2015

CCTV Code of Practice

For the Operation of Closed Circuit Television and Door Access/Concierge System

Version 1.2 June 2015

Overview

This Code of Practice has been prepared to ensure that Solihull Metropolitan Borough Council and Solihull Community Housing's use of Closed Circuit Television systems (CCTV) is appropriate and compliant with the Data Protection Act 1998 and the Information Commissioners "CCTV Code of Practice – 2008" and the "Surveillance Camera Code of Practice – June 2013"

VERSION CONTROL

Title: CCTV Code of Practice
Current version: 1.2
Document type: Draft
Prepared by: Corporate Information Governance Manager for Solihull Council and / CCTV Manager Solihull Community Housing
Approved by: The above
Review date: July 2018
Circulation: All employees / Intranet / CCTV Control Rooms / West Midlands Police

Document revision dates

Revision	Date	Revision description
0.1	September 2013	Draft created.
0.2	October 2013	Feedback from SCH CCTV Control Room Manager, Council's Senior Engineer incorporated into the document.
0.3	November 2013	Feedback from the Council's Litigation Team Leader and Senior Engineer (Traffic Mgt) incorporated into the document.
1.0	July 2014	Final copy agreed by SCH CCTV Control Room Manager, Council's Senior Engineer and CCTV Contractor
1.1	October 2014	Updated to reflect new access arrangement's for blue light services to CCTV images
1.2	June 2015	Updated to reflect operational changes due to change of contractor to CENTRO

CONTENTS

Deciding Whether to Use CCTV

Ensuring Effective Administration

Selecting and Siting the Cameras

Using the Equipment

Storing and Viewing Images

CONTENTS

This Code of Practice has been prepared to ensure that Solihull Metropolitan Borough Council and Solihull Community Housing's use of Closed Circuit Television systems (CCTV) is appropriate and compliant with the Data Protection Act 1998 and the Information Commissioners "CCTV Code of Practice – 2008". It will also help ensure

compliance with the Protection of Freedoms Act 2012 and the accompanying Home Office guidance entitled “Surveillance Camera Code of Practice – June 2013”

Housing and Concierge systems

Solihull Community Housing’s CCTV system consists of more than 40 sites spanning the whole of the north of the Borough. These sites include high rise blocks of flats, office facilities, and local area housing offices which are managed by Solihull Community Housing (SCH) on behalf of Solihull Council.

The system is overseen by the SCH Estate Manager. The system comprises of a number of cameras installed at strategic locations both within premises and externally. All the cameras are fully operational, some with pan, tilt and zoom facilities (PTZ) and others are fixed cameras. Live images from all cameras are presented at the SCH CCTV Control Room. A Personal Address System (PA) is in operation at all High Rise Flats which consists of a two way audio feed activated by personnel requiring assistance.

Council Town Centre CCTV

The system is overseen by the Council’s Senior Engineer and monitors Solihull and Shirley Town Centres, Solihull Car-Parks and industrial and small shop units. The Control Room is linked to the Retail Radio system and takes Out-of-Hours emergency calls for the Council. There is also a facility for relaying images to the Council’s Emergency Planning Office should there be a major incident. More recently the Solihull BID has afforded an additional CCTV Operator at peak times to focus on the town centre night-time economy activity and provide enhanced retail liaison. Some cameras have pan-tilt & zoom facilities others are static, some are linked to alarms. Live images from all cameras are presented at the Council’s CCTV Control Room.

Traffic Monitoring and Control

Solihull’s Urban Traffic Control (UTC) centre has nine fixed dedicated fibre full PTZ cameras and ten dial up mobile cameras for traffic monitoring. These are located at strategic points on the highways network around Solihull in order to identify and assist with the management of traffic congestion. Images from the nine fibre PTZ cameras are fed into the UTC centre via the main Council CCTV Control Room matrix whereas as images form the mobile dial up cameras are fed directly to a PC situated in the UTC centre.

