South Kesteven District Council

SOUTH KESTEVEN DISTRICT COUNCIL

CCTV

OPERATIONAL

CODE OF PRACTICE

Environmental Services
South Kesteven District
Council St Peters Hill
Grantham
NG316PZ

Amended: June 2018

CONTENTS

CCTV MONITORING FUNCTION
CODE OF PRACTICE

1.0 INTRODUCTION

1.1 South Kesteven District Council has installed a comprehensive CCTV surveillance system which covers key areas, namely town centre areas and associated car parks in Grantham, Stamford, Bourne and The Deepings.

1.2 The CCTV system is owned by South Kesteven District Council and the control room is staffed by Council employees. These staff are licensed by the Security Industry Authority.

1.3 The CCTV team will monitor and control the system for 24 hours per day each day of the year. Selected images are also able to be displayed at Police Headquarters and a number of other Police sites throughout the District.

1.4 This Code of Practice provides a clear statement of the purpose of the scheme and provides guidance on the operation and management of the system.

1.5 All recorded material is owned by South Kesteven District Council and will be subject to the statutory conditions of the Data Protection Act 2018 and Regulation of Investigatory Powers Act 2000, and in accordance with paragraphs 17 and 18 of this Code of Practice.

2.0 DEFINITIONS

2.1

SKDC	The Council of the District of South Kesteven
The Owner	South Kesteven District Council, the organisation with overall responsibility for the formulation and implementation of policies, purposes and control of the service
The Surveillance Area	The area covered by the CCTV cameras
CCTV System	The surveillance system installed to cover the public area
CCTV Operator	Any member of staff employed by SKDC to monitor CCTV images at the Control Room
The Management Group	The group comprising of the Assistant Director for Commercial and Operational Services, Community Resilience Lead and the CCTV Control Room Supervisor
The Control Room	The monitoring centre operated by SKDC from where CCTV is monitored and

	images recorded, analysed and processed. It is also the location where radio systems are controlled and accessed.
RIPA	Regulation of Investigatory Powers Act 2000
Police Airwaves	The radio communication network used by CCTV staff to communicate with the police.
DPA	Data Protection Act 2018
An incident	An observation or referral that requires an action to be taken by a member of the control room staff

2.2 For the purposes of this Code, where the context so requires:

(a) singular includes the plural
(b) references to any party shall include its successors in title of that party
(c) reference to any statute shall include that statute as subsequently amended, all such instruments made under the statute and re-enactment of the relevant provisions in the subsequent statute

3.0 PURPOSE

3.1 The primary objective of the scheme is to provide a safe public environment for the benefit of those who live, trade, visit, service and enjoy the facilities of the area. This objective will be achieved by the pro-active monitoring of the system, so as to:

- assist in the detection and prevention of crime; along with the maintenance of public order
- facilitate the apprehension and prosecution of offenders in relation to crime and public order
- reduce Anti Social Behaviour
- reduce the fear of crime and provide reassurance to the public
- provide the Police and the Council with evidence to take criminal or civil action in the courts
- to assist in improving the environment in the areas monitored
- maintain and enhance the commercial viability of the District and to encourage continued investment

3.2 Every consideration will be given to the right of the general public to go about their daily business with minimum loss of privacy. Whereas total privacy cannot be guaranteed within a CCTV area, the cameras will not be used to unduly monitor persons going about their lawful business. It is inevitable that individuals could be caught on camera briefly during general surveillance but persons will only be specifically monitored, for any length of time, if there is suspicion or knowledge that an offence may have occurred or be about to occur. Operators must be able to justify their actions.

3.3 The CCTV system will be used for the provision of recordings for evidential purposes to the Police and other bodies having prosecution powers, such as Customs & Excise or the Health &Safety Executive.

3.4 This Code of Practice is supplemented by a separate procedural manual which is to be used by Operators. Circulation of the manual will be restricted and copies shall be stored securely.

4.0 PRIVACY

4.1 The CCTV system will be included in the South Kesteven District Council's Data Asset register and registered with Information Commissioner and operate in accordance with all data protection requirements.

4.2 Every consideration will be given to the right of the general public to go about their daily business with the minimum loss of privacy. Whilst total privacy cannot be guaranteed within the monitored area, the cameras and their recordings will not be used to unduly monitor people going about their lawful business. Where appropriate, cameras will be configured with 'privacy screening' in order to prevent undue privacy intrusions.

