D'EYNSFORD TENANT MANAGEMENT ORGANISATION CIC

CCTV POLICY

APPROVED BY THE BOARD ON THE
9th March 2020

CONTENTS

ABBREVIATIONS

AVI	Audio Visual Interleave
ASB	Anti-Social Behaviour
CCTV	Closed Circuit Tele Vision
CD	Compact Disc
DBS	Disclosure of Barring Service
DVRs	Digital Video Recorder Systems
DVD	Digital Versatile Disc
GDPR	General Data Protection Regulations
MPEG	Moving Picture Experts Group
PTZ	Pan Tilt Zoom
ICO	Information Commission Office
TMO	Tenant Management Organisation
TMI	Tenant Monitoring Initiative
LBS	London Borough of Southwark
SAR	Subject Access Request

1. BACKGROUND

The idea of CCTV Cameras within D'Eynsford estate has existed since the development stage of the TMO. It was in fact one of the determining factors as to the reason why some residents voted in favour (87%) of the setup of the TMO. The TMO recognised the importance residents place on CCTV and as such included CCTV as part of its business plans in 2015 and also in 2019.

Since the development of the TMO in 2015, the repeated discussion of CCTV Cameras at residents meetings has been noted with the minutes detailing these at meetings on 18th July 2016, 20th March 2017, 18th May 2018, 17th September 2019 & 13th November 2019.

A consultation with residents occurred on the 17th September 2019 regarding which Improvements works they would like to see the TMO undertake and CCTV came out as one of the highest priority projects for the TMO to carry out with the surplus money which has been accumulated through efficiency savings.

The introduction of CCTV follows a long campaign of education across the estate via various means on the subject of fly-tipping, antisocial behaviour and recycling yet issues of this sort persist along with obviously illegal/criminal activities. In assessing the impact of installing CCTV, the TMO has weighted up the potential benefits of both the deterrent effect and the ability to produce clear evidence of behaviour against possible negative impacts on the freedoms and liberties of residents and visitors.

The TMO has concluded that with careful management the impact on residents' freedoms can be adequately mitigated. Principal amongst these is the careful adherence to the key principles of this policy and observation of the relevant legislation covering personal data.

The TMO has also concluded that no alternative measures are now practical given the failure of those already implemented. The TMO has however decided that in order to minimise the impact of CCTV both on individual freedoms and on the TMO financially, the system will be designed with the capability of being expanded easily and cost effectively. Initially the system will be equipped with only a limited number of cameras, further cameras will then be added as and when a need for that expansion is identified. There is no intension to equip the entire estate, very block or all possible angles with cameras, rather the opposite, to use the smallest number of cameras to the greatest effect accepting that in order to effectively achieve the aims of the system, the camera network may need to expand considerably. The design also allows for cameras to be repositioned providing an option for the system to adapt rather than simply expand to meet the perceived need.

The CCTV system will be installed and operated in accordance with this policy which sets out the operational standards and practices which will be adhered to, the oversight of adherence to this policy and how personal data will be protected in accordance with the relevant legislation.

2. WHAT IS THE INTENDED PURPOSE OF CCTV CAMERAS ON D'EYNSFORD ESTATE?

The CCTV system has been engineered to adapt and grow organically in response to ongoing issues and/or changes in behaviour brought about by the existing CCTV system and/or other measures. This approach has been adopted to ensure that the CCTV system achieves the stated aims using the smallest quantity of cameras and the least invasive approach.

Recording will ordinarily be continuous with the system used passively however the system may be monitored live in accordance with this policy under certain circumstances; this includes the provision of live feeds to the police.

The CCTV system aims to;

- **A.** Provide a safer environment for staff, residents and visiting members of the public
- **B.** Deter prospective offenders
- **C.** Assist, by way of providing footage, with the identification, apprehension and prosecution of offenders
- **D.** Assist in determining the cause of incidents and or accidents to assist in insurance claims
- **E.** Monitor Security of the estate buildings and minimise the cost associated with vandalism to property and equipment
- **F.** Proactively utilise the CCTV systems to uphold tenancy & lease conditions
- **G.** Detect, deter and take action against those who use or store motor vehicles on footpaths, pedestrian walkways, within buildings, near building escape routes or in locations which represent a fire hazard or other risk to the safety of residents, visitors or the fabric of the estate.

The D'Eynsford TMO Recharge Policy should be read in conjunction with this policy as the TMO will use footage obtained from the CCTV camera system to generate recharge invoices in relation to fly tipping, criminal damage and neglect/accidental damage caused by anyone living within or visiting the estate. Residents are reminded that under the Recharge Policy they are responsible for recharges arising from their actions, those of their family, guests and visitors.

