STOCKPORT HOMES GROUP CCTV CODE OF PRACTICE

23 August 2018

Prepared by:	Lisa Delezio	EIA Required?	☐
Date effective from:	23/08/2018	EIA Completed?	☐
Policy approved by:	Simon Welch	Revision number:	2
Review Date:	28/08/2021	Lead officer:	Jane Allen

1 INTRODUCTION

1.1 Stockport Homes Group (SHG) operates a Closed Circuit Television system (CCTV) in a number of its managed properties in the Stockport borough.

1.2 This Code of Practice defines the operational and management of the SHG CCTV system.

1.3 SHG has a legal requirement to ensure that the CCTV system is effective and appropriate to its purpose.

2 THE CCTV SYSTEM

2.1 The day-to-day management of the CCTV system and compliance with the Code of Practice is the responsibility of the Carecall Concierge Manager (CCM).

2.2 The CCTV system is housed in the Control Room, based within the Control Centre at Cornerstone, 2 Edward Street, Stockport, SK1 3NQ.

2.3 Footage captured on the CCTV system can be viewed and downloaded in the Control Room using the playback system.

2.4 The CCTV system comprises of moveable and static colour dome cameras situated on intercom panels and throughout the area in various locations. Cameras are located internally and externally.

2.5 The equipment has the capability of recording footage via all cameras simultaneously 24-hours a day. The CCTV system has the capacity to store data, at a minimum this would be for 23 days after recording in all cases.

3 PURPOSE OF THE CCTV SYSTEM

3.1 The CCTV system is intended to provide an increased level of security within a number of areas monitored for the benefit of those that live, work, trade or visit the building/area.

3.2 The CCTV system has been designed to:

- Monitor and protect Council and SHG owned assets and business interests.
- Reduce the fear of crime and Anti-Social Behaviour (ASB) and to help secure a more attractive and safer environment.
- Reduce the incidence of criminal damage, vandalism and graffiti.
- Enhance public safety in and around the monitored areas.

- Help prevent crime by deterring and detecting criminal activity and ASB, identifying and providing evidence (of a quality recording) that assists the Police and SHG's ASB team in the apprehension of offenders or perpetrators of ASB that may lead to prosecution or other legal action.

4 LEGAL REQUIREMENTS

4.1 The Code of Practice complies with relevant legal requirements regarding the management of CCTV. These are:

- Data Protection Legalisation
- Freedom of Information Act
- The Human Rights Act
- Health and Safety (Display Screen Equipment) Regulations
- Police and Criminal Evidence Act (PACE)
- Civil Evidence Act
- Regulation of Investigatory Powers Act (RIPA)

5 CONTROL ROOM

Control Room Arrangements

5.1 All staff operating the CCTV system will be suitably trained to fulfil their duties.

5.2 There must always be at least one member of staff in the Control Room at any time. Two staff members will be present at peak times (2.00pm-10.00pm weekdays, 6.00am – 10.00pm weekends and bank holidays).

5.3 All staff members must electronically sign the Concierge Audit Log at the beginning and end of each shift (stored on the Carecall Concierge drive).Staff members take breaks from viewing the screens on a rotational basis – no less than every two hours.

Control and Operation of Cameras

5.4 Daily checks of all cameras and the playback system are made to ensure their recording functions are in working order. Where a fault is found, this will be recorded on the Openview Portal for repair.

5.5 Staff operating camera equipment are required to act with integrity and be aware that recordings are subject to routine audit.

5.6 As a requirement of the organisation's Code of Conduct and other data protection legislation, staff will be expected to adhere to high levels of confidentiality regarding an individual's right to privacy.

5.7 Staff that are suspected of abusing the CCTV system will be formally investigated under the SHG Disciplinary Policy, Procedure and Guidance on the grounds of misconduct or gross

misconduct. Allegations of gross misconduct that are proven may result in dismissal.

Control Room and Viewing Room Access

5.8 The Control Room is secured by fob access which limits access to only those who have a responsibility to operate and manage the CCTV system or staff, or for those who have responsibility for facilities management. Non-Carecall Concierge staff will always be supervised whilst in the Control Room

5.9 The Viewing Room is located within the Control Room in a private lockable room, away from the main office space.

5.10 Access for contractors will be necessary from time to time for the purpose of maintaining the Control Room and its equipment. This will be limited to that strictly necessary for work. At no time should contractors be left unattended and their attendance will be recorded in the Visitors Log Book.

5.11 Other visits to the Control Room for any purpose must be approved by a member of the Carecall Concierge Management Team and recorded in the Visitors Log Book.

