

A Code of Practice for South Oxfordshire and the Vale of White Horse District Councils' Public CCTV Camera Scheme

INTRODUCTION

This Code of Practice is intended to set out standards and procedures for the management, operation and use of the Closed Circuit Television (CCTV) System under the control of South and Vale District Councils.

This code of practice reflects the Councils' consideration of the response to the 'Surveillance Code of Practice' published by The Home Office in June 2013 and 'In the Picture: A data protection code of practice' produced by The ICO in May 2015.

This code is also supported by an operational handbook which is adhered to by all authorised personnel operating the CCTV system. A copy of the handbook is held in the control room.

The Councils' scheme operates across six market towns in South Oxfordshire and the Vale of White Horse. There are 86 cameras in total, monitored from a control room within Abingdon Police Station, by staff employed by the district councils.

In addition to the Public CCTV Camera Scheme, the Community Safety Team manage the installation of temporary covert guard cameras to help victims of crime and vulnerable people feel safe in their own homes. Guard cameras are installed in accordance with data protection and reviewed periodically to ensure they are still required.

The Environmental Protection Team manage the installation of temporary covert cameras to detect and prevent the crime of fly tipping across the two districts. Signage is placed at these fly tipping hotspot locations informing the public that covert surveillance is potentially taking place. This means the

process is excluded from the requirements of RIPA as the surveillance is overt. These camera locations are periodically reviewed to ensure they are still required.

PRINCIPLE ONE

‘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.’

1.1 Aims of our CCTV scheme

- a) to contribute to the reduction of crime and fear of crime
- b) to provide a safer environment for the community across all areas covered by the scheme
- c) to manage demand on services through working together
- d) to protect vulnerable people
- e) to target and manage harm and risk

1.2 Purposes

- to help prevent, detect and reduce crime, disorder and anti-social behaviour.
- to help reduce the fear of crime by providing reassurance for all those who work, trade and visit the South and Vale Districts.
- to provide evidence to assist in criminal and civil cases.
- to assist statutory agencies (e.g. police) to deploy their resources effectively.
- to assist in the management of the public areas covered by the scheme and support local authority’s enforcement and regulatory functions.
- to assist in civil emergencies and countering terrorism.

Our cameras are permanently sited and have pre-set positions when not being controlled by authorised personnel. The need for and use of cameras and their pre-set positions are reviewed annually in association with Thames Valley Police (TVP) and other relevant stakeholders.

PRINCIPLE TWO

‘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.’

2.1 The system continuously records all camera inputs at a minimum rate of 12.5 images per sec. The images are retained for a nominal period of 31 days. The DVRs automatically over write the existing image data with new data which maintains a rolling first in first out retention process.

2.2 When cameras are commissioned a privacy impact assessment is completed. Where necessary, permanent ‘privacy zones’ are employed e.g. to block the view into a residential property.

2.3 Should any request for Regulation of Investigatory Powers Act (RIPA) or directed surveillance be requested or it is believed that the circumstances may require a RIPA authorisation, the necessary authority must be authenticated and the Supervisor notified as soon as possible.

PRINCIPLE THREE

‘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.’

3.1 Where cameras have been commissioned, signage is displayed to indicate the data controller of the system and appropriate contact details. Further information about our CCTV scheme is available on both district councils’ web sites:

<http://www.southoxon.gov.uk/services-and-advice/community-advice-and-support/community-safety/town-centre-cctv-schemes>

and

<http://www.whitehorsedc.gov.uk/services-and-advice/community-advice-and-support/community-safety/town-centre-cctv-schemes>

3.2 We produce quarterly CCTV performance reports which are created from statistical evidence recorded by operators when using the cameras to monitor. Each event is recorded as a ‘Record of Occurrence’ and captures information for a particular event e.g. camera used, type of incident, place, time etc.

3.3 A copy of this Code of Practice and the latest quarterly reports can be downloaded directly from the district councils' websites. They also display the relevant contact details for the CCTV Control Room.

PRINCIPLE FOUR

'There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.'

4.1 The system is managed and controlled as shown below:

Role	Responsible
Employer of CCTV Staff	South and Vale District Councils
Owner	South and Vale District Councils
Manager	South and Vale District Councils or nominated representative on behalf of owners
Data Controller	Chief Executive of South and Vale District Councils
Data Manager	South and Vale Community Safety Team Leader or CCTV control room supervisor for day to day management
Data Processor	South and Vale District Councils authorised personnel i.e. CCTV Operators

Operators have a clear guide to work to in the form of our operational hand book.