SELECTING AND SITING THE CAMERAS

1.0 Responsibilities

Solihull Metropolitan Council

1.1 Although Solihull Metropolitan Borough Council (the Council) has appointed Solihull Community Housing (SCH) to manage its housing stock and tenancies under an 'Arms Length Agreement', it continues to be legally responsible for all information held about housing stock and tenants. The Council, therefore, remains the Data Controller in respect of any personal data processed in connection with this statutory function.

1.2 As Data Controller:

- The Council's Corporate Information Governance Manager will be responsible for ensuring that there is appropriate policy and guidance in place regarding the use of CCTV.
- The Council's Senior Engineer will maintain overall responsible for ensuring compliance with legislation governing the use of Town Centre CCTV.
- Day to day responsibility for the operation of the CCTV System will be the responsibility of the CCTV Manager. In the case of contractors the CCTV Manager might not be based in the control room but either they or a nominated representative will be available 24 hours per day.

1.3 For the purposes of directed surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA):

- The Council's nominated RIPA coordinator is the Council's Litigation Team Leader.

Solihull Community Housing

1.4 As System Controller, SCH's representative will be the Estate Manager in respect of the overall management of the SCH CCTV and Concierge systems. The Estate Manager has appointed a CCTV Manager to supervise the day to day operation of the CCTV and Concierge systems.

1.5 Formal consultation will take place between the System Controller's nominated representative and the Data Controller's nominated representatives with regard to all aspects, including this Code of Practice and any relevant Procedural Manuals.

1.6 The System Controller will provide information and access to facilities as may be reasonably requested by the Data Controller.

1.7 The System Controller will report to the Data Controller, without delay, any alleged or actual breach of confidentiality or security. The System Controller will allow the Data Controller to conduct such investigations as may be necessary and will act upon any recommendations that may transpire from an investigation.

2.0 Contractors

2.1 SCH and the Council may appoint a company or organisation to operate the CCTV and Concierge systems on its behalf. Wherever a surveillance camera system covers public space a CCTV Operator should be aware of the statutory licensing requirements of the Private Security Industry Act 2001. Under these requirements, the Security Industry Authority (SIA) is charged with licensing individuals working in specific sectors of the private security industry. A public space surveillance (CCTV) licence is required when operatives are supplied under a contract for services. It is a criminal offence for staff to carry out licensable activities without an SIA licence.

2.2 The Contractor is responsible under the contract requirements for ensuring the operators they have the required qualifications and licence and that they are renewed as required.

3.0 Objectives of the System

3.1 The objectives of the CCTV and Concierge systems, which form the lawful basis for the processing of data are:

a) The prevention and detection of crime and disorder.
b) To enhance community safety and help reduce the fear of crime, to protect the health, safety, well-being and welfare of residents, visitors and employees.
c) The provision of access control to controlled areas.
d) To assist The Council where appropriate in the general management of areas controlled by The Council's CCTV systems including housing stock, tenancies and town centres.
e) Traffic Management.

SCH CCTV and Concierge systems

3.2 These have been installed with the aim of providing a safe and comfortable environment for the benefit of all those who live in, work, or visit the facilities managed by SCH. In more detail the purposes for which the CCTV and Concierge system are:-

- To provide a concierge function to allow access to genuine trades people (vetted using the ID card as a means of cross reference) and to thereby only allow access to residents and genuine visitors. Where bogus callers are identified, evidence of their activities should be gathered and steps taken to ensure that they do not obtain access to the block.
- To verify the identity of residents when accessing the blocks, by cross referencing them to tenancy information provided by SCH. To deal with callers to the block(s) for residents who do not want to be disturbed, or where anti social behaviour requires management intervention.
- To identify and report incidents of vandalism, graffiti, drug abuse, anti-social behaviour, fly tipping, loitering and gather evidence of the person or persons carrying out these criminal acts. To make recommendations on the placement of cameras to assist addressing these issues.