3. HOW DO WE INFORM RESIDENTS AND THE PUBLIC ABOUT OUR CCTV SYSTEM?

The TMO will aim to provide individuals with fair processing information and will use the TMO pages on the 'D'Eynsford' website to publicise the use of CCTV by the TMO, including the aim and purpose of the scheme, how a subject access request can be made and who it should be sent to. Full access to key documents will be provided including:

- This CCTV Policy
- Data Access Request Form
- Subject Access Request Form
- GDPR Policy
- CCTV Leaflet?
- TMO Complaints policy
- Information Commissioners Office (ICO) CCTV Code of Practice
- Details of the ICO website

Camera Positioning will also be publicised both on the website and in the relevant areas within the TMO reception area. Signs located at estate entrances and selected sites within the estate will advise of CCTV monitoring, identify the TMO as the owner and operator of the system and include the website address where more detailed information can be accessed.

4. STORING AND RECORDING INFORMATION

The CCTV system is owned and operated by the D'Eynsford TMO which acts on behalf of its members (residents). The system is operated by the TMO under the guidance of the Security Sub-committee and Board with periodic review of the system, its use, expansion, contraction, adaptation and performance by the members at the Board.

The TMO will ensure it follows the steps below when storing the information recorded by the CCTV system:

- Regularly verify that the date and time on the recording devices are accurate
- Check that they have enough recording space for a retention period of 1 month.
- Not intentionally store any information or images for longer than is necessary subject to a minimum retention period of 1 month (31 days)
- Make sure that the information recorded is used only for the purposes for which the system was installed
- Keep the recordings secure and keep access to them to a minimum

Retention of images
In normal operation the images recorded by the CCTV cameras will be stored until such time as the recording medium is full whereupon images will be automatically removed.

Images/recordings of identified events/incidents will be retained until such time as the TMO is satisfied that all parties with an interest have exhausted their need for the data and the last statute of limitation date for potential legal claims.

Digital Video Recorder Storage
The data DVRs will be stored in a secure cabinet or locked safe room and kept locked at all times when unattended.

Data Usage
Digital systems will have their hard drive left in the recording device and set to record for a minimum of 30 day rolling basis. These will only be removed in exceptional circumstances such as maintenance, in the event of a system failure or as part of a police investigation.

Data required for evidential purposes
Must be retrieved from the DVR(s) promptly and stored on separate media, indexed and securely stored to avoid accidental loss or unauthorised access.

Disposal of data
The TMO shall ensure the secure disposal or destruction of data and/or media when appropriate.

Labelling
Data storage media (CDs, DVD, Memory Stick and hard drives) will be individually and uniquely identified and labelled by the Operator.

Suspicious Incidents

Where Police have reasonable grounds for believing that a suspicious incident has been recorded, a Police Officer will arrange to view the data or request a copy. A police data access request form must be provided before a copy of any data is provided.

The Police may remove the data from the TMO as evidence as part of their investigation provided the removal is authorised in accordance with procedures. This would normally be given except where it may incriminate the TMO in which case it should be ordered through the normal judicial process. The Estate Manager or designated officer and the Police Officer will log all removal of such data in the data register.

Data Removal
Once the data has been removed by the Police Officer, the Police will assume full responsibility for its security and integrity as evidence to be produced in court.

Copies
No copies of data will be made without the express permission in accordance to procedure.

Copies shall not be made other than for the prevention or detection of crime, for the presentation of evidence in court or for access by the defence in accordance with GDPR or investigation by an insurance company.

Data Management
All data will be kept in a secure location at all times. Access to the digital recording equipment will be restricted, with only nominated people holding keys.

Operating Controls
Only staff with responsibility for using the equipment shall have access to operating controls.

Viewing
Cameras will not intentionally be used to look into private dwellings or into sensitive areas concerning personal privacy (e.g. balconies). Residents who believe a camera is capable of being instructed to move to a position where it can observe their property, can request that a privacy mask be programmed into the camera to obscure that part of its view should it move to such a position. The resident will be permitted to briefly observe a live image of the camera so positioned towards their property to verify the obscuration.

Checking
Checks will be carried out to ensure compliance with operational procedures and objectives, to ensure technical functionality and effectiveness including but not limited to directional positioning, environmental effects, picture quality etc and to ensure camera positions are maintained to respect individual privacy and only capture images to achieve the aim of the policy. These checks will be undertaken on both live and recorded footage.

Staff will be made aware that all CCTV recordings, forms and records are subject to routine audit and they may be required to justify their interaction with the system if not in strict adherence to this policy.

5. WHO CAN ACCESS THE DATA?

It is hoped that the CCTV system will cover most of the estate and help to reduce the anti-social behaviour, fly-tipping and criminality on the estate while providing reassurance and a

greater sense of security for residents and visitors. The system is therefore intended to be passive, owned and operated by the TMO in accordance with policies and data protection regulations.