N.B. We use a contractor to deal with day to day maintenance and repair of equipment.

4.2 When newly appointed, our operators attend a course to earn the Security Industry Authority (SIA) CCTV operators' qualification. To lone work, they must acquire the SIA licence and undergo a three-month induction period, where they work alongside other operators and become familiar with basic procedures, our Code of Practice and operational handbook. Operators also undertake various training events as required by their employer.

4.3 A record of events is kept by the operator on duty – a daily log. Each event involving camera usage is recorded as a separate ‘Record of Occurrence’ log. Details of all visual material that is requested for evidential purposes is recorded on a central data base before it leaves the control room. Master copies of the material itself are held securely and then confidentially destroyed after three years.

PRINCIPLE FIVE

‘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.’

5.1 Rules, policies and codes of practice are laid out in this document and the accompanying operational hand book. All operators are expected to have sound knowledge of their content before lone working.

5.2 There is a declaration of expected behaviours for all visitors to the control room, situated at the entrance. Visitors must sign a register to show agreement to these conditions before entering the control room itself. There are also individual notices displayed around the control room as reminders of these conditions e.g. not to record footage on hand held mobile devices.

PRINCIPLE SIX

‘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.’

6.1 Images are stored on our servers for a nominal period of 31 days. Master copy of images on DVD-R or paper and associated documents are kept for three years and then securely destroyed via a confidential waste disposal collection.

6.2 When cameras are not being controlled by an operator, they are in a resting or pre-set position. This view is aimed to capture activity in possible ‘hot – spots’ and has been agreed with TVP. Each camera view is reviewed on a yearly basis. N.B. Some cameras have more than one pre-set position as they may be moved to support night time economy.

PRINCIPLE SEVEN

‘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.'

7.1 Even though the CCTV Control Room is situated within the Police Station, because it is run by the local councils, access to the control room is restricted via a coded key pad entry system.

7.2 Unauthorised personnel must sign a visitors' book, thus agreeing to the conditions of entry and attendance displayed at the entrance. Entry is strictly at the discretion of the Supervisor and/or operator on duty. All visitors are supervised at all times.

7.3 Viewing of recorded material is logged and all requests for copies of material are preceded by a formal, written request.

7.4 Release of data is only via a designated path backed up by designated request forms at discretion of The Data Manager or their representative.

7.5 Members of the public and other organisations such as insurance companies and solicitors can apply to view footage by submitting a subject access request form to the supervisor. Release of such footage will be judged on a case by case basis.

PRINCIPLE EIGHT

'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.'

8.1 Operators receive in house induction and on-going training to enable optimal use of the system. As outlined under Principle Four, all our operators must have an SIA licence and are vetted through Thames Valley Police.

PRINCIPLE NINE

'Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.'

9.1 As outlined under Principle Seven, we have clear procedures for accessing and using CCTV data. Any images captured are only accessible to authorised personnel and shared with those who have a legitimate interest e.g. police, other council departments.

PRINCIPLE 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.’

10.1 A yearly review of pre-set camera positions is undertaken in consultation with Thames Valley Police and other relevant stakeholders. Periodically, we carry out an in-depth review of camera usage in order to determine an ongoing need for cameras in any given location. Data acquired from camera monitoring is published in a quarterly report on the district councils’ web sites.

PRINCIPLE 11

‘When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is pressing needs 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.’

11.1 Where requested, footage or stills are released to police officers with witness statement. Operators would also make themselves available for a court appearance if requested.

11.2 Requests from council colleagues, other organisations e.g. solicitors or insurance companies or members of the public are also considered. However, there must be an identifiable purpose and benefit indicated in any subject access request made. Any release of material to another party is at the discretion of the Data Manager or their designated representative.

PRINCIPLE 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.’

12.1 Only data relevant to a specific request is released. Each ‘job’ is given its own unique reference number and details are recorded electronically in a central database. All information, hard copy or electronic, is retained for three years after which time it is permanently deleted or securely destroyed.

12.2 Master copies of all footage and stills are kept for three years and again, securely destroyed.

Signed by Community Safety Manager

.....*Shona Ware*..... (Signature)

.....*13 February 2018*..... (Date)