WBHC CCTV Policy

Document Control

A. Confidentiality Notice

This document and the information contained therein is the property of West Byfleet Health Centre – *CCTV Data Controller.*

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 the *CCTV Data Controller*.

B. Document Details

Classification:	POLICY
Author and Role:	*CCTV Data Controller – (*NHS tri-practice data Lead)
Organisation:	Shared Services & Site Support – Wey Family, Parishes Bridge, Madeira Medical
Document Reference:	Caldicott
Current Version Number:	6
Approved By:	Practices, PCN, & Shared Services, management
Date Approved:	03/07/24

C. Document Revision and Approval History

Version	Date	Version Edited By:	Version Approved By:	Comments
1	26/01/2022	BN	Shared manager	Initial draft after DPIA
2	07/03/2022	BN	Shared manager	Review with management
3	08/06/2022	BN	Shared Manager	CCG IG comments incorporated
4	01/10/2022	BN	Shared Manager	Review after completing LIA
5	26/06/2023	BN	Shared Manager	Yearly review
6	26/06/2024	BN	Shared Manager	Yearly review

WBHC GP Shared Services & Support office operates common resources on behalf of the NHS GP Practices at West Byfleet Health Centre: *Madeira Medical, Parishes Bridge Medical Practice, and Wey Family Practice.*

The CCTV *Data Controller /IG lead* roles fall within this remit and thus subsequent references to *CCTV Data Controller* cover these roles responsibilities.

Contents:

We comply with the 12 principles listed in the surveillance camera code of practice issued by the Home Office: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice.

We also comply with In the picture: A data protection code of practice for surveillance cameras and personal information issued by the Information Commissioner's Office https://ico.org.uk/media/1542/cctv-code-of-practice.pdf.

1 Purpose and scope

1.1 WBHC use closed circuit television (CCTV) to provide a safe and secure environment for staff, visitors, & customers, and to protect property. This policy relates to the use and management of CCTV throughout the premises.

1.2 This policy sets out the accepted use of the CCTV equipment and images to ensure compliance with relevant data protection and privacy laws including: the General Data Protection Regulation, (UK) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018) (together referred to as the 'Data Protection Legislation'), The Surveillance Camera Code of Practice 2021, and related laws including but not limited to, the Human Rights Act 1998 (all referred to collectively in this policy as the CCTV Laws).

1.3 This policy has been produced in line with the Information Commissioner's Office (ICO) CCTV Code of Practice. This policy should be read alongside our Data Privacy Policy, which is available on request.

1.4 We reserve the right to change this policy at any time.

2 Your responsibility to comply with this policy

2.1 Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to the *CCTV Data Controller*.

2.2 All staff including but not limited to employees, workers, contractors, self-employed consultants and agency workers must comply with this policy and any document referenced in it. We take compliance with this policy very seriously. Failure to comply with the policy puts at risk the individuals whose personal information is being processed, carries the risk of significant civil and criminal sanctions for the individual and for us, and may, in some circumstances, amount to a criminal offence by the individual.

2.3 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. Non-employees, such as contract staff and consultants may have their contract terminated with immediate effect.

3 Data transfer

3.1 We do not allow personal data to be transferred to a person or entity (whether a group company or a third party) located outside the UK without the prior written approval of *CCTV Data Controller*. We may transfer personal information outside the EEA only on the basis that that country, territory or organisation is designated as having an adequate level of protection.

4 Why we use CCTV

4.1 We have considered and determined that the purposes for which the CCTV is deployed are legitimate, reasonable, appropriate and proportionate. For ease of reference, CCTV systems are deployed at our premises at our health centre in West Byfleet for the following purposes and on the legal basis of our legitimate interest. We have installed CCTV systems to:

4.1.1 deter crime and assist in the prevention and detection of crime and/or serious breaches of policies and procedures;

4.1.2 assist with the identification, apprehension and prosecution of offenders; and

4.1.3 monitor security and health and safety at our premises.

4.2 The CCTV system will NOT be used:

4.2.1 to record sound;

4.2.2 for any automated decision taking; or

4.2.3 monitoring private and/or residential areas or premises.

4.3 Before installing and using CCTV systems on our premises, we:

4.3.1 assessed and documented the appropriateness of and reasons for using CCTV;

4.3.2 established and documented who is responsible for day-to-day compliance with this policy; and

4.3.3 ensured signage is displayed to inform individuals that CCTV is in operation, and that CCTV operations are covered in appropriate policies;

4.4 We keep a record of the CCTV installed and used.

4.5 Reviews are regularly undertaken to ensure that the use of the CCTV systems and the processing of the personal data obtained through it remains justified.

