

## **Data Protection Policy (Use of CCTV)**

### **Background**

The purpose of this policy is to outline KWMCC's approach to the use of CCTV cameras and how information will be stored and used in line with the Data Protection Act. KWMCC Employees should read in conjunction with the Data Handling and Retention Policy, Information Security Policy and the relevant CCTV section within the Employee Handbook.

KWMCC uses closed circuit television (CCTV) images for the prevention, identification and reduction of crime and monitoring of its property in order to provide a safe and secure environment for residents and to prevent the loss or damage to KWMCC property.

CCTV surveillance is intended for the purposes of:

- protecting KWMCC's assets;
- promoting the health and safety of staff and users;
- reducing the incidence of crime and anti-social behaviour (including vandalism);
- supporting the Police in a bid to deter and detect crime; and
- assisting in identifying, apprehending and prosecuting offenders.

### **1. How the system operates**

- 1.1 The system comprises fixed cameras positioned around the premises located at Twelve Acres Approach, Kesgrave (the "Centre").
- 1.2 The CCTV system is owned and operated by KWMCC and the deployment of which is determined by KWMCC through the General Manager.
- 1.3 The CCTV is regularly monitored and data/images are retrieved upon receipt of reports of potential criminal or anti-social behaviour.
- 1.4 All authorised operators and employees with access to images must be aware of the procedures that need to be followed when accessing the recorded images and operators trained to understand their responsibilities under the CCTV Code of Practice. It is important that all employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.
- 1.5 KWMCC complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure its CCTV system is used responsibly and it safeguards both trust and confidence in its continued use.
- 1.6 The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.
- 1.7 CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by KWMCC, including its Complaints Policy.

### **2. Justification for Use of CCTV**

The use of CCTV to monitor the Centre for security purposes has been deemed to be justified by KWMCC. The system is intended to capture images of individuals damaging or misusing property or any anti-social behaviour within or close to the Centre.

### **3. Data Protection Impact Assessments**

Where new CCTV systems or cameras are to be installed, KWMCC will carry out a full Data Protection Impact Assessment identifying risks related to the installation and ensuring full compliance with data protection legislation. This may involve the need for consultation with staff, users and local residents.

#### **4. Location of Cameras**

- 4.1 Cameras are sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated.
- 4.2 KWMCC will continue to ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.
- 4.3 Cameras are placed to record external areas however are positioned in such a way as to prevent or minimise recording of passers-by outside the perimeter of the Centre.
- 4.4 CCTV Video Monitoring and Recording of Public Areas may include the following:
  - Protection of KWMCC property: Centre perimeter, entrances and exits
  - Criminal Investigations (carried out by police): robbery, burglary and theft surveillance.

#### **5. Covert Surveillance**

KWMCC will not engage in covert surveillance.

#### **6. Notification**

- 6.1 A copy of this CCTV Policy will be provided on request to staff, users or residents and is available on KWMCC's website.
- 6.2 The location of CCTV cameras are indicated and adequate signage must be placed at each location in which a CCTV camera is sited to indicate that CCTV is in operation. Appropriate locations for signage includes:
  - at entrances to premises i.e. external doors, gates; and
  - at or close to each camera.

#### **7. Storage and Retention**

- 7.1 The images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.
- 7.2 The images/recordings must be stored in a secure environment with a log of access kept.
- 7.3 Access is restricted to authorised personnel. Supervising the access and maintenance of the CCTV system is the responsibility of the General Manager. The General Manager may delegate the administration of the CCTV system to another staff member.
- 7.4 In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis only.

#### **8. Access**

- 8.1 Recorded data/images are securely stored in a restricted place. Unauthorised access will not be permitted at any time. The area must be locked when not occupied by authorised personnel. A log of access must be maintained.
- 8.2 Access to the CCTV system and stored images is restricted to authorised personnel only.
- 8.3 A record of the date of any disclosure request along with details of who the information has been provided to (the name of the person and the organisation they represent), why they required it and how the request was dealt with will be made and kept, in case of challenge.
- 8.4 Data will be provided to those requests authorised in a permanent format where possible. If this is not possible the data subject will be offered the opportunity to view the footage.

- 8.5 In relevant circumstances, CCTV footage may be accessed:
- By the police where KWMCC is required by law to make a report regarding the commission of a suspected crime; or
  - Following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on or near KWMCC property, or
  - By the HSE and/or any other statutory body charged with child safeguarding; or
  - By data subjects (or their legal representatives), pursuant to a Subject Access Request; or
  - By individuals (or their legal representatives) subject to a court order; or
  - By KWMCC's insurance company where it requires same in order to pursue a claim for damage done to the insured property.

## **9. Subject Access Requests (SAR)**

- 9.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.
- 9.2 Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified, for example, date, time and location.
- 9.3 Requests should be sent to the General Manager who is the KWMCC Data Protection Officer and will respond to requests within a month of receiving the request in line with KWMCC's Data Handling and Retention Policy.
- 9.4 KWMCC reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.
- 9.5 A record of the date of the disclosure along with details of whom the information has been provided (the name of the person and where applicable the organisation they represent) and why they required it will be made.
- 9.6 In giving a person a copy of their data, KWMCC will provide a still/series of still pictures, a disk or memory stick with relevant images. However, other images of other individuals will be obscured before the data is released.

## **10. Complaints**

Complaints about the operation of CCTV will be dealt with in accordance with KWMCC's Complaints Policy.

## **11. Staff Training**

- 11.1 Staff authorised to access the CCTV system will be trained to comply with this Policy. Staff must understand that all information relating to the CCTV images must be handled securely.
- 11.2 Staff will receive appropriate training to enable them to identify and handle different requests according to regulations.
- 11.3 Staff misuse of surveillance system information will lead to disciplinary proceedings.

## **12. Responsibilities**

- 12.1 The General Manager (or nominated staff member) will:
- Ensure that the use of CCTV systems is implemented in accordance with this Policy.
  - Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes.
  - Ensure that all existing CCTV monitoring systems are evaluated for compliance with this Policy.
  - Ensure that KWMCC's CCTV monitoring is consistent with the highest standards and protections.
  - Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this Policy.

- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system.
- Ensure that the perimeter of view from fixed location cameras conforms to this Policy.
- Give consideration to residents' complaints, if any, regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals and be mindful that no such infringement is likely to take place.
- Ensure that cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy".
- Ensure that monitoring footage are stored in a secure place with access by authorised personnel only.
- Ensure that images recorded are stored for a period not longer than 30 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil).
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy.
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

Further information can be found at <https://ico.org.uk/>.

<b>Version Control Table</b>			
<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Reason for change</b>
0.1	May 2021	Rod Gibson	New