Version History	
Policy name	**Close Circuit Television (CCTV) Policy**
Version code	1.1
Owner	Kent and Medway GP DPO team
Adopted by and date	Waterfield House Surgery 30th May 2022
Date of Issue	September 2020
Review Date	May 2024
Parent Policy	Data Protection Policy

1 INTRODUCTION

1.1 Waterfield House Surgery uses surveillance images including CCTV footage (images), to provide a safe and secure environment for staff, patients, contractors and visitors and to protect the Practice's property. The Practice believes that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff and visitors.

1.2 Images recorded by surveillance systems are personal data which must be processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring that the legal rights of staff, relating to their personal data, are recognised and respected.

1.3 However, we recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns and to set out the accepted use and management of CCTV equipment and images, and other recording and monitoring systems[1] (referred to together in this Policy as "CCTV") to ensure the Practice complies with the General Data Protection Regulation (GDPR)[2], the Human Rights Act 1998 and other legislation (referred to together in this Policy as "the Legislation").

1.4 This policy is intended to assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence.

1.5 The Wells Medical Practice has produced this policy in line with the Information Commissioner's CCTV Code of Practice (www.ico.org.uk) and has updated the policy in light of the GDPR.

[1] This includes noise recorders, the office phone recording, intercom and any monitoring system on the Practice's premises etc.

[2] References to the GDPR in this Policy mean the GDPR as varied or supplemented by the Data Protection Act 2018

1.6 Relationship with other policies and procedures

1.6.1 Other policies and procedures within the Practice interface with the CCTV Policy, they include:-

- Data Protection Policy
- Subject Access Request Procedure
- Data Breach Procedure
- Privacy Notice and Website Privacy information
- NHS Record management and Retention schedule
- Data Protection Impact Assessment procedure and form

2 INSTALLING NEW SURVEILLANCE SYSTEM

2.1 Before installing a new surveillance system, a data protection impact assessment (DPIA) must be carried out to identify the potential risks in relation to Practice's use of CCTV and approach to compliance with the Legislation.

2.2 The DPIA should identify the purposes for the CCTV system potentially including:

- Deter crime;
- Assist in prevention and detection of crime;
- Assist with the identification, apprehension and prosecution of offenders;
- Assist with the identification of actions that might result in disciplinary proceedings against staff and volunteers;
- Monitor security of the Practice's buildings and areas; and
- Create a safe environment.

2.3 And the benefits to be gained from use of the CCTV system such as greater security for employees, patients, apprentices, suppliers and our property including cash, controlled medication and other goods. Once identified, the purpose for which the CCTV system is to be used must be recorded in writing within the Information asset register/data flow map.

2.4 In order to assist in demonstrating compliance with the Human Rights Act, the DPIA must consider the effect and potential effects on the privacy of individuals having regard to the siting of the camera(s) and detail any mitigating steps which can be taken to avoid/lessen the risk of breach of privacy. It must also follow the principles laid down in the GDPR for DPIAs and include:

i. a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by Practice.
ii. an assessment of the necessity and proportionality of the processing in relation to the purpose.
iii. an assessment of the risks to individuals.
iv. the measures in place to address risk, including security and to demonstrate that we comply.

Staff must seek the advice of the designated data protection officer (DPO), when carrying out a data protection impact assessment.

2.3 The personal data potentially processed by the CCTV system are images of employees, directors, officers, consultants, contractors, freelancers, volunteers, interns, casual workers, zero hour's workers, agency staff or any health care professionals, patients, visiting/passing members of the public in and around the practice's premises and car parks.

2.4 The legal basis for the processing of personal data by the CCTV system is for practice's legitimate interests to prevent crime and anti-social behaviour on its premises. This is in line with Article 6(1) (f) GDPR.

2.5 The Practice Manager or a representative nominated by them will be responsible for the management and operation of all CCTV systems operated by Practice on its premises.

2.6 A central record of all CCTV installations will be maintained by the Practice Manager/Assistant Practice Manager. Any new CCTV system must be reported on a timely basis to the Practice Manager/Assistant Practice Manager for update of the central records – the same will apply where CCTV systems are taken out or where a live CCTV is replaced by a dummy and vice versa.

2.7 The details held about the CCTV systems will be reviewed periodically by the Practice Manager/Assistant Practice Manager.