4.3 Persons will only be actively monitored for any length of time if there is suspicion or knowledge that an offence may have occurred or be about to occur or where other relevant authorisation is in place, e.g. an authorisation to use Directed Covert Surveillance under RIPA. In any event, a comprehensive incident log will be recorded giving a reason for the monitoring of the individual. All operators and duly authorised officers must be able to justify their actions at all times.

4.4 The cameras will only view public areas and not look through windows/doors of private premises. Exceptions to this may be made when a RIPA authorisation is in place or when there is an urgent pressing need such as when responding to a request by police when a crime is believed to be taking place or when the safety of an individual is at risk.

5.0 REGULATION OF INVESTIGATORY POWERS (RIPA)

5.1 The CCTV system will operate in accordance with the RIPA and SKDC's policy on covert surveillance.

5.2 Surveillance requests from the Police that fall within the remit of RIPA must be authorised by an officer of at least the rank of Superintendent and will remain valid for up to three months. In the event of an urgent need, an officer of at least Superintendent can verbally authorise for a maximum period of 72hrs. This must be followed up by a written authorisation. This process is set out in the Lincolnshire Police "Procedure for use of CCTV in Covert Policing Operations.

6.0 OTHER LEGISLATION

6.1 The CCTV system will be operated in accordance with all prevailing legislation and Statutory Codes of Guidance, including but not limited to; the Human Rights Act 1998, Data Protection Act 2018 and Freedom of Information Act 2000.

6.2 The CCTV system will comply with the Home Office Surveillance Code of Practice (June 2013) and will have regard to its 12 guiding principles which can be found in Section 11 of this document.

7.0 THE MANAGEMENT GROUP AND CHANGES TO THIS CODE

7.1 The Management Group will oversee compliance with this policy and collectively recommend any changes necessary. At all times the Management Group will have due regard to the 12 guiding principles set out within the Surveillance Camera Code of Practice, 2013 (see Section 10).

7.2 Minor and consequential changes to this policy can be made by the Community Resilience Lead on behalf of the management group. Any changes necessary will be fully documented and communicated to all relevant staff and external agencies where appropriate.

7.3 Any major changes necessary to this document will also require formal approval by the Council's Cabinet.

7.4 A major change will only take place after relevant consultation, the Cabinet member with the responsibility for CCTV will be briefed in this event.

7.5 A minor change may be agreed by the Management Group without the necessity of bringing it to the Cabinet Member.

7.6 A major change will have a significant impact upon the Code of Practice or upon the operation of the scheme. A minor change is one which is required for clarification will not have a significant impact.

8.0 LEAD AND DULY AUTHORISED OFFICERS

8.1 Recorded images are personal data under the DPA. South Kesteven District Council is the Data Controller for the purpose of the Act. The Community Resilience Lead is the Information Asset Owner.

8.2 The Lead Duly Authorised Officer for the scheme is the CCTV Operational Supervisor, additionally all members of control room staff are duly authorised officers and with reasonable and justified grounds can view recorded images in order to undertake urgent assessments of recorded images related to recent or ongoing incidents.

9.0 ACCOUNTABILITY

9.1 Copies of this Code of Practice and particulars of the complaints system will be made available on the council's website.

9.2 The Community Resilience Lead will report to the relevant Overview and Scrutiny Group on an annual basis and will also provide regular updates to the relevant Portfolio Holder.

9.3 Spot monitoring or audits should be carried out by at least two members of the Business Group. If the audit involves the duties of one member of the Group, then that member should not be part of the audit team and the other representatives should carry out the audit.

10.0 GUIDING PRINCIPLES

10.1 In accordance with Home Office Surveillance Code of Practice (2013), the 12 guiding principles have been recognised by SKDC. They are as follows:

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 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.

11.0 PUBLIC INFORMATION

11.1 Cameras should not be hidden but should, as far as is consistent with the purposes of the scheme, be placed on public view.

11.2 Signs that CCTV cameras are operating shall be displayed in and around the surveillance area in locations visible to pedestrians.

11.3 There is no requirement to place signs directly under cameras.

11.4 This Code of Practice shall be freely available to the public.

11.5 The owner will publish an Annual Report which will be available on the South Kesteven District Council website.

12.0 ASSESSMENT OF THE SCHEME

12.1 The Owner is responsible for ensuring that the scheme is evaluated periodically, at least on an annual basis.

12.2 Evaluation of the scheme will include data on the following performance indicators as part of a written report to be included within the annual report.

