

# CCTV Policy

## Overview

This CCTV system and the images produced by this practice are controlled by: <INSERT NAME> who is responsible for how the system is used under the UK GDPR and Data Protection Act 2018.

We, Pav Dental, have considered the need for using CCTV and have decided it is necessary for the prevention and detection of crime and for protecting the safety of individuals, or the security of premises. We will not use the system for any incompatible purposes, and we conduct regular reviews of our use of CCTV to ensure that it is still necessary and proportionate.

Closed Circuit Television (CCTV) is installed at the practice premises for the purposes of staff, patient, and premises security. Cameras are located at various places on the premises, and images from the cameras are recorded. The use of CCTV falls within the scope of the GDPR.

Under the UK GDPR and DPA 2018, we have an obligation to implement appropriate technical and organizational measures. These show that we have considered and integrated the principles of data protection law into our processing activities. It is also important that we identify an appropriate lawful basis, and justify any processing to be necessary and proportionate.

The accountability principle requires us to take responsibility for what we do with personal data and how we comply with the other principles. We must ensure we have appropriate measures and records in place to be able to demonstrate our compliance.

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

For surveillance systems, we must 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; or
- Monitoring individuals at a workplace.

We will continue to regularly assess whether our use of surveillance is appropriate in the circumstances. As part of our assessment, we take into account the reasonable expectations of the individuals whose personal data are processed and the potential impact on their rights and freedoms.

We will record our 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 ICO is required.

In order to comply with the requirements of the GDPR, data must be:

- Fairly and lawfully processed
- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant, and not excessive
- Accurate
- Not kept for longer than is necessary
- Processed in accordance with individuals' rights
- Secure

## **Data Protection Statement**

CCTV is installed for the purpose of staff, patient, and premises security. Access to stored images will be controlled on a restricted basis within the practice.

Use of images, including the provision of images to a third party, will be in accordance with the practice's Data Protection registration.

CCTV may be used to monitor the movements and activities of staff and visitors whilst on the premises. CCTV images may be used where appropriate as part of staff counselling or disciplinary procedures.

External and internal signage are displayed on the premises and in the practice leaflet stating the presence of CCTV and indicating the names of the Data Controllers and a contact number during office hours for enquiries.

## **Retention of Images**

Images from cameras are recorded on videotape/disc/computer system ("the recordings"). Where recordings are retained for the purposes of security of staff, patients, and premises, these will be held in secure storage and access controlled. Recordings which are not required for the purposes of security of staff, patients, and premises, will not be retained for longer than is necessary (state retention period, e.g., 8 weeks).

The system has/has not got an automatic power backup facility which may operate in the event of a main supply power failure.

## **Access to Images**

It is important that access to, and disclosure of, images recorded by CCTV and similar surveillance equipment 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.

## **Access to Images by Practice Staff**

Access to recorded images is restricted to the Data Controllers, who will decide whether to allow requests for access by data subjects and/or third parties (see below). Viewing of images must be documented as follows:

- The name of the person removing from secure storage, or otherwise accessing the recordings
- The date and time of removal of the recordings
- The name(s) of the person(s) viewing the images (including the names and organizations of any third parties)
- The reason for the viewing
- The outcome, if any, of the viewing
- The date and time of replacement of the recordings

## **Removal of Images for Use in Legal Proceedings**

In cases where recordings are removed from secure storage for use in legal proceedings, the following must be documented:

- The name of the person, their job role and organization, removing from secure storage, or otherwise accessing the recordings
- The date and time of removal of the recordings
- The reason for the removal
- Specific authorization of removal and provision to a third party
- Any crime incident number to which the images may be relevant
- The place to which the recordings will be taken
- The signature of the collecting police officer, where appropriate
- The date and time of replacement into secure storage of the recordings

## **Access to Images by Third Parties**

Requests for access to images will be made using the ‘Application to access to CCTV images’ form (see below).