6 DATA

6.1 The CCTV system will only hold data for the purposes specified and staff can only disclose information to people or agencies as defined within this Code of Practice.

Personal data

6.2 Electronic personal data is stored in the form of:

- Visual recordings
- Name, emergency contact number and date of birth for all tenants in receipt of the Concierge service.

6.3 All personal information stored should be accurate and of a good quality admissible in a Court of Law. Storage of data should follow guidelines laid down by the Data Protection legalisation.

Recorded material

6.4 SHG has ownership and copyright of all recorded material.

6.5 Recorded material will only be used for purposes defined in this Code of Practice.

6.6 No information processed by the cameras will be sold in any form to any outside agency for commercial, documentary or entertainment purpose.

Use of Removable Media

6.7 Data will be stored on hard drives and retained for a minimum of 23 days before it is over-written.

6.8 Data required for evidential purposes is recorded onto removable media and issued to the requesting organisation following proper authorisation. Evidential data should be copied within this timeframe to ensure it is available and not overwritten.

6.9 Copies of data can be made to a removable media device. Once the copy has been made and issued, storage of the data reverts back to using the hard drive. In normal circumstances, no data is stored on disc.

Sharing Data with members of the public

6.10 Under Data Protection legalisation members of the public have the right to obtain a copy of their personal data as well as other supplementary information.

6.11 The Information Governance Policy describes the SHG's approach to such requests for information. Requests for information are dealt with under the relevant legalisation (Freedom of Information Act/Data Protection Legalisation).

6.12 Requests for information should be directed to the Assurance Team (assurance@stockporthomes.org).

Sharing Data with other SHG staff members

6.13 There are particular roles with SHG that may from time to time, require data/information captured by the CCTV system, such as Neighbourhood Housing Managers, Neighbourhood Housing Officers, the Anti-Social Behaviour Team or the SHG Reception Management Team.

6.14 All requests for data/information must be requested using the CCTV Request Form, clearly stating the reason for the request.

6.15 Any footage that relates to potential criminal activity must be shared with the Police in accordance with the provision of the Police & Criminal Evidence Act 1984.

6.16 Where there are concerns over a request, the final decision as to whether the request will be fulfilled lies with the CCM, or in their absence another member of the Carecall Concierge Management Team.

Sharing data with other agencies

6.17 Access to data may be given:

- In connection with civil disputes where ordered by the Courts or in accordance with the provisions of the Civil Evidence Act 1995.
- To solicitors acting for defendants or victims in connection with criminal proceedings. Footage can be requested if the

defendant or victim is a data subject. Such requests should be made in writing and directed to the CCM who will authorise this with the Assurance Manager.

- To Stockport Council in connection with legal or civil action being taken regarding nuisance or other anti-social or criminal behaviour.

6.18 In some circumstances, approval for access to those not listed above may be given by the CCM.

Sharing Data with the Police

6.19 Where requests are made for footage from the Police that relates to the detection/prevention of crime or disorder, this can be shared with the Police in line with the Police and Criminal Evidence Act.

Exemptions of the Provision of Information

6.20 Data Protection legalisation recognises that it is sometimes appropriate to disclose personal data for certain purposes in relation with criminal justice. In these cases, individuals' rights may occasionally need to be restricted.

6.21 In particular, the Act deals with several situations in which personal data is processed for the following "crime purposes":

- The prevention or crime and disorder.
- The capture or prosecution of offenders.

Privacy of tenants

6.22 Cameras must not be used to look into residential property; this excludes surveillance of communal areas, pathways, roads, parking areas or service facilities such as lifts. Where the equipment permits it, digital privacy zones will be programmed into the system as required, in order to ensure that the interior of any private residential property within range of the system is not surveyed by the cameras.

6.23 Cameras adjacent to residential areas and properties will have electronic stops that will prevent intrusion of privacy, impact upon civil liberties and observations of private properties. Except wider angle, long distance or panning shots, every effort will be made to ensure that domestic premises are not included within camera's field of view in order to preserve personal privacy.

6.24 Cameras will be operated with due regard to the privacy of individuals and ad hoc spot checks will be made on staff operating the CCTV system.

7 EQUIPMENT - CAMERAS

7.1 The design and installation of the CCTV System will be overseen by the CCM and technical consultants, taking account of the needs of the

community and visitors and in liaison with the Police and other agencies as appropriate. The location of cameras will be co-ordinated to maximise coverage.

7.2 A maintenance agreement is in place with an approved Contractor who will attend critical fault within four hours of reporting

7.3 All CCTV cameras are not capable of recording sound.

7.4 In order to enhance public confidence in the system, dummy cameras will only be used when installed by the ASB team, in line with the ASB policy.

