



Kingsclere Community Association

The Fieldgate Centre

Closed Circuit Television Policy

Reviewed	March 2020
Next Review	March 2023

Contents

1	MANAGING THE POLICY	3
2	INTRODUCTION	3
3	PURPOSE AND OBJECTIVES	3
4	ROLES AND RESPONSIBILITIES	4
5	USE OF CCTV IN THE BOROUGH	4
6	OPERATION.....	4
7	SUBJECT ACCESS REQUESTS	6
8	FREEDOM OF INFORMATION	6
9	REVIEW.....	7
10	SURVEILLANCE CAMERA CODE OF PRACTICE.....	7

1 MANAGING THE POLICY

1.1 Compliance

This policy applies to all staff, volunteers, trustees, members, guests and visitors.

1.2 Advice and Training

If you do not understand anything in this policy or feel you need specific training to comply with it you should bring this to the attention of a member of the committee.

1.3 Equality and Diversity

Every policy must consider equality and identify any potential barriers or discrimination faced by people protected by equality legislation.

2 INTRODUCTION

2.1 This policy sets out how the Kingsclere Community Association (KCA) (or also referred to as ‘the committee’) will operate and maintain CCTV at the Fieldgate Centre (The Centre).

3 PURPOSE AND OBJECTIVES

3.1 The purpose of this policy is to ensure the management, operation and use of CCTV is regulated to ensure consistency and compliance with relevant legislation.

3.2 The Policy takes into account the:

- Surveillance Camera Code of Practice issued by the Home Office in June 2013
- CCTV Code of Practice issued by the Information Commissioner’s Office (ICO)
- Requirements for processing personal data as set out in the Data Protection Act 2018 (General Data Protection Regulations)
- Right to privacy as set out in Article 8 of the Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Crime and Disorder Act 1998

3.3 All associated information, documents and recordings obtained by CCTV must be held and used in accordance with the Data Protection Act, the ICO’s CCTV Code of Practice and the Surveillance Camera Code of Practice

- 3.4 Images obtained from CCTV recordings will not be used for any commercial purpose. Recordings will only be released to the media for use in an investigation of a crime provided the written consent of the Police has been given. Recordings will not be released to the media for entertainment purposes.
- 3.5 Archived CCTV images will not be kept for longer than is necessary for the purpose of Police or KCA evidence. Images no longer required will be securely disposed of and such disposal will be recorded on the KCA's Disposal Log.

4 ROLES AND RESPONSIBILITIES

- 4.1 This section sets out the roles and responsibilities in relation to the effective operation of CCTV.
- 4.2 The committee are responsible for ensuring compliance with the policy in relation to all CCTV.
- 4.3 The committee are responsible for ensuring compliance with the Data Protection Act and Regulation of Investigatory Powers Act in relation to the processing of images and the use of any covert CCTV.
- 4.4 All staff and Members are responsible for complying with this policy.

5 USE OF CCTV AT THE CENTRE

- 5.1 Predominantly the KCA will use CCTV for the purpose of reducing and detecting crime and anti-social behaviour as well as ensuring the safety of the public and its staff.
- 5.2 The use of CCTV in the Fieldgate Centre should always be for a specific purpose and clear signage indicating CCTV is in operation will be provided in a prominent place.

6 OPERATION

- 6.1 Images are recorded but are not monitored in real time.
- 6.2 Images are recorded and retained until overwritten unless they are required for an ongoing investigation. Where footage is required for an investigation a copy will be held for up to one year, or such other time period as may be necessary to progress the investigation.
- 6.3 Recorded information is held on digital recorders or in secure computer files with access restricted to nominated people.

Recorded images will only be viewed in secure monitoring centres or in offices with restricted access.

6.4 Requests to access or view recorded images should be made to a member of the committee

6.5 All requests for access to recorded images must be logged. This applies to requests from members of staff or third parties, for example, the Police. Requests from individuals for a copy of their personal data, including recorded images, will be considered as a subject access request under the Data Protection Act. Section 8, below, relates to such requests.

6.6 In order to ensure the preservation of images for evidential purposes, the following will apply:

- DVDs must be identified by a Name, Date, time, Camera Location and Recording equipment used
- The DVD must be signed by the person who downloaded the images, dated, witnessed and stored in a sealed envelope
- An original copy of the image downloaded must be retained, date stamped and stored in a secure area.
- The log must be completed detailing the release of the DVD to the Police, or other agency if appropriate
- If a DVD is required as evidence, a copy may be released to the Police, who will become the Data Controller and, therefore, responsible for the images

- The Police may require the committee to retain stored DVDs for possible future evidence. Such DVDs will be indexed and securely stored for a period of 1 year, at which point they will be securely destroyed.
- Applications received from external agencies (for example solicitors or insurance companies) to view recordings must in the first instance be made via a member of the committee. If appropriate images may be downloaded to DVDs and released where satisfactory documentary evidence is produced confirming legal proceedings, or in response to a Court Order.

6.7 It should be noted that, where it is necessary to download images onto removable media (DVD) they will be unencrypted in order to allow viewing by third parties. A suitable method to ensure the secure transfer of the removable media must be used and documented.

6.8 Still photographs of CCTV images must not be taken as a matter of routine. The taking of each photograph must be capable of justification (for example for the prevention or detection of crime and anti-social behaviour) and only done so with the permission from the immediate person in charge of the CCTV system –.

7 SUBJECT ACCESS REQUESTS

7.1 The Data Protection Act provides individuals with the right to access a copy of their personal information held by the KCA. This includes the right to access a copy of CCTV images.

7.2 Subject access requests should be forwarded to a member of the Committee for processing.

8 FREEDOM OF INFORMATION

8.1 The Centre may receive requests for a copy of recorded information under the Freedom of Information Act 2000 (FOI). If a request for a copy of a CCTV recording is made the following will be considered:

- Is the information the personal data of the requester? If so disclosure is exempt under FOI, but the request will be considered as a subject access request under the Data Protection act 1998.
- Is the information the personal data of individuals other than the requester? If so, it is likely to fall under the exemption for personal data unless disclosure would not breach the data protection principles.

8.2 Requests may also be received regarding the CCTV itself – for example the siting and operation of cameras or the costs associated with using and maintaining them.

8.3 Information following such a request would be released unless a valid exemption applied

8.4 All requests made under FOI should be referred to a member of the committee.

9 REVIEW

9.1 All uses of CCTV should be reviewed on an annual basis to ensure:

- There is still a legitimate reason to maintain the CCTV
- The CCTV cameras continue to provide images of sufficient quality
- Signage remains up to date and relevant

9.2 If it is determined additional cameras are necessary, either to supplement existing CCTV or to cover another area, a Privacy Impact Assessment (PIA) must be completed.

10 SURVEILLANCE CAMERA CODE OF PRACTICE

10.1 The Surveillance Camera Code of Practice was issued in 2013 following the introduction of the Protection of Freedoms Act 2012. The Code provides guidance on the appropriate and effective use of surveillance camera systems.

10.2 The code applies to the use of surveillance camera systems that operate in public places, regardless of whether or not there is any live viewing or recording of images or information or associated data.

10.3 The code provides 12 guiding principles which the KCA has adopted. These are:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used and these must be communicated to all who need to comply with them
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system and such images and information should be deleted once their purposes have been discharged
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice and regular reports should be published
11. When the use of a surveillance camera system is in pursuit of a legitimate aim and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.