- Provide evidence on the frequency of residents visiting their blocks to assist in the enforcement of tenancy conditions (identification of sub-letting or mis-use of property).
- To speak via the public address system, to any persons identified loitering in or around the block, particularly around the communal entrance during the hours of **09.00am to 21.00pm**.
- To speak via the public address system through a two way audio feed activated by personnel requiring assistance and entry into SCH's property.
- To report high priority incidents directly to the Police and to report incidents of a lower priority to the Low Level Anti Social Behaviour Team (LLASB).
- Operation of SCH KEYFAX system for advice and assistance to residents.

Monitoring of other Public Spaces

3.3 CCTV in Solihull was first introduced in 1992 to monitor the town centre multi-storey car parks. In 1997 when Home Office funding became available the Service was extended to cover the town centre. The Service has since expanded to include new internal Council customers, e.g. schools, property, parks and cemeteries. In Solihull the CCTV Service is very much valued and seen as 'critical' by the Police, our Town Centre partners and Solihull BID (and integral to partnership working and broader town centre safety and economy objectives).

3.4 The Police are able to offer many examples of where CCTV use and evidence has led to the prevention and detection of crime (some very serious with involvement of firearms) and enhanced their own personal safety in operations. There are also examples of its use for safeguarding purposes (involving lost children and missing persons, some very vulnerable). Records show that in 2009 the Police made 80 requests for potential evidential footage for use in prosecutions, in 2010 it was 82 and in 2011 to date it is 48. Over a typical Thursday to Sunday peak night-time economy period, there is almost continuous contact between the Police and the CCTV Service with 30 to 40 contacts to identify early disorder and help aid arrests (mainly alcohol and assault related).

3.5 Our Town Centre partners and Solihull BID also feel very strongly that the CCTV is integral to maintaining and enhancing the vitality of Solihull's town centre day and night-time economy.

Traffic Monitoring

3.6 CCTV cameras were first installed in the UTC centre for traffic monitoring purposes in 2001; in line with the Traffic Management Act the main objectives being –

i. To contribute to improvements in vehicle and pedestrian journey times, a reduction in delays and to help assist with efficient use of the highways network.

ii. To assist in the management of incidents on the highways network.

iii. To assist with day to day traffic management of the highways network.

iv. To assist the Police in managing the highways network.

v. To support neighbouring West Midlands Local Authorities with cross boundary highways issues.

Rationale

3.7 CCTV can be privacy intrusive, as it is capable of putting a lot of law-abiding people under surveillance and recording their movements as they go about their day to day activities. Careful consideration should be given whether to use it; the fact that it is possible, affordable or has public support should not be the primary motivating factor. The Council and SCH will take into account what benefits can be gained, whether better solutions exist, and what effect it may have on individuals.

3.8 Determining whether to use CCTV, the benefits to be gained, the location of cameras and the number of cameras used requires careful consideration. The Council and SCH will work with partners such as the Police, CENTRO and the Safer Solihull Partnership under a framework which considers alternative interventions like mobile cameras and the development of a business case for permanent CCTV from the lead proposer (being the partnership organisation that promotes expansion) to carefully consider such matters and to ensure that the use of CCTV is justified and is a proportionate and measured response to the goals it is aiming to achieve.

3.9 The use of CCTV will be regularly reviewed to ensure it remains to fulfil its stated objectives and compliance with this code by for example the completion of Privacy Impact Assessments.

4.0 Use and Control of Images

4.1 All personal data obtained by virtue of CCTV and Concierge systems shall be obtained fairly and lawfully and, in particular shall only be processed in the exercise of achieving the stated objectives of the system.

4.2 In processing personal data there will be total respect for everyone's right to respect for his/her private and family life and their home.

4.3 The processing of the data will be strictly in accordance with the requirements of the Data Protection Act 1998, the Information Commissioner's CCTV Code of Practice and other relevant guidance such as the "Surveillance Camera Code of Practice – June 2013".

The Data Controller for the CCTV and Concierge systems is:
Solihull Metropolitan Borough Council
Council House
Manor square
Solihull
West Midlands
B91 3QB

4.4 The SCH CCTV and Concierge system will be covered under the Data Controller's notification with the Information Commissioner (Notification Number: Z5888433)

4.5 The day today responsibility for the management and operation of the SCH CCTV and Concierge system will be devolved to the system controller, namely:

Solihull Community Housing
Endeavour House
Meriden Drive
Solihull
West Midlands
B37 6BX

5.0 Training

5.1 All equipment associated with, and recorded information gathered by, CCTV Systems will be handled only by authorised personnel who have been properly trained.

