access to recordings, about sharing information and for complaints about surveillance.
* we keep a record of who has had access to the information, when and why.
* we have a clear policy about keeping information and recordings secure, how long you keep them for, and when and how you destroy them.
* if someone else has to handle personal data on behalf of our practice, we will contract with them to set out clear rules on how they process it.

**7 Monitoring and Review**

The table below highlights the effective monitoring and audits required to ensure compliance.

|  |  |  |  |
| --- | --- | --- | --- |
| **Standard/process/issue required to be monitored** | **Process for monitoring** | **Responsible individual /group** | **Frequency of monitoring** |
| Duties | Policy review – with MLCSU Primary Care IG Business Partners to advice on any relevant changes but to be signed off by responsible person in practice. | Practice Manager | Every 2 years |
| Use of Surveillance Technology Policy | Audit of CCTV recordings/ complaints/request for access and disclosure of images procedure and recording in relevant practice-retained logs. | Practice Manager | Annually |
| Compliance with the code of practice  | Review of recorded images as well as key compliance audits to include training for key personnel. | Practice Manager | Quarterly |

**8** **References/Bibliography**

Data Protection Act (2018)

UK General Data Protection Regulations (2021)

CCTV Code of Practice (2020)

Surveillance Camera Code of Practice (2013)

Human Rights Act (1998) (Article 8 on people’s right to privacy)

Care Quality Commission guidance on Surveillance in Healthcare Settings

Protection of Freedoms Act 2012 (POFA)

1. [↑](#endnote-ref-1)