2.8 Support from third-party service providers will be required in relation to installation and maintenance only.

3 CCTV EQUIPMENT

3.1 The equipment selected for the CCTV system must be appropriate to satisfy the purposes set out in this policy. The equipment must be able to:

i. cover the area to be monitored and exclude areas that do not need to be monitored for the purposes set out in this policy;

ii. produce clear images of a high quality, (i.e. of a standard that would be capable of having evidentiary value to the police);

iii. work effectively 24 hours per day, 7 days a week;

iv. have night time monitoring;

v. work effectively within normal indoor conditions;

vi. produce images of sufficient size, resolution and frames per second to meet the requirements of the purposes;

vii. record high quality facial images which can be used in court to prove someone's identity beyond a reasonable doubt; and

viii. record in real time on a continuous basis.

4 SITING THE CAMERA

4.1 The position of the CCTV cameras is critical to ensuring our compliance with the Legislation. We must apply the following principles whenever we are siting cameras:

i. cameras should be restricted to monitor only those areas which are intended to be monitored;

ii. cameras should not be used to monitor any adjoining areas which are not intended to be covered by the system or where there is reasonable expectation of privacy (such as gardens, private dwellings, changing rooms or toilet areas where there is an expectation of privacy);

iii. where cameras are adjustable, they should be restricted so that they cannot be adjusted to overlook areas outside the CCTV monitored site;

iv. cameras should be positioned to record images which are relevant to the purposes for which we run the system;

v. cameras must be sited to ensure they can produce images of the right quality;

vi. cameras should be sited so that they are secure and protected from vandalism or other damage.

5 SIGNAGE

5.1 We are required to notify individuals if they are in an area where CCTV surveillance is being carried out. Typically this is achieved through the use of

prominent signs which are located at the start of the CCTV zone, with reminder notices placed at various locations inside the monitored zone.

5.2 **Dummy CCTV:** Where a dummy CCTV has been installed on the Practice's premises, appropriate signage as if the CCTV is a live one must be put in place.

5.3 The signs should:

i. alert individuals that they are entering a CCTV monitored zone;
ii. be legible and visible (the size of the sign will depend on the location and how visible it is to individuals);
iii. include the following information where this is not obvious:
    a) the identity of the organisation responsible for the system;
    b) a description of the purpose(s) of the system; and
    c) details of who to contact regarding the system (i.e. the Practice Manager for the Practice).

6 STORING IMAGES

6.1 We must maintain the integrity of all images whilst they remain in our possession. This is necessary to ensure that the evidentiary value of those images is protected (i.e. so they can be used as evidence in court).

6.2 CCTV images must be stored on a secure medium such as encryption and in a secure place to which access is controlled (this is particularly important where images may be used for evidentiary purposes). We have an obligation to keep CCTV images secure at all times so as to prevent unauthorised viewing or disclosure. To ensure that we meet our security obligations you must ensure that:

i. access to the images is restricted to authorised staff only;

ii. disclosure of images (where permitted) is undertaken using a secure method of transmission or delivery (so as to minimise the risk of images getting lost in transit or being intercepted);

iii. CCTV storage boxes where images are stored are kept secure at all times and locked when unoccupied; and

iv. any images stored on computer must be password protected.

6.3 All images stored on CD or tape shall be secured in locked boxes.

6.4 Where CCTV images are to be cross-referenced with other databases in order to identify individuals, these databases must be kept current and accurate and the quality of data must be such that mismatches do not occur.

6.5 Images should be retained for no longer than the retention periods specified in this policy.

7 VIEWING IMAGES

7.1 As a general rule, CCTV images should only be viewed and accessed by authorised members of staff. Other staff and third parties (such as the police) should only be allowed to view the images where it is necessary in connection with the purposes set out above or as otherwise permitted in this Policy. The mere act of viewing is a processing activity that is subject to the Practice's subject access request and general GDPR compliance.

7.2 The following rules apply to the viewing of CCTV images:

i. the viewing of live images on monitors should be restricted to an authorised operator of the CCTV system;

ii. recorded images should be viewed in a restricted area (e.g. a designated secure office). Access to this area should be restricted whilst the viewing is taking place; and

iii. a CCTV system must not record images from areas that individuals would expect to be private (e.g. shower rooms or toilets).