5.2 Each person having direct involvement with the system will be able to access a copy of both this Code of Practice and any associated Procedural Manuals. They will be fully conversant with the contents of the documents, and will be expected to comply with them at all times.

5.3 Each member of staff/contractors responsible for the operation of CCTV and Concierge systems staff will read the Code of Practice and associated Procedural Manuals and will sign to confirm this. A record of this will be kept on their personal file. Appropriate supervising arrangements will be in place to ensure the CCTV Operators engaged in the provision of the service are adequately supervised and properly perform their duties.

5.4 All CCTV Operators must have been security checked prior to the commencement of their employment of contract, and have signed a confidentiality agreement regarding anything they see during the course of their employment, or contract.

5.5 All staff employed within the CCTV Control Room will have completed their PSS CCTV Course and hold a current licence issued by the Security Industry Authority or dispensation license.

5.6 Staff will be properly and presentably dressed in the appropriate manner in accordance with the Council's Dress Policy or Contractors Company Policy.

5.7 Where a person's employment is terminated, he/she shall be required to cease use of the CCTV Control Room immediately.

5.8 The appointed maintenance contractor or manufacturer for the CCTV system will train the CCTV Operators in the use of the CCTV equipment who may also receive awareness training from the Police, to ensure that staff are aware of legal evidence requirements and patterns of suspect behaviour.

5.9 If the CCTV system is changed or extended then the CCTV Operators should receive further training from the installers.

5.10 CCTV Operators should receive ongoing evaluation of their performance and be subject to ongoing training as may be necessary to ensure a high standard of performance.

5.11 The appointed CCTV Manager(s), will ensure that new or relief CCTV Operators are fully briefed and trained on all functions, operational and administrative, arising within the CCTV operation.

5.12 Any breach of these conditions may be dealt with as a disciplinary matter.

6.0 General Principle

6.1 It is essential that the location of the equipment is carefully considered. Any CCTV images must be adequate for the purpose for which they are being collected. The cameras must be sited and the system must have the necessary technical specification to ensure that images are of the appropriate quality.

7.0 Operating Standards

7.1 The equipment should be sited in such a way that it only monitors those spaces which are intended to be covered by the equipment.

7.2 Operators must be aware of the purpose(s) for which the scheme has been established.

7.3 Operators must be aware that they are only able to use the equipment in order to achieve the purpose(s).

7.4 If cameras are adjustable by the operators, this should be restricted so that operators cannot adjust or manipulate them to overlook spaces which are not intended to be covered by the scheme.

7.5 If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the scheme, then operators should be trained in recognising the privacy implications of such spaces being covered. For example – individuals sunbathing in their back gardens may have a greater expectation of privacy than individuals mowing the lawn of their front garden.

7.6 If domestic areas such as gardens or areas not intended to be covered by the scheme border those spaces which are intended to be covered by the equipment, then the Data Controller or nominated representative such as SCH should consult with the owners of such spaces if images from those spaces might be recorded. In the case of back gardens, this would be the resident of the property overlooked.

8.0 Signage

8.1 Signs should be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment. The signs should be clearly visible and legible to members of the public.

8.2 Signs should contain details of the organisation operating the system and or Data Controllers details, the purpose for using CCTV and who to contact about the scheme (where these things are not obvious to those being monitored).

8.3 Signs should be an appropriate size depending on context, for example, whether they are viewed by pedestrians or car drivers.

9.0 Quality

9.1 The quality of the images that will be necessary must take into account the purpose for which CCTV is being used. For example, monitoring traffic flow will require a lesser quality of image than CCTV used to recognise a person's face for the purposes of law enforcement.

9.2 High level of compressions settings may result in poorer picture quality. Any compression setting will take into account the quality of the images that are necessary for the purpose of the CCTV monitoring taking place.

