
CCTV Policy

Municipal and Owen Carter Almshouse Charity

Bree Norton-Smith - 26 September 2023

The term 'premises' includes offices and all sites and estates owned or controlled by The Municipal and Owen Carter Almshouse Charity (MOC).

1. Purpose and aim of the Policy

- 1. We use closed circuit television (CCTV) images to help provide a safe and secure environment for employees, residents and for visitors to our premises, such as clients, customers, contractors and suppliers, and to protect our property.
- 2. This policy sets out the use and management of the CCTV equipment and images in compliance with the Data Protection Act 2018 and the CCTV Code of Practice.
- 3. Our CCTV facility record images only. There is no audio recording ie conversations are not recorded on CCTV (but see the section on covert recording).

2. Purposes of CCTV

The purposes of our installing and using CCTV systems include:

- Provide reassurance to our residents.
- Assist in the prevention or detection of crime or equivalent anti-social behaviour and provide evidence of the same.
- Assist in the identification and prosecution of offenders.
- Monitor the safety and security of our premises.
- Help ensure that health and safety rules and our procedures are being complied with.
- Assist with the identification of unauthorised actions or unsafe working practices that might result in disciplinary or training proceedings being instituted against employees and to assist in providing relevant evidence.

3. Location of cameras

Cameras are located at strategic points throughout our premises, principally at the main entrance and exit points. We have positioned the cameras so that they cover communal or public areas on our premises and they have been sited so that they provide clear images.

No camera focuses, or will focus, on toilets, shower facilities, changing rooms, staff kitchen areas, staff break rooms or private offices.

All cameras (with the exception of any that may be temporarily set up for covert recording) are also clearly visible.

Appropriate visible and readable signs are prominently displayed so that employees, clients, customers and other visitors are aware they are entering an area covered by CCTV.

4. Recording and Retention of Images

- 4.1. Images produced by the CCTV equipment are intended to be as clear as possible so that they are effective for the purposes set out above.
- 4.2. Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly and that the media is producing high quality images.
- 4.3. Images may be recorded either in constant real-time (24-hours a day throughout the year), or only at certain times, as the needs of the business dictate.
- 4.4. As the recording system records digital images, any CCTV images that are held on the hard drive of a PC or server are deleted and overwritten on a recycling basis and, in an event, are not normally held for more than one week. Once a hard drive has reached the end of its use, it will be erased prior to disposal.
- 4.5. Images that are stored on, or transferred to a removable media are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of one month. However, where a law enforcement agency is investigating a crime, images may need to be retained for a longer period.

5. Access to and disclosure of images

Access and disclosure of images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected.

The images that are filmed are recorded centrally and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system and to those line managers who are authorised to view them in accordance with the purposes of the system.

Viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing is occurring. If media on which images are recorded are removed for viewing purposes, this will be documented.

Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

- The police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.

- Prosecution agencies, such as the Crown Prosecution Service.
- Relevant legal representatives.
- Line managers involved with our disciplinary and performance management processes.
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

The Chief Executive (CEO) is the only persons permitted to authorise disclosure of images to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

6. Individual Right to Access

- 6.1. Under the Data Protection Act 2018 (GDPR); Individuals have the right on written request to receive a copy of the personal data that we hold about them, including CCTV images if they are recognisable from the image.
- 6.2. If you wish to access any CCTV images relating to you, you must make a written request to our Data Protection Officer (CEO). Your request must include the date and approximate time when the images were recorded and the location of the particular CCTV camera, so that the images can be easily located and your identity can be established as the person in the images. We will respond promptly and in any case within 28 days of receiving the request.
- 6.3. We may not have any CCTV images given that images as they are normally held for more than one week (see section 4.4.).
- 6.4. We will always check the identity of the person making the request before processing it.
- 6.5. The Data Protection Officer (CEO) will first determine whether disclosure of your images will reveal third party information as you normally have no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.
- 6.6. If MOC is unable to comply with your request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, you will be advised accordingly.

7. Covert Recording

MOC will only undertake covert recording with the written authorisation of the Chief Executive & Chairman of the Board of Trustees, where there is good cause to suspect that criminal activity or equivalent anti-social behaviour or malpractice is

taking, or is about to take, place and informing the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection.

- 7.1. Covert monitoring may include both video and audio recording.
- 7.2. Covert monitoring will only take place for a limited and reasonable amount of time consistent with the objective of assisting in the prevention and detection of particular suspected criminal activity or equivalent anti-social behaviour or malpractice. Once the specific investigation has been completed, covert monitoring will cease.
- 7.3. Information obtained through covert monitoring will only be used for the prevention or detection of criminal activity or equivalent antisocial behaviour or malpractice. All other information collected in the course of covert monitoring will be deleted or destroyed unless it reveals information which Eventide cannot reasonably be expected to ignore.

8. Drones

- 8.1. Permission, in writing, must be granted by the Charity to operate a Drone on site.
- 8.2. Drone use is used to assist us in detecting and diagnosing maintenance issues. For example, we might do so to examine the roofs of high buildings that might otherwise require the expense, inconvenience and potential dangers associated with scaffolding being erected to carry out our investigations.
- 8.3. Permitted Drone users are governed by the Civilian Aviation Authority. Any permitted Drone User will hold a valid flyer ID and operator ID and will have completed the Charity's approved contractor process.

9. Staff training

9.1. We will ensure that all employees handling CCTV images or recordings are trained in the operation and administration of the CCTV system and on the impact of the Data Protection Act 2018 with regard to that system.

10. Implementation

10.1. Our Chief Executive is responsible for the implementation of, and compliance with, this policy and the operation of the CCTV system and will conduct a regular review of our use of CCTV. Any complaints or enquiries about the operation of our CCTV system should be addressed to us.