7.3 When a duly request is received (in writing) and it is necessary to allow other members of staff, or a third party (such as the police) to view the CCTV images, a record should be made of the following:

i. the date of the written request;

ii. the date and time of the viewing;

iii. the name of the person viewing the images and the organisation he or she represents;

iv. the reason for the viewing;

v. the basis upon which the viewing was allowed i.e. the lawful processing ground relied on under Article 6 GDPR; and

vi. the outcome, if any, of the viewing.

7.4 The police can request and receive a copy of a CCTV footage but it must be in accordance with Section 19 of the Police and Criminal Evidence Act (1984) which states that they can have it if they presents that "it is evidence in relation to an offence which they are investigating or any other offence".

8 RETENTION

8.1 CCTV images held on the hard drive of a PC or server will be overwritten on a recycling basis once the drive is full, and in any event will not be held for more than necessary except where they need to be retained longer for evidential purposes.

8.2 In such cases the images will be stored on removable media and will be held securely by the Practice Manager until such time as handed over to the police or other authorised body.

8.3 It is the responsibility of the Practice Manager to ensure that images stored on removable media such as CDs is securely disposed once the purpose of the recording is no longer relevant.

8.4 Alternatively, data recorded by the CCTV system may be stored digitally using a cloud computing system.

8.5 Data from CCTV cameras will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. In all other cases, recorded images will be kept for no longer than 90 days. We will maintain a comprehensive log of when data is deleted.

8.6 At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

9 COVERT RECORDING

9.1 The Practice will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

9.2 In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of a senior partner (or director) of the Practice and the Practice's Data Protection Officer that it is appropriate not to notify the individuals at the time of the monitoring, after consideration of the following factors;

i. the decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom

ii. members of staff and any other health professional would have been given prior warning that in certain circumstances covert surveillance would be undertaken by Practice (for example in the staff's handbook or contract);

iii. the purpose for the monitoring must be in respect of identified and specific criminal activity;

iv. the monitoring must be necessary in order to obtain evidence of that criminal activity;

v. the use of signage must be likely to prejudice the purposes for the covert monitoring (i.e. the success of obtaining evidence of a criminal activity);

vi. the covert monitoring should only take place over a specific time period and should not continue after that time period has expired or the investigation has ended;

vii. any monitoring which is likely to be oppressive must be limited (e.g. an individual's office) unless there are overriding reasons for doing so;

viii. covert monitoring must not be used in areas where individuals expect privacy (such as toilets) unless there is a real suspicion of serious crime and with guidance from the police;

ix. the risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision. Should there be any risk that innocent members of staff or members of the public would be recorded (due to the area of coverage for example) there must be signage to indicate that the premises is under surveillance;

x. any information that is not relevant to the main purpose of the covert monitoring (i.e. detecting and preventing criminal activities and unlawful acts) should be disregarded and, where possible, deleted.

9.3 Any such monitoring will only be carried out for a limited and reasonable amount of time consistent with the objectives of the monitoring and only for a specific illegal activity. All such occasions will be fully documented showing when and why the decision was made by the Director/senior partner concerned.

10 PROCESSORS

10.1 Any third party appointed on behalf of the business to collect information about individuals will be a 'processor'. For example, we may hire an external organisation to maintain our CCTV system, or to edit images on our behalf, or to carry out covert monitoring under certain (limited) circumstances.

10.2 The GDPR requires us to comply with the following requirements whenever we use a processor:

i. we must put in place a data sharing agreement with such third party under which they agree to process personal data only in accordance with our instructions;

ii. the agreement must set out the security obligations with which the processor must comply; and

iii. the agreement must also include provisions dealing with the confidentiality of personal data, including ensuring the processor's staff respect confidentiality and restrictions on the appointment and use of sub-processors or transfer of the personal data.

10.3 No third party except by appointment will have the authority to install CCTV o the Practice's premises. Patients or staff members are not permitted under any circumstances to install CCTV on any of our properties for legal reasons which include protection of individual's privacy and human rights.

11 DISCLOSURE OF IMAGES

11.1 In certain circumstances it may be necessary to disclose the CCTV images to a third party, such as the police. The disclosure is likely to involve the physical delivery of the images or copies to the third party (e.g. on a disk or by email). Disclosures to third parties must be consistent with the purposes set in this Policy. Any disclosure of images must be approved by the relevant manager following a written request and approval of the Practice Manager.