9.3 There will be regular checks to ensure that the time and date stamps of images remain accurate and that the quality of recorded images remains sufficiently clear.

STORING AND VIEWING IMAGES

10.0 General

10.1 The appointed CCTV Managers in each CCTV Control Room will undertake all the actions necessary to perform the service in accordance with the purpose of the scheme and in particular in accordance with the Code of Practice and any associated Procedures Manual.

11.0 Description of Duties

11.1 Duties of the CCTV Managers shall include but not be limited to:-

- The management and supervision of the CCTV Control Room, staff and all the operations and activities undertaken by such staff within the CCTV Control Room.
- The management and control of the security of and access to the CCTV Control Room.
- The management and control of the integrity, security and confidentiality of all the information and recorded material associated with the provision of the service.
- The operation of the CCTV Control Room 24 hours per day 365 days per year.
- The operation of the CCTV & Concierge system and continuous surveillance of all the monitors within the CCTV Control Room.
- Referring incidents to the West Midlands Police in accordance with Solihull MBC Exchange of Information Protocol.
- Regular checking of the CCTV & Concierge system and the reporting of any malfunction.
- Liaising with Council Departments during normal working hours.
- Operation of all necessary telephone and radio telephone systems, within the CCTV Control Room.

STORING AND VIEWING IMAGES

12.0 Camera Control

12.1 The primary role of a CCTV Operator is the monitoring of the live images, according to the schemes requirements and responding to live images that they see via the CCTV Cameras and to provide a Concierge service to all residents of high rise blocks.

12.2 At least one controller must be present within the CCTV Control Room throughout operating hours, to allow camera surveillance to be maintained at all times.

12.3 Only CCTV Control Room staff authorised by the appointed CCTV Manager may operate the cameras.

12.4 Any person operating the cameras will act with utmost probity at all times.

12.5 The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.

12.6 The observation log must be completed when checks are carried out, incidents arise and when formal requests are received from the Police.

12.7 Proactive monitoring should take place at all times performing regular tours which involve the viewing and checking of each camera on each site. Several of the optical sites also contain warning systems to alert the CCTV Operators of any activity in areas alarmed.

12.8 The camera tours are monitored in accordance with a set timetable. These guard tours also allow CCTV Operators to check the equipment as well as the site.

12.9 If sites have alarms and sensors connected to the cameras, the CCTV Operators should respond to these when they are activated.

12.10 CCTV monitoring arrangements need to be relatively flexible in order to respond to changing issues on a daily basis.

13.0 Audio Broadcast

13.1 When a CCTV Operator, monitoring cameras, views a situation, which could lead to an injury, crime or distress but might be prevented by intervention with a warning, where present, the public address system should be used.

Examples of such situations are:

i. Suspicious behaviour.
ii. Offensive behaviour.
iii. A crime being committed.
iv. A person in view of a camera is incapacitated or in a distress situation.
v. The area required is to be evacuated on instructions from Police.
vi. The area in question needs to be kept clear at all times for emergency vehicles, or to assist The Council in the maintenance of the Waste & Recycling collection/contract.
vii. Behaviour likely to cause damage or injury to property/public.

13.2 Assessment of some situations will be subjective and the CCTV Operators will need to use discretion and judgement. If in doubt about the use of the system the CCTV Manager on duty in the CCTV Control Room should be consulted.

Issuing Warnings and Alerts

13.3 To issue a warning the CCTV Operators will select the camera viewing the situation on a spot monitor, switch on the P.A. system. The warning(s) should be brief, clear and targeted at the offender. The CCTV Operators should not converse with the public.

For example in the case of anti-social behaviour:

"This is a security announcement – you are in a CCTV controlled area and your actions are being monitored and recorded please leave the area or the Police will be called."

13.4 Microphones should only be active during transmission of the message.

13.5 Concierge systems may have a two way audio feed that is activated when persons requiring assistance make a call from a control panel. A two way audio feed is also available in communal areas within the blocks i.e. foyer area and lifts. This facility is in place to address anti-social behaviour in communal areas and assist where applicable with lift entrapments.