5 Covert recording and monitoring of staff

5.1 All cameras in use are highly visible in conspicuous locations and signage notifies site users of their operation.

5.2 Cameras are not used inside the building, and will not be used to monitor staff performance, job efficiency, or work related grievances unless related to a crime being investigated.

6 Positioning cameras

6.1 We will make every effort to position cameras to ensure they only cover our premises. No cameras will focus on residential or private accommodation or property. Camera operators will receive training and access to written procedures for maintaining and respecting the privacy of neighbours (business and residential), staff and customers.

6.2 Cameras will not be hidden from view and must be sited in such a way as to ensure that they only monitor spaces intended to be covered.

6.3 The installation of cameras in areas in which individuals would have an expectation of privacy will not be authorised under this policy, unless there are exceptional circumstances, and subject to approval by the *CCTV Data Controller*.

6.4 We will clearly display signs in the vicinity of the cameras so that staff, visitors and customers/clients are aware they are entering an area covered by CCTV.

6.5 Our CCTV signs will state:

6.5.1 that we are responsible for the CCTV recording;

6.5.2 the legal purpose(s) of the CCTV recording and how recordings may be used;

6.5.3 how long recordings will be kept;

6.5.4 that individuals can access recordings; and

6.5.5 contact details for queries regarding the CCTV scheme.

6.6 If neighbouring domestic areas are included in the camera view, the occupants of the property should be consulted prior to any recording and the purposes of the recording explained. We will take reasonable steps to minimise the impact of recording.

7 Image quality

7.1 Images produced by the equipment must be as clear as possible so that they are effective. To achieve this:

7.1.1 the equipment be properly installed, serviced, checked and maintained (and maintenance logs maintained) to ensure it works properly;

7.1.2 any recording media, if needed, will be of good quality and will be replaced if the quality of the images has begun to deteriorate;

7.1.3 where time/date of images are recordable the equipment will be set accurately and this will be regularly checked and documented;

7.1.4 cameras will be correctly positioned;

7.1.5 assessments will be made as to whether constant real-time recording is necessary, or if recording can be limited to those times when suspect activity is likely to occur;

7.1.6 cameras will be protected from vandalism so far as is possible; and

7.1.7 if cameras break down or are damaged, The *CCTV Data Controller* is responsible for arranging timely repair.

8 Data and image retention

8.1 Images and recording logs must be retained and disposed of in accordance with our Data Retention Schedule. Images stored on removable media will similarly be erased or destroyed once the purpose of the recording is no longer relevant. Data will only be retained for legal and/or compliance reasons in accordance with the relevant retention and disposal of data policies.

8.2 For digital recording systems, 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 unless authorised by the *CCTV Data Controller*, will not be held for more than 30 days. If images are retained longer than this, the reason(s) will be recorded in the CCTV register.

8.3 Where a request to retain information is authorised, reasonable steps will be taken to safeguard any footage which may otherwise be deleted.

8.4 All digital recordings will be password protected [if relevant, set out summary of any other security measures as well]. Recording media no longer in use will be securely destroyed. Where images have been authorised to be used for legal reason, the footage must be retained securely.

9 Access to images

9.1 Staff images

9.1.1 Images will only be accessed if a serious event occurs that will need reporting to the police; such as criminal activity, fraud, gross misconduct, or behaviour that puts others at risk.

9.1.2 Access to recorded images will be restricted only to the *CCTV Data Controller* on explicit request in relation to a reported incident, and will not be made more widely available. The request, date, time and the reason for authorisation for release of images and CCTV footage will have to be recorded by the *CCTV Data Controller* for audit purposes on a CCTV register. Requests must be approved by the *CCTV Data Controller* will make the necessary access arrangements.

9.1.3 The following information must be kept on a CCTV register maintained for that purpose and held by the *CCTV Data Controller* when media are removed for viewing:

(a) the date and time they were viewed or removed;
(b) the name of the person viewing/removing the media;
(c) the name(s) of the person(s) viewing the images including the department to which the person viewing the images belongs or, if they are from an outside organisation, the organisation's name (eg the police);
(d) the reason for viewing the images; and
(e) the date and time the media were returned to the system or secure storage (if applicable).

9.1.4 Viewing of recorded images will take place in a restricted or secure area to which other members of staff will not have access while viewing is occurring. Images retained for evidence will be securely stored with limited access for authorised staff only.

9.2 Access to and disclosure of images to third parties will only be granted to the police or similar authority

9.2.1 Access to and disclosure of images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are protected, and also ensure that the images can be used as evidence if required. Images may only be disclosed in accordance with the purposes for which they were originally collected. Our *Data Privacy Policy* and *Data Retention Guidelines* should also be consulted in relation to the capture, storage, access to and disposal of personal data, in this case images of an identifiable individual.