- Number of incidents
- Number of incidents by type
- Number of discs processed (evidential)
- Number of incidents reviewed
- Number of arrests

13.0 STAFF

13.1 The owner will be responsible for selecting and employing all staff employed to work with CCTV systems.

13.2 An effective and fair system of recruitment and selection of staff shall be employed which includes measures to ensure that the selection process provides for validation of the suitability of candidates for the role.

13.3 A disciplinary procedure shall be in place which incorporates compliance with the Code of Practice and operations manual and also makes plain the risk to staff in the event of breaches of the code or misappropriation of recordings or photographs.

13.4 All employees must be bound by an agreement of confidentiality which can be enforced during employment. Any proven breach of confidentiality could mean dismissal.

13.5 A defined system of staff monitoring and supervision that ensures compliance with the Code of Practice and operations manual shall be compiled and adopted.

14.0 COMPLAINTS

14.1 To obtain universal recognition this Code of Practice must address the interests of all who may be affected by it, and not confined to the interests of the “owner”, or the needs of the criminal justice system.

14.2 Complaints regarding any aspects of the scheme can be made via the SKDC website using the Customer Services Complaints link or by telephoning the SKDC Customer Services department.

14.3 All investigations following a complaint must be carried out in an impartial manner and dealt with in accordance with SKDC’s Complaints procedures.

15.0 BREACHES OF THE CODE

15.1 Responsibility for security issues in respect of CCTV will rest with the CCTV Supervisor or any duly appointed Officer.

15.2 All breaches of this Code of Practice and of security will be subject to proper investigation in line with the Council’s Disciplinary procedure.

16.0 CONTROL AND OPERATION OF CAMERAS

16.1 All Monitoring staff who have access to the camera equipment and recording equipment must act with the utmost probity.

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

16.3 All use of the cameras and control equipment shall be in accordance with the purposes and key objectives of the scheme.

16.4 All camera operators shall be subject to supervision procedures and work practices that are sufficient to ensure compliance with this Code.

16.5 All monitoring staff are to be made aware that their actions, operations and recordings are subject to routine audit and that they may be required to justify actions or their interest in a member of the public or premises.

16.6 As per Home Office Guidance Principle 2, Recordings from the system will be reviewed at least on a monthly basis by the Control Room Supervisor to ensure its use is justified and appropriate.

17.0 ACCESS AND SECURITY OF CONTROL ROOM AND POLICE COMMUNICATIONS

17.1 Only those persons with a legitimate reason to do so will be allowed access to the Control Room.

17.2 Public access to the Control Room or the demonstration of equipment shall not be allowed except unless they have been pre-arranged and authorised by the control room supervisor.

17.3 A SIA licensed operator will be present during the operation of the monitoring equipment. If monitors are to be left unattended, the room must be secured against unauthorised entry. The operation of the monitoring equipment shall be limited to staff with the correct authorisation, training and responsibility (other than those under supervised training).

17.4 Any visitor to the control room will be required to sign a Visitor Log before entry to the Control Room and this will include the reason for the visit. Duty Operators will use an in house system log to record periods of duty.

17.5 The operation of the monitoring equipment shall be limited to staff with the correct authorisation, training and responsibility.

17.6 Arrangements for the Control Room must include the following requirements to ensure that the Control Room is secure at all times:

- Records are kept of all access to the Control Room, recording details of the individual concerned, nature of visit and time of arrival and departure.
- Operation times and the numbers of staff on shift are clearly defined and complied with.
- Technical repairs and cleaning and similar tasks should be carried out in controlled circumstances.
- Access by visitors should be carefully controlled and will be the responsibility of the duty control room staff.
- Police visits will be made in order to collect or review recorded footage.
- All Police visits must comply with the audit provisions in place.

17.7 Security procedures on access to the Control Room must be maintained and strictly adhered to. Access must be monitored and all concerned should know that security procedures on access to the Control Room are included in the regular audit.

17.8 All security systems must be fully maintained and any defects reported to the Individual with day-to-day responsibility for the scheme.

17.9 Airwaves uses an encrypting mechanism called TEA2 and its use is strictly controlled. The owner will require a TEA2 licence and will be required to comply with the terms of any related agreement.

18.0 MAJOR INCIDENTS

18.1 The CCTV system may be used should it be considered an operational asset during a major incident or declared emergency. If required, the Councils Gold or Silver Commander can authorise the deployment of a liaison officer from any category one responder into the control room. The CCTV staff will provide assistance and technical advice as required in all matters concerning the use of the system.

