Cottington Close RMO CCTV Policy and Procedures

1. INTRODUCTION

1.1 The purpose of this Policy is to regulate the management, operation and use of the Closed Circuit Television (CCTV) system at Cottington Close Estate, SE11. Cameras are used to monitor activities within Estate buildings, on its sites, its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the residents, staff, and visitors.

1.2 CCTV monitoring and recording systems will only be installed in or on CCRMO property when this has been reviewed and approved by the CCRMO Board.

1.3 The system comprises a number of fixed and fully functional (Pan/Tilt/Zoom) cameras located in buildings and externally around the Estate, and in public areas of the CCRMO offices. These are monitored by appropriate personnel.

1.4 CCRMO's use of CCTV complies with the requirements of the Data Protection Act and, where applicable, the Regulation of Investigatory Powers Act 2000.

1.5 This policy document will be subject to review annually to include consultation as appropriate with interested parties.

1.6 The CCTV system is owned by CCRMO.

2. OBJECTIVES OF THE CCTV POLICY

2.1 The objectives of the CCTV Policy are to:

(a) Protect Cottington Close Estate residents' and RMO property.

(b) Ensure a safer environment at Cottington Close.

(c) Support the Police in a bid to deter and detect crime, by providing evidence in support of an enquiry or prosecution.

3. OPERATION OF THE CCTV SYSTEM

3.1 Management of the system

3.1.1 The CCTV operating system will be administered and managed by the Estate Supervisor in accordance with the principles and objectives expressed in CCRMO policy documents.

3.1.2 The day-to-day management will be the responsibility of the CCRMO Manager during the working week.

3.1.3 All cameras are monitored only by authorised personal on computers within the CCRMO office.

3.1.4 The CCTV system is operated 24 hours a day, 365 days of the year.

3.1.5 Maintenance and emergency maintenance are provided by a duly authorised contractor.

3.1.6 Emergency procedures will be used when it becomes necessary to call the Emergency Services.

3.1.7 Warning signs, as required by the Code of Practice of the Information Commissioner, will be placed at all access routes to areas covered by the Estate's CCTV cameras.

3.1.8 Liaison meetings may be held with all bodies involved in the support of the system.

3.2. System control - Monitoring procedures:

On a daily (weekdays) basis a member of the Estate Team will check and confirm the efficiency of the system, ensuring that:

- the cameras are functional
- the equipment is properly recording

3.2.2 Access to the CCTV System is strictly limited to the Estate Supervisor, CCRMO Manager and specific authorised persons. Unauthorised persons are not permitted to view live or pre-recorded footage.

3.2.3 Only staff who are trained in the system's use and familiar with the policy will operate the system.

3.2.4 Viewing screens are based within an 'Authorised Personnel Only' locked room at the CCRMO offices. When not being used, screens will be closed as a further safeguard against misuse of the monitoring system.

3.2.5 Unless an immediate response to events is required, Authorised Users must not re-direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained from the CCRMO Manager or a Police Officer, for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

If covert surveillance is planned or has taken place, copies of the written authorisation, including any review or cancellation, must be returned to the CCRMO Manager or nominated deputy.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Recording is carried out on digital data apparatus. These are located within the 'Authorised Users Only' room at the CCRMO Offices, 1 Opal Street, SE11.

Recorded data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Recorded data will never be released to the media for purposes of entertainment.

3.3 Exemptions:

3.3.1 The CCTV system is designed to ensure maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3.4 Retention and disposal of material:

Data disks will be disposed of by a secure method. Footage will be stored on data recorder hard drives for up to 30 days.

Footage will only be stored on data disks if footage is requested by external agencies in the process of detecting crime and in the prosecution of offenders.

4. DIGITAL RECORDING PROCEDURES

4.1 Rules for retention of data

4.1.1 In order to maintain and preserve the integrity of the Digital Video Recorder (DVR), hard disks used to record events from the CCTV cameras and the facility to use them in any future proceedings, the following procedures for their use and retention of data must be strictly adhered to:

4.1.2 Each DVR must be identified by a unique mark or serial number. This is maintained by the Estate Supervisor.

4.1.3 Each DVR must be kept in a secure location with access restricted to authorised staff.

4.1.4 The Estate Supervisor or Manager will check daily to ensure the system is operational.

A disk required for evidential purposes must be of the CD-R type only, disks will be provided in pairs each carrying an identical identification number, one a Master Disk to be retained by the Estate, the other a Copy which can be released to the police or other authorised third party on production of a signed data access request form.

The disk should be loaded with the required CCTV data and viewer programme; identical information should be loaded on both Master and Copy disks.

Each disk should be sealed in its own case, the Master Copy should be kept in a secure disk storage drawer. The Copy disk is handed to the person making the request on production of positive ID such as Police Warrant Card, Picture ID Card, Driving Licence, etc.

The record sheet should then be completed and the Copy disk signed for and counter signed by the DMT.

4.2 Dealing with official requests: use of CCTV in relation to criminal investigations:

4.2.1 CCTV recorded images may be viewed by the Police for the prevention and detection of crime, authorised officers of CCRMO for supervisory purposes, discipline reasons or authorised demonstration and training.

4.2.2 A record will be maintained of the release of Data on Disk to the Police or other authorised applicants. A register will be available for this purpose.

4.2.3 Viewing of CCTV images by the Police must be recorded in writing and entered in the log book. This will be under the management of the Estate Supervisor. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.

4.2.4 Should a disk be required as evidence, a copy may be released to the Police under the procedures described in paragraph 4.1.4 of this Code. Disks will only be released to the Police on the clear understanding that the disk remains the property of CCRMO, and both the disk and information contained on it are to be treated in accordance with this policy.

4.2.5 CCRMO retains the right to refuse permission for the Police to pass to any other person the disk or any part of the information contained therein.

4.2.6 The Police may require CCRMO to retain the stored disk(s) for possible use as evidence in the future. Such disk(s) will be properly indexed and securely stored by Authorised Staff until they are needed by the Police.

4.2.7 Applications received from outside bodies (e.g. solicitors) to view or release disks will be referred to the Estate Supervisor. In these circumstances disks will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, or in response to a Court Order. A fee can be charged in such circumstances.

5. BREACHES OF THE POLICY (INCLUDING BREACHES OF SECURITY)

5.1 Any breach of the Policy will be initially investigated by the CCRMO Manager or his nominated deputy, in order for him/her to initiate the appropriate disciplinary action.

5.2 Any serious breach of the policy will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

6. ASSESSMENT OF THE SCHEME

6.1 Performance monitoring, including random operating checks, may be carried out by any Authorised Personnel.

7. COMPLAINTS

7.1 Any complaints about the CCRMO's CCTV system should be addressed to the Estate Manager, CCRMO, 1 Opal Street, SE11.

7.2 Complaints will be investigated in accordance with Section 5 of this policy.

8. ACCESS BY THE DATA SUBJECT

8.1 The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to access data held about themselves, including that obtained by CCTV. Anyone can ask to see images that are recorded of them; if approved and only of the person requesting the images in writing. We will provide the images within 40 days.

8.2 Requests for information, including Data Subject Access Requests, should be sent to: Estate Manager, CCRMO, 1 Opal Street, SE11.

Approved: October 2019

Reviewed: March 2022

Updates: None