You must ensure that any disclosure of information to third parties from your surveillance system is controlled and that the disclosure itself is consistent with the purpose(s) for which you set up the system. For example, in most cases, it is appropriate to disclose video surveillance information to law enforcement when the purpose of the system is to contribute to the prevention and detection of crime. Unless a court order applies, this is not a legal requirement and is often voluntary.

You should note that even if your surveillance system was not established to prevent and detect crime, it is still acceptable to disclose information to law enforcement agencies if relevant. Failure to do so could prejudice an ongoing investigation.

Example: An assault takes place in a nightclub and the event is captured on CCTV, which is installed inside the premises for public safety and crime prevention.

The local police force requested a copy of the footage from the nightclub owner to investigate the incident. When satisfied by the request, the nightclub owner can efficiently review and retrieve the captured footage and provide a specific clip of the incident to the police to assist in the ongoing investigation.

The data controller will assess applications and decide whether the requested access will be permitted. The release will be specifically authorized. Disclosure of recorded images to third parties will only be made in limited and prescribed circumstances. For example, in cases of the prevention and detection of crime, disclosure to third parties will be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies
- Relevant legal representatives
- The press/media, where it is decided that the public's assistance is needed to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be considered
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)

All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented as above.

## **Disclosure of Images to the Media**

If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of other individuals must be disguised or blurred so that they are not readily identifiable. If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out. If an editing company is used, then the data controller must ensure that there is a contractual relationship between them and the editing company, and:

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images.
- The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the data controllers.
- The written contract makes the security guarantees provided by the editing company explicit.

## **Access by Data Subjects**

Requests for access to images will be made using the 'Application to access to CCTV images' form (see below). Individuals should also be provided with the CCTV Policy and Code of Practice leaflet which describes the type of images which are recorded and retained, the purposes for which those images are recorded and retained, and information about the disclosure policy in relation to those images.

## **Procedures for Dealing with an Access Request**

All requests for access by Data Subjects will be dealt with by the Registered Manager.

- The data controller will locate the images requested.
- The data controller will determine whether disclosure to the data subject would entail disclosing images of third parties.
- The data controller will need to determine whether the images of third parties are held under a duty of confidence. In all circumstances, the practice's indemnity insurers will be asked to advise on the desirability of releasing any information.
- If third-party images are not to be disclosed, the data controllers will arrange for the third-party images to be disguised or blurred.
- If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out.
- The Registered Manager will provide a written response to the data subject within 21 days of receiving the request setting out the data controllers' decision on the request.
- A copy of the request and response should be retained.

## **Assessing Compliance**

We will commit to regularly completing the CCTV Compliance audit checklist to ensure we remain compliant with data protection considerations. A copy of this can be found in the DCME portal.

## **Complaints**

Complaints must be in writing and addressed to the Registered Manager. Where the complainant is a third party, and the complaint or enquiry relates to someone else, the written consent of the patient or data subject is required. All complaints will be acknowledged within 3 days, and a written response issued within 14 days.

## **GDPR – Application for CCTV Data Access**

All sections must be fully completed. Attach a separate sheet if needed.

- Name and address of Applicant, including job role and organisation
- Name and address of "Data Subject" – i.e., the person whose image is recorded
- If the data subject is not the person making the application, please obtain a signed consent from the data subject opposite Data Subject signature .....
- If it is not possible to obtain the signature of the data subject, please state your reasons
- Please state your reasons for requesting the image
- Date on which the requested image was taken.
- Time at which the requested image was taken.
- Location of the data subject at the time the image was taken (i.e. which camera or cameras.)
- Full description of the individual, or alternatively, attach to this application a range of photographs to enable the data subject to be identified by the operator.
- Please indicate whether you (the applicant) will be satisfied by viewing the image only.
- On receipt of a fully completed application, a response will be provided as soon as possible, and in any event within 21 days.

**Practice Use Only**

- Access granted (tick)
- Access not granted (tick) Reason for not granting access:
- Data Controller's name: Signature:
- Date:

**Approved By:** Hassan Bhojani