Placement of cameras

7.5 The cameras will be prominently placed in fixed positions within public view to obtain the best views for detection, to deter crime and anti-social behaviour and to assist the public to feel safer.

Camera capability

7.6 All cameras have high resolution colour capabilities to enhance images for easier identification, to aid detection of offences and ASB and to improve evidential material. Moveable dome cameras pan up to 360 degrees and tilt to required angles. Cameras will operate efficiently at night and in poor lighting conditions.

Remote control of the cameras

7.7 All moveable dome cameras are remote controlled from the Control Room. Cameras have automatic movement when not being operated manually and also have an auto park facility which returns the camera to a home position.

8 SIGNAGE

8.1 The public must be made aware of CCTV in operation to gain their understanding and acceptance. The following principles are adopted:

- Signs are displayed at key points clearly stating that a CCTV system is in operation
- Signs specify the general area that the system covers.

9 THE SIGNS CLEARLY IDENTIFY SHG AS BEING RESPONSIBLE FOR THE CCTV SYSTEM. SECURITY

Maintaining security of the Control Room and Viewing Room

9.1 SHG has in place security measures to prevent unauthorised or accidental access for the purpose of alteration, disclosure, or loss and destruction of information.

9.2 The hard-drive will be secured through password protection.

9.3 Removable media CDs and DVDs will be stored in a lockable cabinet within the Control Room.

9.4 The Control Room and Viewing Room will be kept secure at all times and arrangements include:

- Records are kept of all access to the Control Room and Viewing Room, recording details of the individual concerned and the times of arrival and departure
- The playback system will be password protected and only those granted access are provided with this
- Access to the Control Room and the Viewing Room will be restricted to specified persons who have been granted permission.
- Technical repairs will be carried out in controlled circumstances according to the maintenance arrangements in place
- Police visits will usually be prearranged and always recorded as with other visits

Major incidents

9.5 In the event of a major incident, the Business Continuity Plan contingency plans shall be activated between staff, the CCM, the Police, other emergency services and SHG's Management Team.

9.6 Should the Control Centre need to be evacuated, the GDX monitor will be switched to 'monitor' mode. This will automatically override the doors and send the intercom directly to the flat rather than the Control Centre. The CCTV will continue to record direct to the server and OpenView will be instructed to carry out a full check of the CCTV backups. No recordings should be lost as long as power supply is not affected at the recording sites. Within Cornerstone, there is an uninterrupted power supply of up to eight hours in the event of a power failure.

10 POLICE USE OF THE SYSTEM

Police Use of the System

10.1 Police use of the System must be in accordance with the Code of Practice and the Regulation of Investigatory Powers Act (RIPA) and the Police and Criminal Evidence Act (PACE)

10.2 On occasion, the Police may request to use or takeover the control of the CCTV System to view live images to monitor a serious incident.

10.3 If Police request access to live images, they must provide an application for the Use of Directed Surveillance under R.I.P.A (Regulation of Investigatory Powers Act.). This must be signed by a Superintendent or someone of a more senior rank.

Police Access to Data

10.4 The Police may apply for access to specific data in accordance with the agreement made with the CCM and where the Police reasonably believe that access to the said data is necessary for an investigation.

10.5 Data provided to the Police shall at no time be used for anything other than the purpose specified and identified when the data is released by the Control Room.

10.6 The Police can request to take possession of the original hard drive when a serious incident has occurred. Removal of the original hard drive must be authorised by the CCM. In the absence of the CCM, authorisation can be given by the Head of Neighbourhoods.

10.7 In cases of the Police requiring large amounts of footage, the original hard drive will be removed by the Police and a replacement hard drive will be provided by the Police.

Requests outside of the Code of Practice

10.8 Requests from the Police for use of the CCTV System in any manner that is not provided for by the Code of Practice, must be the subject of a specific agreement between the Head of Neighbourhoods and the Police prior to the use of the system, with the reason for the request stated in writing.

Recording the use of the system

10.9 When footage is downloaded to DVD as per the request of the Police, a copy must be filed onto the hard drive.

10.10 When using the CCTV system, the Police must supply a copy of an application for the Use of Directed Surveillance under R.I.P.A. which is secured in the Control Room for future audit.

10.11 Records with the same details are also retained by the Police. If monitoring is taking place by both the Control Room and the Police, recording will only be carried out by the Control Room to avoid creation of two sets of recordings.

11 CHANGES TO THE CODE OF PRACTICE

11.1 Major changes to the Code of Practice will only be made after appropriate consultation with relevant interested groups and will be reviewed in line with regulatory changes.