

Closed Circuit Television (CCTV) Policy

Originator:	Policy and Strategy Team
Executive Management Team Approval Date:	November 2019
Review date:	November 2022

1	Introduction
1.1	The Policy sets out provisions that OVH has in place for operating CCTV systems and providing associated services within the Sovini Group including out-off hours call services.
1.2	<p>This Policy sets out:</p> <ul style="list-style-type: none"> • The ownership of systems that are in operation • The line management responsibility for the systems in operation • 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
1.3	<p>The Policy covers:</p> <ul style="list-style-type: none"> • Closed Circuit Television (CCTV) systems that are installed and operated by OVH (to provide safety & security of users, protect asset value) in buildings it owns and controls • Sovini Group sites where OVH has an agreement to provide full or partial CCTV services
1.5	<p>Operation of the Policy ensures OVH meets legal requirements in the use of CCTV. The principle legislation in this area is as follows:</p> <ul style="list-style-type: none"> • General Data Protection Regulations (GDPR) 2018 • The Data protection Act 2018 • The Freedom of Information Act 1998 • The Human Rights Act 1998 • The Private Security Industry Act 2001 • The Working Time Regulations 2012

<p>1.6</p> <p>1.7</p> <p>1.7.1</p> <p>1.8</p> <p>1.81</p> <p>1.8.2</p> <p>1.8.3</p> <p>1.9</p>	<ul style="list-style-type: none"> • The Protection of Freedoms Act 2012 <p>In operating this Policy, OVH also ensures compliance with the Regulatory Framework for Social Housing, adopted by the Regulator for Social Housing.</p> <p>Access and Communication</p> <p>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.</p> <p>Equality, Diversity and Human Rights</p> <p>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 our duty with positive regard for the following core strands of equality; Age, Disability, Gender, Race, Transgender, Sexual Orientation, Maternity and Pregnancy, Marriage and Civil Partnerships, Religion and/or Belief.</p> <p>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.</p> <p>OVH will also ensure that all services and actions are delivered within the context of current Human Rights legislation. OVH will strive to ensure that its staff and others with whom OVH 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"> • OVH Complaints, Appeals and Feedback Policy • OVH Information Management Policy • OVH Data Protection Policy • OVH Lift Maintenance Policy
<p>2</p>	<p>Statement of Intent</p>
<p>2.1</p> <p>2.2</p> <p>2.3</p>	<p>OVH will ensure that CCTV systems under its control are installed for a legitimate reason and in accordance with required standards as per the relevant legislation.</p> <p>OVH will employ competent staff to manage and/or operate CCTV systems who will be based at its purpose built Central Control Room located within its head office at:</p> <ul style="list-style-type: none"> • One Vision Housing Limited, Atlantic House, Dunnings Bridge Road, Bootle, Merseyside, L30 4TH <p>OVH will have clearly defined roles for staff with line management responsibilities and those that operate CCTV systems including in relation to data protection and maintenance.</p>

<p>2.4</p> <p>2.5</p>	<p>In operating CCTV systems, OVH will comply with the current guidance and good practice produced by the Information Commissioners Office, the Circuit Television (CCTV) – Management and Operation – Code of practice 2015.</p> <p>In operating CCTV systems, OVH aims to:</p> <ul style="list-style-type: none"> • Promote 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 assist the controlled access to restricted areas in OVH properties in conjunction with door entry system technologies • To maintain the asset value of properties and equipment owned by OVH by deterring / preventing vandalism or theft • Promote early intervention actions that would save further damage to persons or properties (e.g. making safe / repairing broken windows) • Assist in the prevention of crime, anti-social behaviour, public order offences and other statutory enforcement issues and in any subsequent apprehension and prosecution of those found to be responsible for these actions in consultation with the Police
<p>3</p>	<p>Policy</p>
<p>3.1</p> <p>3.1.1</p> <p>3.1.2</p> <p>3.1.3</p> <p>3.1.4</p>	<p>OVH CCTV Systems</p> <p>OVH will operate and/or manage a number of CCTV systems across various locations in buildings across the Sovini Group including:</p> <ul style="list-style-type: none"> • High rise accommodation • Independent living housing, accommodation • Office and business premises <p>The systems used across these locations includes: fixed position cameras, pan tilt and zoom (PTZ's) cameras, monitors, multiplexers and digital recorders. The systems will be capable of recording images in real time and time lapse mode but will not record sound.</p> <p>In operating CCTV systems, OVH will ensure that:</p> <ul style="list-style-type: none"> • All Cameras are 'overt' and clearly visible at all times • Appropriate signage is displayed and a regular audit schedule will be carried out to ensure the signage is in situ and clearly visible <p>All CCTV systems operated by OVH will be required to have cameras that are appropriately and carefully located to ensure:</p> <ul style="list-style-type: none"> • They provide maximum coverage of only areas under OVH's control, 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 man-made (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