Accordingly TMO staff, Board and Subcommittee members may have a legitimate need to access the images captured by the CCTV system. In the most serious of situations the Police may take legal control of the data and/or physical assets of the CCTV system.

Other people e.g. insurance companies, the Police, Southwark Council etc may have a need for footage however these requests will be serviced by TMO staff and/or Board/Subcommittee members.

As such the TMO will seek to provide requested footage wherever possible, where it is required to do so and provided doing so does not disproportionately disadvantage others. Where necessary the TMO will redact elements of the footage to protect the personal data of those unconnected with the incident/event in order that footage can be provided.

All requests for footage must have a legitimate purpose or be made under a Subject Access Request (SAR) and pertain only to the person making the request and/or their property. The TMO may make a charge (currently capped at £10) for providing footage requested via an SAR and have 40 days in which to provide this.

An access request for data can only be made by the Police and bonified insurance companies who may be investigating an insurance claim. The TMO will not normally provide footage to residents or the public. When considering such direct release of footage, the TMO will consider the potential implications of such a release based on the ease with which other residents featured in the images may be identified and the potential for recriminations or embarrassment e.g. in relation to whom they may be in the company of. to the TMO will ensure it complies with the GDPR regulations in order to protect the interest of other residents.

The brief guidance from ICO in regards to Subject Access Request are as follows:

> *Individuals whose information is recorded have a right to be provided with that information or, if they consent to it, view that information. Information must be provided promptly and within no longer than 40 calendar days of receiving a request. Providing information promptly is important, particularly where you may have a set retention period which will mean that the information will have been routinely deleted if you take the full 40 calendar days to respond. In such circumstances it is good practice to put a hold on the deletion of the information.*
> *You may charge a fee of up to £10 (this is the current statutory maximum set by Parliament). Those who request access must provide you with details that allow you to identify them as the subject of the information and also to locate the information on your system. You should consider:*
>
> - *how staff involved in operating the surveillance system will recognise a subject access request; and*
> - *whether internal procedures for handling subject access requests are in place. This could include keeping a log of the requests received and how they were dealt with, in case you are challenged*.

The TMO is responsible for the CCTV system and to ensure the following:

- Day to day responsibility is delegated to authorised, trained staff and volunteers only
- Detailed operational guidelines are available, up to date and implemented
- Complaints from the public about operation of the system are formally logged and processed in accordance to the TMO's complaints policy
- Only designated trained staff will have access to CCTV images
- Access to and removal of data is only carried out following authorisation in accordance to procedure and is documented.
- Individual data privacy is safeguarded and respected
- CCTV signage is clearly visible in all areas where CCTV is in operation
- Legislation changes are reflected in policy and procedure documents as and when necessary
- All persons accessing CCTV footage must be DBS Checked

Governance

Designated TMO staff members have day-to-day responsibility for the use of the system in accordance with this policy. The Security Subcommittee are to provide regular monitoring of the use, effectiveness and scope of the system and the policies including a responsibility to review requests, decisions made, footage released etc to ensure that the TMO as an organisation is adhering to policy and the law.

The Board will be directed by the recommendations of the Subcommittee and will sanction any changes to policy or the camera network and will ultimately adjudicate.

In cases where a recharge invoice is challenged by a resident, the Finance Subcommittee may be provided with access to CCTV footage relating to the charge for the purposes of assessing the case. In turn, the footage may be shown to the Board who will decide whether or not to cancel or amend the invoice.

Finally, at least once per year, summary data and sample footage will be presented to the members of the TMO and residents at a general meeting and always at the annual general meeting so a decision can be taken as to the continued use of CCTV on the estate.

The Southwark Council TMI team will also play a role in overseeing the use of CCTV on the estate to ensure that footage from the system supplied to Police or the Council meets their evidential requirements.

Access to Images

As all CCTV cameras are situated in and exclusively record images of public spaces on the estate, there is no reasonable expectation of privacy. Nevertheless the TMO undertakes to redact footage where it is appropriate to do so. The TMO will consider the need to redact part or all of the footage and thereby conceal the presence or identity of persons unconnected with the primary subject of the footage in order to ensure; the protection of vulnerable residents (e.g. those not dressed in appropriate outdoor attire) or residents in the company of others where this may prove to be embarrassing or that footage which may be used by 3rd parties does not inadvertently expose residents to public scrutiny.

All requests (Police & Insurance Companies) for footage must be made by completing a *'data access request form'* and those receiving footage must undertake to use it only for the purpose asserted. Specifically recipients must undertake to not post footage to any online platform, video sharing site or other public forum.