14.0 Audio Recordings

14.1 The Concierge and Public Address (PA) system will be the only part of the CCTV system to record audio. The purpose of the recording will be for the same purpose that the images are recorded and will therefore be retained for exactly the same length of time.

15.0 Equipment Functionality Checks

15.1 The functionality of all cameras, recording equipment and associated items must be checked at the start of every shift and then on a pro-active monitoring basis. All faults will be reported to the CCTV Manager. If a fault is identified then the Fault Reporting Process must be followed.

16.0 General Access Control

16.1 Appropriately trained and licensed personnel will operate the equipment located within the CCTV Control Room. The monitoring equipment associated with the Council's CCTV systems are situated within a dedicated CCTV Control Room.

16.2 All personnel entering the CCTV Control Room must provide proof of identity and confirm the reason for their visit.

16.3 All personnel entering the CCTV Control Room must sign the visitor's book and confidentiality agreement providing their name; organisation; date and time of entry/departure; purpose of visit.

Control room – Police Access

16.4 Police officers may require access to the CCTV Control Room for agreed purposes, these include:-

- Emergencies and major incidents.
- The viewing of recordings for evidence purposes.
- Liaison and training purposes.

16.5 All police officers entering the CCTV Control Room must register their entry and provide their name; organisation; date and time of entry/departure; purpose of visit. Non uniformed officers will be required to provide identification.

Operational Command of the System by the Police

16.6 The Police may make a request to control the use of the CCTV systems to which this Code of Practice applies. These circumstances may be a major incident or event that has a significant impact on the prevention and detection of crime or public safety.

16.7 Such requests will be viewed separately to the use of the systems' cameras with regard to the requirement for an authority for specific types of surveillance under the Regulation of Investigatory Powers Act 2000.

16.8 Any applications must be made in writing by a Police Officer with the rank of Superintendent or above.

Two ways in which command can be taken

16.9 **CCTV Control room normally staffed -** In the event of such a request being permitted, the CCTV Control Room will normally continue to be staffed, and equipment operated by, only those personnel who are specifically trained and authorised to do so. They will then operate under the command of the Police Officer designated in the written request.

16.10 **Police take control -** In very extreme circumstances a request may be made for the Police to take total control of the System in its entirety, including the staffing of the control room and personal control of all associated equipment, to the exclusion of all representatives of the Council or SCH. A request for total exclusive control must be made in writing by a police officer not below the rank of Superintendent or person of equal standing.

16.11 In case of emergencies when it is not practical to complete the paperwork in advance, the Police will telephone the control room in advance of taking control of the system or as soon as is practical after taking control. The appropriate paperwork will be completed after the event and signed off by a police officer not below the rank of Superintendent or person of equal standing.

16.12 When the Police take over control of the CCTV cameras they become the Data Controller for the duration.

Control room – Contractor Access

16.13 All visits to the CCTV Control Room by contractors must be by prior and must sign the visitor's book and a confidentiality agreement prior to entering the CCTV Control Room.

17.0 Guiding Principles

17.1 Members of the community must have total confidence that information recorded about their ordinary every day activities by virtue of CCTV systems will be treated with due regard. It is important that access to and disclosure of images recorded by CCTV systems is restricted and controlled. This will ensure that the rights of the individual are preserved and evidence remains admissible. Those involved in the operation and management of CCTV will need to ensure that the reason for the disclosing of images is compatible with the objectives of the CCTV scheme.

17.2 Every video or digital recording has the potential of containing material that has to be admitted in evidence at some point during its life span. Access to and the use of recorded material will be strictly for the purposes defined in this Code of Practice only.

17.3 For the purposes of this Code 'recorded material' means any material recorded by, or as the result of technical equipment which forms part of the CCTV and Concierge systems.

17.4 It is important that irrespective of the means or format (e.g. paper copy, video tape, digital tape, CD, or any form of electronic processing and storage) of the images obtained from the system, they are treated strictly in accordance with this Code of Practice and associated Procedural Manual from the moment they are received by the monitoring room until final destruction.