11.2 Disclosures are permitted in the following circumstances:

i. Crime prevention or detection purposes - where the disclosure is requested for the purpose of preventing or detecting crime, apprehending or prosecuting offenders, or assessing or collecting tax (the crime and taxation purposes). The third party making the request must:

a) justify its request for the CCTV images;

b) confirm that a failure to make the disclosure would be likely to prejudice any of the crime or taxation purposes; and

c) put their request in writing, signed by a suitably senior person.

ii. Statutory or other legal obligation - the disclosure of the images may be required under statute (other than under the GDPR) or may otherwise be legally required (e.g. under a court order). In this situation:

a) we must disclose the CCTV images if the statutory provision imposes upon us a **mandatory** duty to disclose or a court order requires disclosure;

b) we can choose whether to disclose the CCTV images if the statutory provision imposes upon us a **discretion** as to whether or not to disclose; and

c) any decision to disclose must be authorised by the manager following notification of the Practice's DPO of such request.

11.3 In limited circumstances it may also be possible to make a disclosure where it is necessary for the purpose of establishing, exercising or defending legal rights, obtaining legal advice or in connection with legal proceedings. This covers not just our legal rights but also those of third parties.

11.4 A record should be kept of all requests for disclosure of CCTV images, together with any reasons for refusing a request. If a disclosure is approved and CCTV images are disclosed to a third party, a record should be made of the following:

i. the date the written request was received

ii. the date and time of the disclosure;

iii. the name of the person to whom the disclosure is made and the organisation he or she represents;

iv. the reason for the disclosure and the images disclosed;

v. the basis upon which the disclosure was made (by reference to the GDPR);

vi. the location where the images are to be kept;

vii. the outcome, if any, of the disclosure;

viii. the date and time the images were returned (if applicable); and

ix. if the disclosure is to the police, record any crime incident number to which the images relate and ask the collecting police office to sign for the images when they are handed over.

11.5 Where a decision has been made to disclose CCTV images, the disclosure must be made securely so that the images are received by the intended recipient. For example, where a wireless transmission system is used to disclose the images, sufficient safeguards must be put in place to protect the transmission from being intercepted in transit (e.g. encryption).

12 INDIVIDUAL ACCESS RIGHTS BY DATA SUBJECTS

12.1 The GDPR gives individuals (data subjects) the right to access personal information about themselves, including CCTV images.

12.2 All requests for access to images by data subjects (when they are asking for access to images of themselves) should be made in writing to Practice for the attention of the Practice Manager in line with the Practice's subject access request procedure (SAR).

12.3 The Practice Manager responsible for the system will liaise with the Practice's DPO to determine whether disclosure of the images will reveal third-party information.

12.4 Requests for access to CCTV images must include sufficient information to enable Practice to identify:

i. The date and time when the images were recorded;

ii. The location of the CCTV camera; and

iii. Further information to identify the individual, if necessary

12.5 No fee is payable for disclosure which will be in accordance with Practice's Subject Access Request Procedure.

12.6 Waterfield House Surgery is required by the GDPR to respond promptly and at the latest within one month of receiving the request or if later, sufficient information to identify the images requested.

12.7 If Waterfield House Surgery cannot comply with the request, the reasons must be documented. The requester will be advised of these in writing. A refusal to comply is only permitted in limited circumstances (see our Subject Access Request Procedure).

12.8 Decisions regarding the disclosure of information following a request from a data subject will be made and communicated to the requester in accordance with Practice's Subject Access Request Procedure.

13 PERIODIC REVIEW

13.1 The Practice Manager will carry out an annual review of the continued justification for and effectiveness of the CCTV system in operation within our business in fulfilling the purposes in this Policy and general compliance with this Policy.

13.2 This policy will be reviewed every 2 years; or on account of any relevant changes in law or guidance from the Information Commissioner.

13.3 We may carry out checks or audits from time to time to ensure that the requirements of this Policy are being followed.

14 CONTACTS

14.1 If you have any queries about this Policy, please contact the Practice Manager.

15 COMPLAINTS

15.1 Complaints and enquiries about the operation of The Wells Medical Centre's CCTV systems should ideally be made in writing in the first instance to those having day-to-day responsibility as specified in section 8. If a complainant is not satisfied with the response received, they should write to the Data Protection Officer of Waterfield House Surgery. Complainants can also make a complaint directly to the Information Commissioner's Office at www.ico.org.uk or by calling 0303 123 1113.