3.2 Responsibilities

3.2.1 OVH employs a line manager (the Neighbourhood Service Manager and the Assistant) who has ultimate responsibility for the operation of the CCTV systems, management of staff (operatives) that operate the systems and for ensuring the effective implementation and review of this Policy. The contact details for those with line management responsibility for the operation of CCTV systems and functions are as follows:

- Neighbourhood Service Manager – Neil Kenwright
0151 530 5599
Neil.kenwright@ovh.org.uk
- Assistant Neighbourhood Service Manager – Chris Hamill
0151 530 5645
Chris.hamill@ovh.org.uk
- CCTV Supervisor-Michael Bilby
0151 530 5473
Michael.bilby@ovh.org.uk

3.2.1.2 Where OVH operates ‘observation and retrieval’ type of CCTV systems’, the operatives of the system will be able to view real time footage from cameras via a Central Control Room (see section 2.3) and can retrieve archived footage.

3.2.1.3 OVH may, where required, retrieve captured images (via the Central Control Room) for the purposes of investigations into matters of internal staff discipline.

3.2.1.4 OVH will ensure that CCTV systems under its control are not used for the purposes of:

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

3.3 Control of Operations

3.3.1 Where OVH is responsible for the operation of CCTV, all captured images will be relayed to the Central Control Room which is staffed 24 hours a day 365 days a year (with exception of staff rest periods when the responsibility is transferred to a contracted third party). The Central Control Room (see 2.3 for details) has secure access limited to those staff whose role it is to monitor the equipment / images, mobile patrol staff, authorised senior staff and external authorised parties such as the Police see 3.4 for details).

3.3.2 The Central Control Room is designed to obscure visual access to monitors capturing live or recorded images and also has facilities for secure viewing by authorised parties.

3.3.3	All staff working in the Central Control Room and mobile patrols will also receive internal 'Lone Worker' training and refresher training.
3.3.4	OVH will ensure all staff that either work in the Central Control Room or that undertake operations of CCTV systems have valid Disclosure and Barring Service (DBS) checks (Previously Criminal Records Bureau –CRB). These checks will be reviewed every three years and will be completed for any new staff before their employment commences.
3.3.5	All work activities that are required for the safe and effective operation of CCTV systems will be detailed in a comprehensive procedures manual which will be available to relevant staff at all times. The manual will be held in the OVH Document Management System and will be updated and maintained through annual audits and a system of change requests, as required by changed working practices or to deliver operational improvements.
3.4	Data Security, Retention and Disposal
3.4.1	OVH will ensure that all images captured by CCTV systems under its control are digitally recorded for 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	OVH will normally keep images recorded for a period of 30 days, when they will automatically be wiped from the hard drive of OVH systems and any remote back-up systems.
3.4.3	Where requested by the Police or other statutory enforcement agencies OVH may 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. This will normally involve OVH retaining a hard copy of images on a DVD (of specified time periods and areas of interest to the relevant body).
3.5	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 Authority). The protocols extend to images that have been captured by CCTV systems controlled by OVH and may assist the statutory bodies in the conduct of their duties, including co-operation in live operations where required.
3.5.2	Statutory bodies may access images that have been recorded at any time and a facility exists within the CCTV Central Control Room for confidential viewing of recorded material.
3.5.3	<p>If an operative from a statutory enforcement body needs to remove a copy of the recorded material, for any reason from the CCTV Control Central Control Room (in hard format, i.e. DVD) they will be required to sign a release form detailing:</p> <ul style="list-style-type: none"> • The date and time the recorded material was taken • The date and time range of recorded images and details of which cameras / areas the images are from • The badge number / name of operative taking the information