19.0 RECORDED MATERIAL AND STILL IMAGES

19.1 All recorded material produced from the CCTV system remains the property of SKDC and is protected by copyright until the point when the Authorised Body signs the “Transfer of Data” form and therefore becomes the Data Controller for that material. Recorded material is held for a maximum of 30 days unless retained for training purposes.

19.2 Recorded material shall only be used for the purposes as defined in the Code of Practice.

19.3 Access to recorded material will only take place as defined in this Code of Practice.

19.4 The showing of recorded material to the public will only be allowed in accordance with the law; either in compliance with the needs of the Police in connection with the investigation of crime, which will be conducted in accordance with the provisions of any relevant Code of Practice under the Police and Criminal Evidence Act 1984 and

any advice and guidance given to the Police from time to time; or in any other circumstances provided by law. All recorded material is subject to the conditions and provisions of the Data Protection Act and RIPA 2000.

19.5 The following points must be observed when handling recorded material:

- Random sections of footage should be checked monthly to check recording quality
- A library of blank discs specifically printed with a "South Kesteven District Council" design must be maintained which is sufficient for the purpose of the scheme
- Faults identified with the recording equipment should be immediately raised with the CCTV Supervisor.

19.6 Evidential use of recordings

- Any disc that is provided for evidential purposes must be of proven integrity
- Duty Operators will be required to provide the Police with witness statements required for evidential purposes
- Copy discs must be individually and uniquely identified and labelled
- An Incident Management Record must be maintained giving the exact date and time of the production of each disc, the name of the person requesting the evidence and the reason for the request
- A Master Copy and a Working Copy will be produced for each evidential request
- The Master Copy will be sealed in a numbered evidence bag
- All disc copies relating a specific incident will be handed over to the authorised body
- Evidential discs not collected by the authorised officer within six weeks of preparation will be destroyed
- Before any copies are removed from the Control Room, the seizure log must be completed and signed by an authorised officer
- By signing the seizure log, the authorised officer accepts responsibility for the retention, secure storage and of the evidential copies
- Evidential discs not collected by the authorised officer within six weeks of preparation will be destroyed

19.7 Police access to recordings

- Police may request evidential camera footage where the Police reasonably believe that access to such recordings is necessary for the proper investigation and detection of a particular offence or offences or for the prevention of crime
- Police may obtain access under the provisions of the Police and Criminal Evidence Act 1984 (PACE)
- Discs provided to the Police shall at no time be used for anything other than the purpose specified and identified when the discs are released to the Police by the Control Room
- Arrangements may be made from time to time for a Police officer appointed in accordance with liaison arrangements to visit the Control Room and confirm that agreed procedures are being followed

- Charges may be incurred by the Police to cover operational, administration and recording media costs. The Police Force(s) will be invoiced upon these charges being incurred

19.8 Third party access to CCTV images should be considered in accordance with the subject access requirements.

- Access to recordings may be obtained in connection with civil disputes by court order or be extended to lawyers acting for defendants or victims in connection with criminal proceedings

- No other access will be allowed unless approved by the individual appointed to have day-to-day responsibility for the scheme for reasons which fall within the purposes and objectives of the scheme and in accordance with the Code of Practice

- In certain circumstances within the boundaries of the Data Protection Act, Insurance Companies may have access to recordings of incidents in connection to their enquiries e.g. road traffic collisions

- Individuals are able to request images of themselves providing they are eligible and can prove their identity, the relevant application forms shall be made available on the councils website

- Charges will be incurred to cover operational, administration and recording media costs

19.9 It will be necessary to provide a viewing station and to make arrangements to protect the images of other individuals on recordings from being disclosed.

19.10 All still photographs released on DVD's will remain the property of the owner. A record will be kept of the reason for production of the photograph, date and time, the particulars of production of a live photograph, and information identifying the Control Room staff member responsible for producing the photograph.

19.11 Any still photograph released to the police will be dealt with by the police as an exhibit and shall be used in the course of their investigation to detect and prevent crime and disorder and may be used as evidence for prosecution. At no time should it be used for anything other than the purpose specified and identified when released to the Police.

20.0 REFERENCES AND USEFUL LINKS

Data Protection Act 2018

RIPA 2000

Protection of Freedoms Act 2012

Surveillance Camera Code of Practice, Home Office June 2013

Data Protection Code of Practice

Surveillance Camera Commissioner