



Closed Circuit Television (CCTV) Policy

Originator:	Policy and Strategy Team
PCHA Approval Date:	5 th July 2022
Review date:	July 2025

1	Introduction
1.1	The Policy sets out measures that Pine Court Housing Association (PCHA) has in place for managing Closed Circuit Television (CCTV) / video surveillance systems and provision of associated services to other companies within the Sovini Group including out-of hours call services.
1.2	<p>This Policy sets out:</p> <ul style="list-style-type: none"> • How PCHA will comply with the principles (where applicable) of the Surveillance Camera Code of Practice (Amended November 2021) • The line management responsibility for the systems in operation including contract arrangements with an appointed third party 'system user' – (Arm Secure) • The type of systems in use • The purposes for which it will be used and the restrictions on its use • How data and images captured by the systems will be stored and disposed of • How requests to view data will be handled • How PCHA will report and review use of systems • How complaints about the operation of CCTV systems can be made
1.3	<p>The Policy covers:</p> <ul style="list-style-type: none"> • CCTV systems that are installed by PCHA (for the purposes of prevention of crime or disorder and to protect asset value) in buildings and communal spaces it owns and controls • Sovini Group sites where PCHA manages the CCTV contract on behalf of other Sovini entities
1.4	<p>Operation of the Policy ensures PCHA meets its legal requirements in the use of CCTV. The principle legislation in this area is as follows:</p> <ul style="list-style-type: none"> • UK Data Protection Act 2018 • UK General Data Protection Regulations 2018 • The Protection of Freedoms Act 2012

<p>1.5</p> <p>1.6</p> <p>1.6.1</p> <p>1.6.2</p> <p>1.7</p> <p>1.7.1</p> <p>1.7.2</p> <p>1.7.3</p> <p>1.8</p>	<ul style="list-style-type: none"> • The Freedom of Information Act 2000 • The Human Rights Act 1998 <p>In operating this Policy, PCHA also ensures compliance with the Regulatory Framework for Social Housing, adopted by the Regulator for Social Housing (RSH) as outlined below:</p> <ul style="list-style-type: none"> • Registered providers must work co-operatively with tenants, other landlords and relevant organisations to take all reasonable steps to ensure the safety of shared spaces <p>Access and Communication</p> <p>PCHA is committed to ensuring that its services are accessible to everyone. PCHA will seek alternative methods of access and service delivery where barriers, perceived or real may exist, that may make it difficult for people to work for PCHA or use its services.</p> <p>Working with our customers we have established a Vulnerable Persons and Reasonable Adjustments Policy to ensure we make best use of every customer interaction to meet customers’ needs in our service delivery and ensure this information is kept up to date.</p> <p>Equality, Diversity and Human Rights</p> <p>PCHA is committed to ensuring that no person or group of persons will be treated less favourably than another person or group of persons and will carry out its duty with positive regard for the following core strands of equality; Age, Disability, Gender, Race, Gender Identity / Gender Expression, Sexual Orientation, Maternity and Pregnancy, Marriage and Civil Partnerships, Religion and / or Belief.</p> <p>PCHA also recognise that some people experience disadvantage due to their socio-economic circumstances, employment status, class, appearance, responsibility for dependants, unrelated criminal activities, being HIV positive or with AIDS, or any other matter which causes a person to be treated with injustice.</p> <p>PCHA will also ensure that all services and actions are delivered within the context of current Human Rights legislation. PCHA will endeavour to ensure its staff and others with whom it works, will adhere to the central principles of the Human Rights Act (1998).</p> <p>This Policy should be read in conjunction with the:</p> <ul style="list-style-type: none"> • PCHA Complaints, Appeals and Feedback Policy • PCHA Information Management Policy • PCHA Data Protection Policy • PCHA Lift Maintenance Policy
<p>2</p> <p>2.1</p>	<p>Statement of Intent</p> <p>As a ‘System Operator’ PCHA will take decisions to deploy surveillance camera systems (CCTV) in appropriate areas of its operations and ultimately is responsible for the processing of images or other information obtained by such systems.</p>

2.2

PCHA will only operate CCTV systems in pursuit of the following legitimate aims:

- Promoting the health, safety and security of residents, staff and other users of buildings, communal areas and open spaces where PCHA has a controlling interest (including systems that ensure passenger safety in PCHA operated lifts)
- To maintain the asset value of properties and equipment owned by PCHA / other Sovini Group companies by deterring / preventing vandalism, theft or other forms of disorder
- Promoting early intervention actions that would save further damage to persons or properties
- Assisting in the prevention of crime, anti-social behaviour, public order offences, other statutory enforcement issues and in any subsequent apprehension / prosecution of those found to be responsible for these actions

2.3

PCHA will not use its CCTV systems for the purposes of:

- Recording sound
- Providing live streaming for use on the internet or commercial purposes

2.4

As a matter of good practice and to provide assurance to customers and others that may be affected by the use of its CCTV systems, PCHA and those managing services and processing data on its behalf will adhere (where applicable) to the 'Guiding Principles' of the Home Office – Surveillance Camera Code of Practice (Reviewed 2021), 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 user 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

2.5	<p>11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value</p> <p>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 (not applicable to PCHA systems)</p> <p>In operating CCTV systems, PCHA will also comply with the current and any subsequent guidance and good practice produced by the Information Commissioners Office and the British Standards Institute.</p>
-----	---

3	Policy
----------	---------------

3.1	Management Arrangements
3.1.1	PCHA have contracted out the operation of its CCTV systems to a National Security Accredited (NSI) and ARK Gold Cat 2 / Cyber Essentials certified third party 'System User', with the contract being managed on PCHA's behalf via Sovini Property Services (SPS).
3.1.2	<p>Responsibility for the operation of PCHA CCTV systems, review of effectiveness and continued use of such systems, authorisation for any amendment to systems including extended or reduced coverage or change of purpose for system use (following appropriate consultation and completion of a Data Protection Impact Assessment) rests with the Director of Operations:</p> <ul style="list-style-type: none"> • David Brown – Director of Operations 0151 709 6878
3.1.3	As the 'System Operator' PCHA will retain responsibility for developing and reviewing any joint working protocols that are established with the 'System User'.
3.2	PCHA CCTV Systems
3.2.1	<p>PCHA operate a number of CCTV systems across various locations in buildings it owns and controls including:</p> <ul style="list-style-type: none"> • Independent living housing – retirement living scheme • Office and business premises (including those owned by Sovini Group entities)
3.2.2	The system used across these locations include; fixed position cameras, pan tilt and zoom (PTZ's) cameras, monitors, multiplexers and digital recorders. The system will be capable of recording images in real time and time lapse mode but will not record sound.
3.2.3	All Cameras used by PCHA will be 'overt' and clearly visible at all times. Where PCHA operate CCTV cameras, appropriate signage will be displayed, and a regular audit schedule will ensure the signage is in situ and clearly visible.
3.2.4	The location and design of all CCTV cameras will be carefully considered to ensure:

- They provide maximum coverage of PCHA owned and controlled sites, whilst minimising unnecessary intrusion into private spaces
- They are secure and protected from vandalism
- They provide low maintenance and high operability at all times and are free from natural (e.g. trees, bird nesting opportunities) or manmade (e.g. passing traffic) obstructions from the areas they are intended to cover
- They provide the right quality of images to meet the required aims (as outlined above in 2.2)

3.3 **Control of Operations**

3.3.1 All images captured by PCHA CCTV systems will be relayed to its contacted 'System User', Arm Secure, which are based at:

- Arm Secure, Unit 10, The Alpha Centre, Armstrong Way, Yate, Bristol BS37 5NG

3.3.2 The Arm Secure facility is staffed 24 hours a day, 365 days a year and access where images are viewed is limited to those staff whose role it is to monitor the equipment / images, management personnel and authorised external parties such as the Police or other enforcement authority.

3.3.3 All Arm Secure staff will be appropriately qualified and have the appropriate level of Disclosure and Barring Service (DBS) checks before commencing employment and these will be refreshed, every two years.

3.3.4 The Arm Secure facility has appropriate security in place to ensure the safety of any data captured via PCHA CCTV systems and to guard against unauthorised use, access or disclosure.

3.4 **Data Security, Retention and Disposal**

3.4.1 All images captured by PCHA CCTV systems are digitally recorded, which aids ease of storage and retrieval when required. Access to the system is limited to authorised staff and appropriate security measures are in place to prevent external interception.