	<ul style="list-style-type: none"> • A brief description of why the information is required and for what purposes it will be used
3.4.4	Once recorded, information is transferred to hard format and removed from the CCTV Central Control Room by a statutory enforcement body, they will become the 'data controllers' as per GDPR and Data Protection Act 2018 requirements and will be responsible for the security and disposal of the information held.
3.4.5	OVH may retain recorded images for periods longer than 30 days if the information held is subject of a disclosure request (either from a statutory enforcement body or a data subject – member of the public).
3.5	Public Access to CCTV Images
3.5.1	Any images that OVH controlled CCTV cameras capture of a recognisable person are classed as personal data and are covered by the provisions of GDPR and the Data Protection Act 2018. Anyone that believes they may have been filmed on OVH controlled 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 complete the 'CCTV Data Request Form' which will be processed by the Group Data Protection Officer (Data and Quality Assurance Manager). The forms will be available via: <ul style="list-style-type: none"> • The OVH website at www.ovh.org.uk • By direct email contact with the Group Data Protection Officer (Data and Quality Assurance Manager) at dpenquiries@sovini.co.uk • Via telephone request to the Customer Service Centre on 0300 365 1111 (and a hard copy will be posted out)
3.5.3	The CCTV Data Request Form will require the person requesting the information to detail / provide: <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 1 hour timeframes) • Photographic proof of identity (sent via email or post)
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 DVD. 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 receiving the request.
3.5.6	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.

3.5.7	The 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. 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 GDPR and Data Protection Act requirements.
3.6	Maintenance and Servicing of CCTV Systems
3.6.1	OVH discharge its responsibility for maintenance and service of CCTV systems it owns through the OVH Asset Management Team.
3.6.2	OVH Asset Management Team has an arrangement in place with a third party to carry out an annual service inspection of all OVH's CCTV systems or as and when repairs are identified or reported. The Team also engage the services of a third party to clean OVH's CCTV equipment (cameras and monitors) as and when it is required to do so.
3.6.3	Where OVH operates CCTV system owned by other companies, it is their responsibility to ensure that the systems are maintained and serviced in line with the relevant legislation.
3.7	Complaints about the operation of CCTV Systems
3.7.1	<p>Any complaints in regard to the operation of OVH owned CCTV systems will be dealt with in line with the OVH Complaints Appeals and Feedback Policy. Complaints can be submitted:</p> <ul style="list-style-type: none"> • 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, Dunning's Bridge Road, Bootle, L30 4TH • In person to any OVH member of staff
3.7.2	Where OVH operates CCTV systems on behalf of a third party, it will provide full co-operation to ensure effective resolution to any relevant complaints and /or queries, as applicable.
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 or the Assistant 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. The Neighbourhood Service Manager and their assistant will also have responsibility for line management of the staff that operate the CCTV systems on a daily basis and for compiling the Annual Report on the systems use to the Executive Management Team (EMT).

4.3	CCTV operational staff will be responsible for dealing with requests for release of recorded images to statutory enforcement agencies in line with the written data sharing protocols and in accordance with the detailed procedures manual that exists for the Central Control Room.	
4.4	The Data Protection Officer (Data and Quality Assurance Manager) will be responsible for dealing with requests from the public, third parties and data subjects for the release of CCTV images. This includes where OVH manage systems on behalf of other companies.	
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 of the request being received.	
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: <ul style="list-style-type: none"> • All 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	The Tenants Policy Review Group was consulted about this Policy on 25/10/2019. All OVH staff have been consulted in the development of this Policy.	
7	Review	
8.1	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.	
8.2	OVH 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?	No

8.2	When was EIA conducted and by who?	An Equality Impact Assessment Relevance Test carried out by the Policy and Strategy Manager and the Policy Writer on 12/06/14 is still relevant for this Policy.	
8.3	Results of EIA	The EIA relevance test did not indicate there would be any differential of adverse impacts for any person with protected characteristics as a result of the operation of this policy.	
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:
27 September 2017	In line with the review schedule	See Section 6	At 2.2 –Details of one supervisor have been removed due to retirement. An update will be made as soon as the new appointment is made.
05/11/2019	In line with the review schedule	See Section 6	<ul style="list-style-type: none"> • 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 including GDPR and the Data Protection Act 2018 • The whole Policy has been updated to take into account CCTV

			services provided to other companies within the Sovini Group
--	--	--	--