The TMO may provide remote access to individual cameras or the CCTV system as a whole or any part thereof to the Police. This may occur as a result of a request from the Police or as result of discussions between the Police and the TMO concerning current security matters on the estate. In such situations the Police will be able to direct the PTZ cameras as they wish and/or disrupt the normal movement patterns/settings. Any privacy screens programmed into the cameras will remain in force and the Police operator will not have access to override or alter any system/camera settings pertaining to the same.

Footage may be provided to Southwark Council and/or used internally in relation to upholding tenancy and lease conditions.

Internal Data access retrieval form
In order for the Police or an Insurance Company to obtain the image, they must provide their data access form or if they do not have a copy then they can complete the TMO's 'data access form'.

Operators of CCTV

- Shall be designated TMO members
- Staff procedure training shall be provided by the Estate Manger

Staff shall be required to

- Maintain high standards of probity and confidentiality.
- Acknowledge receipt and understanding of relevant policies and procedures.
- Ensure proper use of the equipment or recordings. Any abuse or improper use will be subject to the disciplinary policy.

Access to view monitors and/or to operate equipment

- Shall be limited to the designated operators of the systems, the Estate Manager, designated staff, volunteers, the Police and Council Officials.
- CCTV Monitors will be secured in a locked room at all times
- CCTV software for remote use will be limited to authorised staff only and secured with password access only.

Supply of Footage

- The TMO will not charge for the supply of footage internally, to the Police, Southwark Council or Insurance Companies acting on behalf of residents.

- Charges will apply for Subject Access Requests regardless of whom the requesting party is, the maximum permissible fee is currently £10.

- All other requests for footage will attract a charge of £50 + VAT.

Examples of when charges will apply:

- Insurance company acting for a non-resident requests footage either as the claimant or defendant in a claim
- Delivery Company seeking footage of a delivery (e.g. delivery dispute)
- Council Sub-Contractors (i.e Smith and Byford, Silk and Mackman, Spokesmead, DCUK etc) request footage

Footage will ordinarily be provided on CD or DVD media or electronically unless the entity making the request provides an alternative physical storage medium. Where data is provided directly to the receiving party no encryption will be implemented by the TMO on the storage media, it is the responsibility of the receiving party to implement their own security to ensure the data remains secure.

Where media is to be posted, the data will be encrypted and the key/password to access sent to the receiving party via a separate communications channel.

Where data is provided electronically the TMO will provide access to an encrypted copy of the data. The receiving party will be provided with a unique decryption key and access to the data will be logged and limited for the express purpose of decryption and downloading the unencrypted data to their own storage via a secure and encrypted channel. Thereafter the encrypted data source copy will be removed from the online storage location. The TMO will not 'upload' data to 3rd party file sharing sites or services whether 'encrypted' or not and regardless of any claims the 3rd party may make about their security/encryption. The TMO will also not upload data directly to systems operated by the receiving party.

In so doing the TMO is able to accurately log an audit trail for the supply of data and is able to verify the security of such data during the transfer to the receiving party.

Footage will normally be provided in HikVision MPEG format with a copy of the associated player software for use on the Microsoft Windows Operating System only. The receiving party is responsible for obtaining the necessary equipment to access/use these file formats and/or for the conversion to alternatives if their purposes require that.

Redactions will be achieved using the following software:

- Serif Movie Plus X6 (or newer)
- All redacted footage will be supplied in ordinary MPEG or AVI format only.

6. LOCATION OF DVRS AND AREAS OF MONITORING

Location of Digital Video Recorders

The DVR units are located within secure rooms within the estate. Each location has been assessed to ensure it offers dry conditions and the doors have been upgraded to a multi-point locking secure metal door. Access to these locations is strictly under the control of the TMO and all locations are devoid of other services to which contractors or the Council require access.

DVRs installed within intake cupboards may be further secured with a metal cabinet which is locked and only accessible by a key which is kept within the TMO Officer.

The exact location of the DVR units is documented in the operational manual held in the TMO office and will only disclosed to the TMO Staff, Board Members and the Police.

Areas of monitoring

The TMO is fully aware of its obligation not to record images which are private to residents and therefore will ensure the cameras are not directed at windows or doors of properties.

The TMO have agreed to monitor areas of special interests which fall into one of these categories:

- Locations identified in consultation with the Police
- Locations subject ot to frequent instances of fly-tipping
- ASB Hot spots
- Key Estate Entrances

The area of monitoring is available in the office and also on the website.

The TMO reserves the right to use a network to access footage from a central location (e.g. the TMO office).

Interference with any element of the CCTV system will be reported to the Police as criminal damage. The TMO will operate a zero tolerance policy in respect to tampering, disablement, damage or interference with any component of the CCTV system. In addition to criminal prosecution, the TMO will peruse the costs of repair against those responsible.