3.4.2 Arm Secure, working on PCHA's behalf will normally keep images recorded for a period of 30 days, when they will automatically be wiped from the system and any remote back-up systems.

3.4.3 Where requested by the Police or other statutory enforcement agencies, PCHA may instruct ARM Secure to retain digital images for longer periods until such time as they are able to be viewed by the relevant body, following strict data sharing protocols.

3.5 **Data Sharing with Statutory Enforcement Bodies**

3.5.1 PCHA have a number of written protocols for information sharing with statutory enforcement bodies (Police and Local Authorities in areas of its operations). The protocols extend to images that have been captured by PCHA CCTV systems and may assist the statutory bodies in the conduct of their duties.

3.5.2	PCHA will comply with all requests for data release of images captured by its CCTV systems from statutory enforcement agencies e.g. Police or Environmental Protection Departments from local authorities and any court orders it receives.
3.5.3	<p>All requests for CCTV images from statutory or enforcement agencies should be directed to the Sovini Group Data Protection Officer (Data or Quality Assurance Manager) or Deputy at:</p> <ul style="list-style-type: none"> • Email address: contactus@pinecourt-housing.co.uk • Postal address: Pine Court Housing Association, 1 Nelson Street, Liverpool, L1 5DW • Telephone number: 0151 709 6878 •
3.5.4	Requesting authorities or agencies will need to complete a data release form (detailing what images are required, by whom and for what purpose). The selected images will then be encrypted and sent to the enforcement agency via a secure email link (Egress or similar).
3.5.5	Once an enforcement authority has access via a secure link to the images requested, they then become responsible for the security of the data in line with UK Data Protection legislation.
3.6	Public Access to CCTV Images
3.6.1	Any images that PCHA CCTV cameras capture of a recognisable person are classed as personal data and are covered by the provisions of the UK General Data Protection Regulations and UK Data Protection Act 2018. Anyone that believes they may have been filmed on PCHA CCTV systems has a right to request a copy of this data / the images captured.
3.6.2	<p>Anyone requesting a copy of such data must contact the Sovini Group Data Protection Officer (Data and Quality Assurance Manager) or Deputy at:</p> <ul style="list-style-type: none"> • Email address: contactus@pinecourt-housing.co.uk • Postal address: Pine Court Housing Association, 1 Nelson Street, Liverpool, L1 5DW • Telephone number: 0151 709 6878
3.6.3	<p>The Sovini Data Protection Officer or Deputy will complete a 'Data Request Form' on the customers behalf but will liaise with the person requesting the data to determine / obtain:</p> <ul style="list-style-type: none"> • What they want the information for • Details of where and when they think their image may have been captured (to within 2-hour timeframes) • Photographic proof of identity
3.6.4	The Group Data Protection Officer (Data and Quality Assurance Manager) will have the discretion to agree or refuse the request for the release of information unless there is an overriding legal obligation such as a court order in place.
3.6.5	Where requests for information are agreed, it will be supplied to the data subject (the person that is in the images and is requesting the information) in the form of a secure link. Customers can set up an account to use the secure system free of charge and the Data Protection Officer or Deputy dealing with the request will be able to advise how they can do this, if required.

