Closed Circuit Television (CCTV) Policy

Originator:	Policy and Strategy Team
Executive Management Team Approval Date:	20th September 2022
Review date:	September 2025

1	Introduction
1.1	The Policy sets outs measures that One Vision Housing (OVH) 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-off hours call services.
1.2	This Policy sets out: • How OVH 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 OVH will report and review use of systems • How complaints about the operation of CCTV systems can be made
1.3	The Policy covers: • CCTV systems that are installed by OVH (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 OVH manages the CCTV contract on behalf of other Sovini entities
1.4	Operation of the Policy ensures OVH meets its legal requirements in the use of CCTV. The principal legislation in this area is as follows: • UK Data Protection Act 2018 • UK General Data Protection Regulations 2018 • The Protection of Freedoms Act 2012 • The Freedom of Information Act 2000 • The Human Rights Act 1998

1.5	In operating this Policy, OVH also ensures compliance with the Regulatory Framework for Social Housing, adopted by the Regulator for Social Housing.
1.6	Access and Communication
1.6.1	OVH is committed to ensuring that its services are accessible to everyone. OVH 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 OVH or use its services.
1.7	Equality, Diversity and Human Rights
1.7.1	OVH 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.
1.7.2	OVH 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.
1.7.3	OVH will also ensure that all services and actions are delivered within the context of current Human Rights legislation. OVH will endeavour to ensure its staff and others with whom it works, will adhere to the central principles of the Human Rights Act (1998).
1.8	This Policy should be read in conjunction with the: • OVH Complaints, Appeals and Feedback Policy • OVH Information Management Policy • OVH Data Protection Policy • OVH Lift Maintenance Policy
2	**Statement of Intent**
2.1	As a 'System Operator' OVH 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.
2.2	OVH 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 OVH has a controlling interest (including systems that ensure passenger safety in OVH operated lifts) • To maintain the asset value of properties and equipment owned by OVH / 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 OVH 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, OVH 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
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
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 OVH systems)

2.5	In operating CCTV systems, OVH will also comply with the current and any subsequent guidance and good practice produced by the Information Commissioners Office and the British Standards Institute.
3	**Policy**
3.1	Management Arrangements
3.1.1	OVH 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 OVH's behalf via Sovini Property Services (SPS).
3.1.2	Responsibility for the operation of OVH 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 Neighbourhood Services Manager: • Neil Kenwright – Neighbourhood Services Manager 0300 365 1111
3.1.3	As the 'System Operator' OVH will retain responsibility for developing and reviewing any joint working protocols that are established with the 'System User'.
3.2	OVH CCTV Systems
3.2.1	OVH operate a number of CCTV systems across various locations in buildings it owns and controls including: • High rise accommodation • Independent living housing – retirement living schemes • 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 OVH will be 'overt' and clearly visible at all times. Where OVH 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 OVH 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 OVH 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 OVH CCTV systems and to guard against unauthorised use, access or disclosure.

3.3 Data Security, Retention and Disposal

3.3.1 All images captured by OVH 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.

3.3.2 Arm Secure, working on OVH'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.

3.3.3 Where requested by the Police or other statutory enforcement agencies, OVH 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.

3.4 Data Sharing with Statutory Enforcement Bodies

3.4.1 OVH 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 OVH CCTV systems and may assist the statutory bodies in the conduct of their duties.

3.4.2 OVH 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.

3.4.3	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: • Email address: dpenquiries@sovini.co.uk • Postal address: One Vision Housing, Atlantic House, Dunnings Bridge Road, Bootle, Merseyside, L30 4TH • Telephone number: 0300 365 1111
3.4.4	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).
3.4.5	Once an enforcement authority has access via a secure link to the images requested then become responsible for the security of the data in line with UK Data Protection legislation.
3.5	Public Access to CCTV Images
3.5.1	Any images that OVH 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 OVH CCTV systems has a right to request a copy of this data / the images captured.
3.5.2	Anyone requesting a copy of such data must contact the Sovini Group Data Protection Officer (Data and Quality Assurance Manager) or Deputy at: • Email address: dpenquiries@sovini.co.uk • Postal address: One Vision Housing, Atlantic House, Dunnings Bridge Road, Bootle, Merseyside, L30 4TH • Telephone number: 0300 365 1111
3.5.3	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: • 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
3.5.4	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.
3.5.5	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.
3.5.6	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.

3.5.7	In most cases this will be supplied free of charge, although OVH reserve the right to Charge £10 per request received. OVH will normally process requests for information within 10 working days and deal with all requests within one calendar month of the request being received.
3.5.8	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.
3.5.9	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.
3.5.10	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.
3.6	Maintenance and Servicing of CCTV Systems
3.6.1	The maintenance and service of CCTV systems is managed by OVH Asset Management Team.
3.6.2	To meet its responsibility, the OVH 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 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.
3.7	Complaints about the operation of OVH CCTV Systems
3.7.1	Any complaints in regard to the operation of CCTV systems will be dealt with in line with the OVH Complaints Appeals and Feedback Policy. Complaints can be submitted: • By contacting the OVH Customer Service Centre 0300 365 1111 • Through the OVH website at www.ovh.org.uk • Via email enquiries@ovh.org.uk • In writing to One Vision Housing, Atlantic House, Dunnings Bridge Road, Bootle, L30 4TH • In person to any OVH member of staff
4	**Implementation**
4.1	All OVH staff need to be aware of the CCTV Policy to be able to direct any customer enquiries they may receive.
4.2	The Neighbourhood Service Manager 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 Neighbourhood Service Manager will also have responsibility for compiling the Annual Report on the systems use to the Executive Management Team (EMT).
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, OVH 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 21st of the month will be provided by the 21st of the preceding month – where it is agreed by OVH).
5.2	The Neighbourhood Service Manager will compile an Annual Report to the EMT and when approved this report will be made available to the public on request, detailing: • 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 EMT outside of these times or will be dealt with in line with delegated line management responsibilities.
6	**Consultation**
6.1	All OVH staff have been consulted in the development of this Policy. The OVH Tenant Policy Review Group were consulted on this Policy in July 2022.
7	**Review**
7.1	The Policy will be reviewed every three years, from the date of Executive Management Team (EMT) 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 OVH system audits.
7.2	OVH will ensure the 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? — No

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 — EMT
9.2	Responsible officer for formulating policy and reporting to committee on its effective implementation — Operations Director-Housing Services
9.3	Responsible officer for formulating, reviewing and monitoring implementation of procedures — Operations Director –Housing Services

10 Amendment Log

Date of revision:	Reason for revision:	Consultation record:	Record of amendments:
5th November 2019	In line with the review schedule	See Section 6	• Job titles and contact details for staff with line management responsibility for systems have been updated in line with the recent review of the CCTV service • References to Data Protection legislation have been updated include GDPR and the Data Protection Act 2018
20th September 2022	Reviewed in line with change in operational practice	See Section 6	• 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

05/02/2024	As per board approval process, the review period for this policy has been extended to every 3 years	N/A	There have been no changes to the policy during this review except for review period dates.