CCTV SYSTEM OPERATORS POLICY

1. INTRODUCTION

1.1. The purpose of this policy is to regulate the management, operation and use of the closed-circuit television (CCTV) systems installed within any Knights Brown (KB) premises in the United Kingdom.

1.2. The systems usually comprise one or more cameras located internally/externally around the sites. All cameras may be monitored remotely and by KB staff internally.

1.3. This code follows GDPR guidelines.

1.4. The code of practice will be subject to review periodically, but at least annually, to include consultation as appropriate with interested parties.

1.5. The CCTV systems are owned or leased and operated by KB or its agents.

2. OBJECTIVES OF THE CCTV SCHEME (the "Scheme")

(a) To protect KB's buildings and their assets

(b) To increase personal safety and reduce the fear of crime

(c) To support the police in a bid to deter and detect crime

(d) To assist in identifying criminal activity and apprehending and prosecuting offenders

(e) To protect members of the public and private property

(f) To assist with any investigation as part of any potential serious incident on site or KB premises

3. STATEMENT OF INTENT

3.1. The scheme will be included within KB's registration with the Information Commissioner.

3.2. KB will treat the system and all information, documents and recordings obtained and used as data, which is protected by the GDPR.

3.3. Cameras will be used to monitor activities within KB's or its clients' premises 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 KB employees and contractors, together with their visitors.

3.4. KB intend to utilise static cameras which are not to focus on private homes, gardens and other areas of private property.

3.5. In circumstances where non-static cameras are required, unless an immediate response to events is required, staff will not direct cameras at an individual, their property or a specific group of individuals, without appropriate authorisation.

3.6. Footage, images or knowledge secured as a result of the scheme will not be used for any commercial purpose. Data will only be released to the media to assist police investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.

3.7. Footage or images of KB employees, subcontractors or agents will not be used for training without their consent. Reasonable measures will be taken to protect the identity of any third parties whose image is captured on such footage.

3.8. The planning and design has endeavoured to ensure that the scheme will give 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.

3.9. Warning signs, as required by the code of practice of the Information Commissioner, will be placed at all access routes to and the perimeter of areas covered by any KB CCTV.

4. OPERATION OF THE SYSTEM

4.1. The scheme will be jointly administered by KB's plant manager and KB's IT support manager, in accordance with the principles and objectives expressed in this policy. (Hereinafter referenced as the "system manager".)

4.2. The CCTV system will be monitored by Allied Facilities Limited on behalf of KB (the "Remote Monitoring Station").

4.3. The day-to-day management of each site will be the responsibility of the site manager. This includes notifying the system manager of any changes to the site that may impact the effectiveness of the scheme. Notifying the system manager of any movement of cabins, or variation in storage of plant / equipment that may result in the need to add to or change the scope of the cameras.

4.4. The CCTV system will normally be operated 24 hours a day, every day of the year.

4.5. KB's IT support manager will be responsible for ensuring that KB is monitoring the system functionality and in particular, that the equipment is properly recording and that cameras are functional.

4.6. Unless an immediate response to events is required, CCTV operators must not direct cameras at an individual or a specific group of individuals.

5. ACCESS, RETENTION AND USE OF DATA

5.1. Access to the CCTV footage and images will be strictly limited to:

5.1.1. The system manager, remote monitoring station and the IT Department.

5.1.2. Site managers (or their delegate) will be provided with facility to access footage and images relating only to their own site.

5.2. Unless the remote monitoring station has received prior notification, any visitor to a site outside of that site's normal operating hours will be treated as an intruder and may include police or security guard response.

5.3. A log of all events including authorised visitors, intruders, or other events that trip a movement sensor or a system alert, will be kept including time/date of event (eg entry and exit times) will be recorded.

5.4. Emergency procedures will be used in appropriate cases to call the relevant emergency service(s).

5.5. Footage and images will, subject to data storage capacity for the site, be retained for a maximum of 60 days except:

5.5.1. Where KB is undertaking or assisting (or reasonably anticipate assisting) an investigation and require the footage as part of this investigation. KB has a right to extend the time retained for the duration of any investigation or such longer period advised by an investigating authority.

5.5.2. Where the footage or images are (subject to 3.7 above) to be used for training.

6. LIAISON

6.1. There will be regular liaison with all bodies involved in the support of the system and a more formal review meeting will be held at least annually.

7. REMOTE MONITORING STATION MONITORING PROCEDURES

7.1. Camera surveillance may be maintained at all times.

7.2. In exceptional circumstances where covert surveillance is required (eg in the event of, or suspicions of, serious criminal activity) such action will be subject to express written instruction authorised by a KB director.

8. DATA PROCEDURES

8.1. In order to maintain and preserve the integrity of data to facilitate its use in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

(i) The data media used to store a requested copy of the data must be identified by a unique mark.

(ii) Before use, the media must be cleaned of any previous recording.

(iii) The controller shall register the date and time of data transfer, including reference.

(iv) The process for provision/retention of copies of the requested data will be as advised by the appropriate investigating authority.

8.2. On request from the relevant investigating authority, footage or images may be provided for the prevention and detection of crime or accident/incident investigations whether occurring on or adjacent to our sites. The procedure in 8.1 above will apply to the provision of such data.

8.3. Applications received from outside bodies (eg solicitors) to view or release data will be referred to the Data Protection Office. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that it is required for legal proceedings, a subject access request, or in response to a Court Order. A reasonable fee can be charged in such circumstances for subject access requests; a sum not exceeding the cost of materials can apply in other cases.

9. BREACHES OF THE CODE (including breaches of security)

9.1. Breach of this code of practice by any persons involved in the scheme will be initially investigated by the system manager, in order for the appropriate action to be taken. Where appropriate, an independent investigation will be carried out to make recommendations on how to remedy the breach.

10. ASSESSMENT OF THE SCHEME AND CODE OF PRACTICE

10.1. Performance monitoring, including random operating checks, may be carried out by the system manager.

11. COMPLAINTS

11.1. Complaints will be investigated in accordance with KB's complaints procedure and where appropriate, Section 9 of this code.

11.2. Any complaints about the scheme should be addressed to the system manager.

12. ACCESS BY THE DATA SUBJECT

12.1. The GDPR provide data subjects (individuals to whom "personal data" relates) with a right to data held about themselves, including those obtained by CCTV.

12.2. Requests for data subject access should be made in writing to the Data Protection Office (data.protection@knightsbrown.co.uk).

12.3. KB reserves the right to charge a fee for administrative costs where further copies are requested or where the request is deemed excessive. The individual will be advised accordingly before processing the request for data subject access.

13. PUBLIC INFORMATION

13.1. Access to this policy is provided through KB's website.

KEVIN VALENTINE | MANAGING DIRECTOR
JUNE 2023