17.5 Recorded material will not be, sold or used for commercial purposes or for the provision of entertainment.

18.0 Recording Media

18.1 The CCTV Managers on behalf of the Council will ensure the CCTV System is fit for purpose this will ensure the rights of the individuals are preserved and evidence remains admissible.

18.2 The tracking record shall identify every use, and person who has viewed or had access to the Recording Media since the initial installation to the destruction of the Recording Media.

19.0 Recording Media – Retention of Data

19.1 Town Centre CCTV footage will normally be kept for 31 days before being overwritten. SCH CCTV footage will normally be kept for 14 days before being overwritten.

19.2 Upon receipt of a request to keep footage (e.g. Police or a member of the public), the footage will be stored separately in a secure area on the CCTV system for a period of 12 months before being deleted from the system. Any associated paperwork such as log books will be disposed of as confidential waste**.**

20.0 Copies of Information

20.1 A Media Copy is a copy of an image or images which already exist on video tape/computer disc.

20.2 Media Copies will not be taken as a matter of routine. Each time a copy is made it must be capable of justification by the originator who will be responsible for recording the full circumstances under which the copy is taken. The recorded details will include: the date, time and location of the incident, date of the production of the print and the identity of the person requesting the print, (if relevant) and the purpose for which the print was taken .

20.3 The records of the Media Copies taken will be subject to audit in common with all other records in the system.

21.0 General Principles - Release of Personal Data to Third Parties

21.1 Every request for the release of data generated by the CCTV or concierge systems will be channelled through the appointed CCTV Manager. The appointed CCTV Manager will ensure compliance with the Data Protection Act (Subject Access Provisions) at all times.

All requests for the release of data generated by the CCTV System will be made in writing and will provide:-

- The name and other relevant identifying details of the person/agency making the request.
- Sufficient details to enable the CCTV Manager to locate the data being requested.
- If the request is being made by a third party, that party must provide the statutory reasons for requesting the data.

22.0 Information requests from Police and other law enforcement agencies

Routine requests for recorded images

22.1 West Midlands Police will submit a WA170 form. Other authorities and law enforcement agencies will submit their organisations equivalent form. If the request is received using the telephone, the CCTV Operators should advise the Officer of this requirement and ask him to send the written request prior to visiting the CCTV Control Room.

Emergencies/Serious Incidents

22.2 Urgent requests for viewing will be accepted if a major crime/incident is involved, or where the Police are holding a suspect in custody. Examples of a major crime are: Murder, Assault, and Robbery.

22.3 Where law enforcement agencies have identified a serious incident which requires immediate intervention, it may not be possible to produce a WA170 or equivalent prior to the request. In cases of emergency when there is not enough time to complete the paperwork up front the paperwork must be completed after the event.

Blue Light Services indirect access to CCTV images

22.4 Upon receipt of a request, the CCTV control room will be able to relay real-time images from CCTV cameras directly to blue light services at pre-determined locations. All such requests will be logged and regular reports produced for the Council's Senior Engineer, senior leads from the various blue light services and other key stakeholders to scrutinise in order to ensure that access has been appropriately exercised.

22.5 The blue light services will become the Data Controller for the images they receive.

Directed Surveillance – RIPA

22.6 Directed Surveillance is:

- covert, but not intrusive surveillance;
- conducted for the purposes of a specific investigation or operation;
- likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information;
- it is conducted **otherwise** than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought

22.7 Directed Surveillance must only be carried out if the appropriate requests are made as specified by RIPA, with the relevant authority and time period.

22.8 Directed surveillance rules apply to both where the CCTV Operator is asked to target someone and where the Police ask to take control of the cameras for this purpose

22.9 All staff responsible for CCTV cameras and the recording of images must be able to recognise a request that requires RIPA authorisation and what such a request must contain.

23.0 Subject Access Request

23.1 When a request for details of or to view personal data is received from an individual (Data Subject) under the Data Protection Act 1998, the individual must provide sufficient information to prove that they are the subject of the video footage, e.g. a photograph.

