CCTV

Policy Statement

1.0 Introduction

1.1 This policy applies to all CCTV monitoring carried out by HYELM ("us", "our", "we"). All employees who have responsibility for operating CCTV systems belonging to, or on a development belonging to us, or who have responsibility for storing and processing data collected by our CCTV systems, must comply with the provisions of this policy.

1.2 We operate CCTV at our developments for a number of reasons that are set out within this policy. Under the General Data Protection Regulation (GDPR), images of individuals who are identifiable constitute personal data.

1.3 This policy aims to ensure that the monitoring, recording, holding and processing of such images conforms with the statutory requirements, in particular those laid down by the GDPR and Data Protection Act 1998.

1.4 Scheme Managers are responsible for the day-to-day operation of CCTV systems at their individual developments and for dealing with any enquiries.

1.5 Further details on the obligations of data processors can also be obtained from the Data Protection Information Commissioner's Code of Practice, which is available at www.ico.org.uk.

1.6 We are committed to challenging discrimination and promoting equality of opportunity in every area of our work. This policy is written from an equal opportunities perspective.

1.7 This policy, and others, if requested, are available in different formats, such as languages, large print and recorded form.

2.0 Purpose

2.1 CCTV systems currently used at each of our developments are only for the following specific purposes:

- To discourage delinquent and anti-social behaviour.
- To deter and detect crime, including theft and criminal damage and, if relevant, to assist with apprehension of offenders.
- To ensure and enhance the safety and security of employees, residents, contractors, members of the public and any users of our developments.
- To assist in the overall management of buildings and grounds.

2.2 The legal basis for processing personal data is that it is necessary for us or a third party's legitimate interests in managing our developments, tenancies and other occupation arrangements, ensuring the safety and security of those at our developments and in preventing and deterring crime and anti-social behaviour on our premises.

This is in line with Article 6(1)(f) of the GDPR.

2.3 Where, in carrying out the purposes in paragraph 2.1, images of employees, contractors, residents or others are obtained, those images may be used in connection with investigations into:

- disciplinary allegations (and any hearings) for employees.
- breaches of contract terms for contractors.
- breaches of the terms of Tenancy Agreements for residents.
- breaches of the terms of Leases for corporate tenants.

2.4 CCTV systems will not be used for general surveillance of employees, contractors, residents or others or for purposes other than those specifically indicated above.

3.0 Related Documents

3.1 This policy should be read in conjunction with:

- Privacy Notices.
- Staff Handbook.
- Guide for Residents.
- Data Protection Policy.

4.0 Registration and Responsibilities of CCTV systems

4.1 Ultimate responsibility for implementing this policy rests with the Chief Executive.

4.2 All CCTV systems at our developments, fixed or temporary, fully comply with the provisions of this policy. Authority to install further CCTV systems must be obtained in writing from the Chief Executive.

4.3 The Director of Operations is responsible for overseeing the management of the CCTV networks and recorders.

4.4 The Scheme Managers are responsible for the day-to-day operation of CCTV systems at their individual developments, ensuring that equipment is properly maintained and regularly serviced, that maintenance contracts are in place and for dealing with any enquiries.

4.5 Complaints about the operation of the system or a failure to comply with any relevant legal requirements or guidance should be directed to the Company Secretary.

5.0 Visibility and Scope of CCTV Systems

5.1 The following guidelines are observed in the installation of CCTV systems at our developments:

- Cameras are not hidden from view and are sited in such a way as to ensure that they only monitor spaces intended to be covered.
- Cameras do not overlook private property, where possible, and where this is unavoidable, private residents are consulted and steps taken to reduce any interference with privacy.
- Signs are prominently displayed in every external CCTV location so that everyone is aware that they are entering a zone that is covered by surveillance equipment. Where it is not obvious, the sign should include the name of the data controller, a description of the purpose(s) of the system and details of who to contact regarding the system.
- Cameras are not used in private areas, such as public toilets or in the accommodation offered.