3.6.6	In most cases this will be supplied free of charge, although PCHA reserve the right to Charge £10 per request received. PCHA will normally process requests for information within 10 working days and deal with all requests within one calendar month of the request being received.
3.6.7	Any images that are released to a data subject, may have the identities of un-associated third parties obscured to protect their anonymity and prevent an intrusion into their privacy.
3.6.8	The Sovini Group Data Protection Officer ((Data and Quality Assurance Manager) will also respond to any requests for the release of CCTV images that may be received under the Freedom of Information (FOI) Act 1998.
3.6.9	In most cases if the images being requested contain images of identifiable individuals and they are not the people making the request, the request will be refused on the grounds that it may potentially result in a breach of the UK GDPR and UK Data Protection Act requirements.
3.7	Maintenance and Servicing of CCTV Systems
3.7.1	The maintenance and service of CCTV systems is managed by PCHA Asset Management Team.
3.7.2	To meet its responsibility, the Sovini Asset Management Team has an arrangement in place with a third party to carry out an annual service inspection of all CCTV systems or as and when repairs are identified or reported. The Team will also engage the services of a third party to clean its CCTV equipment (cameras and monitors) as and when it is required to do so.
3.8	Complaints about the operation of PCHA CCTV Systems
3.8.1	<p>Any complaints in regard to the operation of CCTV systems will be dealt with in line with the PCHA Complaints Appeals and Feedback Policy. Complaints can be submitted:</p> <ul style="list-style-type: none"> • By contacting the PCHA main office 0151 709 6878 • Through the PCHA website at https://www.pinecourt-housing.org.uk/ • Via email enquiries contactus@pinecourt-housing.co.uk • In writing to Pine Court Housing Association, 1 Nelson Street, Liverpool, L1 5DW • In person to any PCHA member of staff
4	Implementation
4.1	All PCHA staff need to be aware of the CCTV Policy to be able to direct any customer enquiries they may receive.
4.2	The Director of Operations has ultimate responsibility for the operation and effective implementation of the Policy and for ensuring it is reviewed in line with the schedule outlined below in Section 7.
4.3	The Director of Operations also have responsibility for compiling the Annual Report on the systems use to the Departmental Management Team (DMT).

4.4	The Data Protection Officer (Data and Quality Assurance Manager) or Deputy will be responsible for dealing with requests from the public, third parties and data subjects for the release of CCTV images.	
5	Performance	
5.1	In operating the CCTV Policy, PCHA will provide an initial response to all requests for information within 10 working days and will ensure where a decision is made to release data to a data subject (other than statutory enforcement agency) that they receive it within one calendar month from the day of receipt (e.g. a subject access request received on the 21 st of the month will be provided by the 21 st of the preceding month – where it is agreed by PCHA).	
5.2	The Director of Operations will compile an Annual Report to the EMT and when approved this report will be made available to the public on request, detailing: <ul style="list-style-type: none"> • Number of requests for viewing recorded information and the responses given • An outline of why the system and its operation remains justified • Record of system maintenance checks • Any staffing or operational issues by exception, i.e. any matters requiring instigation of disciplinary procedures 	
5.3	Any request for changes to the service including expansion, reduction or any matter requiring capital expenditure may be taken to DMT outside of these times or will be dealt with in line with delegated line management responsibilities.	
6	Consultation	
6.1	All PCHA staff have been consulted in the development of this Policy. The PCHA Tenant Customer Empowerment Panel were consulted on this Policy on 6 th July 2022.	
7	Review	
7.1	The Policy will be reviewed every three years, from the date of Executive Management Team (DMT) approval or sooner in the light of any new legislation or regulation impacting on the use of CCTV systems or through any issues requiring alteration from PCHA system audits.	
7.2	PCHA will ensure there is an independent audit of the operation of the CCTV systems on an annual basis as part of its internal audit arrangements.	
8	Equality Impact Assessment	
8.1	Was a full Equality Impact Assessment (EIA) required?	
8.2	When was EIA conducted and by who?	An EIA Relevance Test was conducted by the Policy and Strategy Manager and the Policy Writer on 14-05-22.

8.3	Results of EIA	The Relevance Test did not identify any differential or adverse impacts for any Groups with protected characteristics as a result of operation of this Policy. Due to new management arrangements, it was recommended the Policy be moved to a 12-month review cycle rather than the previous three year cycle.	
9	Scheme of Delegation		
9.1	Responsible committee for approving and monitoring implementation of the policy and any amendments to it	DMT	
9.2	Responsible officer for formulating policy and reporting to committee on its effective implementation	Director of Operations	
9.3	Responsible officer for formulating, reviewing and monitoring implementation of procedures	Director of Operations	
10	Amendment Log		
Date of revision:	Reason for revision:	Consultation record:	Record of amendments:
This is a first version of the Policy-approved on 27 September 2016	Not applicable	See Section 6	Not applicable
2nd December 2019	In line with the review schedule	See Section 6	<ul style="list-style-type: none"> The whole Policy has been revised in line with PCHA's business practices.
5 th July 2022	In line with the review schedule	See Section 6	<ul style="list-style-type: none"> Policy updated throughout to include revised management arrangements under contact with third party 'system user' – Arm Secure EIA updated and Policy to move to a 12-month review cycle