23.2 Steps should be taken to edit the video footage so that the Data Subject does not receive information they are not entitled to and to protect the privacy of others, e.g. this may require the pixilation of other people faces.

24.0 Request to view images from Staff/other agencies

24.1 An information and or viewing request form should be completed in every circumstance where staff are requesting to obtain information and or images from the CCTV and Concierge system. Staff should only request information in pursuance of the objectives of the scheme or related proceedings.

SCH FOB MANAGEMENT PROTOCOL

Introduction

This document has been produced to assist staff that will be issuing and reprogramming 'Fobs'.

By early 2007 all high rise blocks had a CCTV and Access Control system (ACS) installed. This system was implemented following a planned programme. The ACS assists in providing a safe and secure environment for the benefit of those who live, work or visit high rise blocks.

Access Control System

The Access Control system means that access through the door entry will be by means of a fob. Every resident will be issued with a new programmed door entry fob. Each fob issued will be unique to the tenant and registered onto the Fob Management database using the tenants name and address. The fob will only allow access into the block if they live in that particular block.

The CCTV cameras will be monitored by CCTV Operators who will also operate the door entry, Concierge and Access Control system. Staff will also administer the system by inputting relevant data, for example the system is able to hold details of tenant's car registration numbers and carer's details.

The system is able to produce reports showing fob usage and staff members are able to delete track and monitor fobs.

Fob management integrity

To maintain the integrity of the Fob Management database it is essential staff follow these guidelines for the operation of the system.

The Data Protection Act requires SCH to ensure that only personal data will be held which is adequate and relevant for the purposes specified in this protocol. It is each officer's responsibility to ensure that personal data is accurate and up to date. Staff should advise tenants at the time of issue that their fob is a unique access token which is registered to them to maintain the security of the block. Only residents and bona fide visitors will be allowed access to the block.

Installation of Access Control System into a block

Each resident of a block returned their existing fobs to the engineer at the time their handset was installed. The existing fobs were replaced with a new-programmed fob that was programmed and registered to each individual tenant.

The new fob issued holds a unique registration to the tenant and the block (as per allocation guide below). The unique registration will be held on the Fob Management database. The Fob Management Database will be linked to the Concierge system at the CCTV Control Room. Fobs are easily identified and can be deleted to prevent unauthorised access. The system records each time a fob is used to access the block and this information can be used for Housing Management purposes. For example, monitoring anti social behaviour, access control, tenancy management etc. All requests for information should be directed to the CCTV Manager.

SCH FOB MANAGEMENT PROTOCOL

The concierge operators, at the CCTV Control Room, will be on duty 24 hours a day seven days a week (24/7) and will allow access to these users once confirmation of identity has been established.

How fobs are allocated

The number of free fobs allocated depends on whether it is a single or joint tenancy.

- Single Tenancy 1 fob to be issued
- Joint tenancy 2 Fobs to be issued (Colour coded as per instructions below)

Lost or faulty fobs

Tenants should report lost or faulty fobs to an Area Housing Office. Replacement fobs will be recharged at a cost of £10 each.

Faulty fobs will be replaced free of charge.

Staff should access the GDX Fob Management database to identify current fobs programmed to the tenancy. Once the fob has been identified it should be deleted from the database.

Faulty fobs should be returned to the Estate Manager at Endeavour House using the internal post system.

Fobs should only be programmed and registered to the tenant, once they have accepted and signed for the tenancy.

N.B All fobs should be deleted from the database even if the actual fob has not been returned. Tenants should be advised the fob will be deactivated and will no longer allow access. Tenants should be advised that they will be charged if the fob is not returned.

Abandoned Tenancies

The Fob Management system allows tagging of fobs. This will be useful in the monitoring of abandoned tenancies as tagging a fob will trigger an alarm on the concierge user screen at the CCTV Control Room. The tagging of a fob will not prevent access to the block, but will enable the CCTV Operator to alert the relevant Officer, should it be used. Staff should request this information via the CCTV Manager.