The equipment must be able to:

- Cover the area to be monitored and exclude areas that do not need to be monitored for the purposes set out in this policy;
- Produce clear images of a high quality, (i.e. of a standard that would be capable of having evidentiary value to the police);
- Work effectively 24 hours per day, 7 days a week.
- Have night time monitoring.
- Work effectively within normal indoor conditions.
- Produce images of sufficient size, resolution and frames per second to meet the requirements of the purposes;
- Record high quality facial images which can be used in court to prove someone's identity beyond a reasonable doubt;
- Record in real time on a continuous basis.

5.2 If at any time HYELM employs mobile cameras on a temporary basis, their use will also be governed by the guidelines within this policy.

5.3 Contractors, employees or security personnel wishing to introduce new but separate stand-alone systems may do so only with the express permission of the Chief Executive.

5.4 In order to protect the rights of individuals, CCTV systems will only be operated in ways that comply with the Data Protection principles and with our Data Protection policy.

6.0 Processing CCTV Data

6.1 CCTV systems authorised for installation by the Chief Executive at our developments will form part of integrated networks generating images recorded to hard disc on dedicated digital data recorders located in secure offices at each property and in dedicated data centres.

6.2 All data collected by our CCTV systems will be processed in compliance with data protection legislation and in accordance with our Data Protection policy.

7.0 Security of CCTV Data

7.1 We recognise that it is important that access to and the disclosure of images is restricted and carefully controlled, not only to safeguard the rights of individuals but also to ensure that evidence remains intact should the images be required for evidential purposes.

7.2 With this in mind, the Scheme Managers will ensure that:

- Measures are implemented to safeguard the security and confidentiality of systems and the images that they record.
- Adequate security measures are put in place to prevent unauthorised access to equipment, systems or images and the disclosure of images for purposes other than those for which the system was designed.
- A register of the names of those members of staff or contractors authorised to operate CCTV systems is maintained (e.g. to re-site or refocus cameras) and those authorised to view or process images recorded by the system.
- CCTV operators are fully conversant with their responsibilities in respect of data protection and personal privacy and are adequately trained to deal with security issues.
- Physical and network security measures ensure that only authorised staff have access to recorders, systems and recorded data and that recorded data is only accessible from nominated terminals.
- A comprehensive logging system records all uses of the equipment, accesses to data and processing of images.
- Access to staff is restricted to those who need to have it and only for the purpose(s) for which the system was installed.
- Access to, disclosure and use of recorded data is regulated.
- Practical arrangements are made for ensuring that images are viewed only by authorised employees in a secure and confidential area.
- The CCTV log records all processing of data.
- Images are not retained for longer than the retention periods specified in this policy.

7.3 Employees must comply with our rules and policy statements, including this policy and the Data Protection policy. Any failure to do so, and particularly in relation to data protection issues and the unauthorised use or disclosure of personal information, could result in disciplinary proceedings.

7.4 Criminal liability is possible where CCTV operators use cameras for purposes other than those outlined in this policy.

8.0 Viewing Images

8.1 As a general rule, CCTV images should only be viewed and accessed by authorised employees. Other employees and third parties (such as the police) should only be allowed to view the images where it is necessary in connection with the purposes set out above or as otherwise permitted in this policy. The mere act of viewing is a processing activity that is subject to the GDPR.

8.2 The following rules apply to the viewing of CCTV images:

- The viewing of live images on monitors should be restricted to an authorised operator of the CCTV system;
- Recorded images should be viewed in a restricted area (e.g. a designated secure office). Access to this area should be restricted whilst the viewing is taking place;

8.3 When a request is received and it is necessary to allow other employees, or a third parties (such as the police) to view the CCTV images, a record should be made of the following:

- The date of the written request;
- The date and time of the viewing;
- The name of the person viewing the images and the organisation they represent;
- The reason for the viewing;
- The basis upon which the viewing was allowed i.e. the lawful processing ground relied on under Article 6 of the GDPR;
- The outcome, if any, of the viewing.

9.0 Retention and Deletion of CCTV footage

9.1 We operate an agreed retention and automatic deletion policy.

9.2 Unless retention of CCTV footage is required to facilitate one of the purposes set out above, data recorded by us is deleted 30 days after it is recorded to ensure that data is retained on the system for no longer than is necessary. Such data is permanently deleted from our systems.