9.2.2 Disclosures to third parties will only be made in accordance with the purpose(s) for which the system is used and will be limited to:

(a) police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder;
(b) prosecution agencies (such as the Crown Prosecution Service);
(c) relevant legal representatives of people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings);
(d) individuals who have been caught on our CCTV in accordance with a request made such as one described at 11 below;
(e) in exceptional cases, for others (such as insurers) to assist in identification of a victim, witness or perpetrator in relation to a criminal incident;

9.3 If a police officer requests images from our CCTV system in relation to an investigation that has not been initially reported by the business, then please refer them to the *CCTV Data Controller*. It may be that we are required to disclose the images or we have a discretion whether to do so.

10 Disclosure

10.1 The *CCTV Data Controller* is the only entity who can authorise disclosure of information to the police or other law enforcement agencies. All requests for disclosure should be documented for audit purposes in the CCTV register. If disclosure is denied, the reason should also be recorded in the CCTV register.

10.2 Before any images are disclosed the following must be recorded in the CCTV register:

10.2.1 if the images are being removed from the CCTV system or secure storage to another area, the location to which they are being transferred;

10.2.2 the method of disclosure (encrypted USB, EGRESS, SECURE email etc)

10.2.3 any crime incident number, if applicable; and

10.2.4 the signature of the person to whom the images have been transferred.

11 SAR - Subject access rights to individuals' own data

11.1 The GDPR gives individuals the right to access personal data about themselves, including CCTV images and footage. All requests for access to images by any individual (when they are asking for access to images of themselves) should be addressed to the *CCTV Data Controller* in the *Support office* in a written format, such as email or letter to the health centre postal address.

11.2 Requests for access to CCTV images/footage must be made in writing and must include:

11.2.1 the full name and address of the person making the request (the 'data subject');

11.2.2 Proof of identity such as passport

11.2.3 a description of the data subject and/or details of what they were wearing to ensure

we can locate the individual, and only relevant images are disclosed;

11.2.4 the approximate date and time when the images were recorded to allow for

searching;

11.2.5 the location where the images were recorded.

11.3 Requests from an individual for CCTV images or footage must be handled, and responded to, in accordance with our data *subject access request* procedure.

11.4 If we cannot comply with the request, the reasons for not being able to comply will be documented and the data subject will be advised of these in writing by the *CCTV Data Controller.*

11.5 The *CCTV Data Controller* is responsible for the CCTV system and will liaise with relevant authorities to determine whether disclosure of the images will reveal third-party information.

11.6 Particular care should be exercised when images of other people are included in the materials for disclosure. Images of other individuals will, if possible, be redacted unless there would be an expectation that their images would be released in such circumstances. Non-disclosure will be appropriate in most circumstances. If there is any doubt about what information must be provided to enquirers, please contact the *CCG IG lead* or *DPO* for advice.

11.7 Requests to restrict processing and objections to processing:

11.7.1 The GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data. The GDPR also gives individuals the right to object to the processing of their personal data in certain circumstances.

11.7.2 All such requests should be addressed in the first instance to the *CCTV Data Controller*, who will provide a written response within one month of receiving the request, setting out their decision on the request. A copy of the request and response will be retained for an appropriate period determined on a case-by-case basis.

12 Responsibility for CCTV systems and staff training

12.1 The *GP Shared Services & Support office* has nominated the *CCTV Data Controller* to assist with the day-to-day responsibility of the systems and the training of staff responsible for operating or administering CCTV. However, the overall responsibility lies with *CCTV Data Controller*.

13 Complaints

13.1 Complaints and enquiries about the operation of our CCTV systems should be made by staff in line with the practices grievance procedure or, by clients and visitors, under our complaints procedure, available upon request and on our website.

13.2 Enquiries relating to GDPR or CCTV Laws should be addressed to the *CCTV Data Controller*. If a member of staff believes that there has been a breach of the GDPR or any CCTV Laws they must contact either their own Practice Manager or the *CCTV Data Controller* as a matter of urgency in accordance with the data breach reporting process set out in our *Data Privacy Policy*. If a complainant or enquirer is not satisfied with the response received, they can write to the ICO. Details of how to do this can be found on the ICO website: http://www.ico.org.uk./

14 Enforcement and compliance

14.1 All authorised users of our surveillance technology and its underlying data are required to adhere to the controls around the use of CCTV as set out in this policy and as may be advised separately from time to time. The use of the CCTV system for any purpose other than those specifically authorised will be subject to a full investigation and could lead to disciplinary action up to and including dismissal without notice.

14.2 The misuse of our surveillance systems and unauthorised use of images and CCTV footage may constitute a criminal offence.

14.3 Any concerns regarding the use of CCTV should be shared with your line manager or, if you are not comfortable with escalating concerns via your line manager, in accordance with the NHS Whistleblowing Policy: https://www.england.nhs.uk/ourwork/whistleblowing/