9.3 The Scheme Managers have responsibility for undertaking systematic checks to ensure that the retention and deletion policy is being observed in practice.

10. Processors

10.1 Any third party appointed by us to process personal data on our behalf will be a 'processor'. For example, we may hire an external organisation to maintain our CCTV system or to edit images on our behalf.

10.2 The GDPR requires us to comply with the following requirements whenever we use a processor:

- We must put in place a data processing agreement with such third party under which they agree to process personal data only in accordance with our instructions;
- The agreement must set out the security obligations with which the processor must comply;
- The agreement must also include provisions dealing with the confidentiality of personal data, including ensuring the processor's employees respect confidentiality and restrictions on the appointment and use of sub-processors or transfer of the personal data.

11. Disclosure of Images

11.1 In certain circumstances it may be necessary to disclose the CCTV images to a third party, such as the police. The disclosure is likely to involve the physical delivery of the images or copies to the third party (e.g. on a disk or by email). Disclosures to third parties must be consistent with the purposes set in this Policy. Any disclosure of images must be approved by the relevant manager following a written request.

11.2 Disclosures are permitted in the following circumstances:

- Crime prevention or detection purposes - where the disclosure is requested for the purpose of preventing or detecting crime, apprehending or prosecuting offenders, or assessing or collecting tax (the crime and taxation purposes). The third party making the request must:
  - justify its request for the CCTV images;
  - confirm that a failure to make the disclosure would be likely to prejudice any of the crime or taxation purposes;
  - put their request in writing, signed by a suitably senior person.
- Statutory or other legal obligation - the disclosure of the images may be required under statute (other than under the GDPR) or may otherwise be legally required (e.g. under a court order). In this situation:
  - we must disclose the CCTV images if the statutory provision imposes upon us a mandatory duty to disclose or a court order requires disclosure;
  - we can choose whether to disclose the CCTV images if the statutory provision imposes upon us a discretion as to whether or not to disclose;
  - any decision to disclose must be authorised by the manager.

11.3 In limited circumstances it may also be possible to make a disclosure where it is necessary for the purpose of establishing, exercising or defending legal rights, obtaining legal advice or in connection with legal proceedings. This covers not just our legal rights but also those of third parties.

11.4 A record should be kept of all requests for disclosure of CCTV images, together with any reasons for refusing a request. If a disclosure is approved and CCTV images are disclosed to a third party, a record should be made of the following:

- The date the written request was received
- The date and time of the disclosure;
- The name of the person to whom the disclosure is made and the organisation they represent;
- The reason for the disclosure and the images disclosed;
- The basis upon which the disclosure was made (by reference to the GDPR);
- The location where the images are to be kept;
- The outcome, if any, of the disclosure;
- The date and time the images were returned (if applicable);
- If the disclosure is to the police, record any crime incident number to which the images relate and ask the collecting police office to sign for the images when they are handed over.

11.5 Where a decision has been made to disclose CCTV images, the disclosure must be made securely so that the images are received by the intended recipient. For example, where a wireless transmission system is used to disclose the images, sufficient safeguards must be put in place to protect the transmission from being intercepted in transit (e.g. encryption).

12.0 Access to Personal Data

12.1 Arrangements for access to information held by us on residents, employees and others, which includes CCTV images, is covered by The Group's Data Protection policy.

12.2 Anyone seeking access to their personal information should submit a request to the Company Secretary. The Company Secretary will ensure that:

- All employees are made aware of the rights of individuals to access personal information and the conditions under which access may be granted to third parties.
- All access requests are dealt with by the Company Secretary and are referred to the Chief Executive.
- All requests for access or disclosure and subsequent responses are recorded in a register.

12.3 All requests from the police for access or disclosure are dealt with according to procedures detailed in accordance with guidance provided by the Information Commissioner's Office from time to time and with our own procedures.

12.4 Recorded images will be disclosed to third parties (e.g. the police or other law enforcement bodies) only in limited and prescribed circumstances.