

Residential Closed-circuit Television (CCTV) POLICY

Review Date:	October 2027
Approved:	Executive Team
Author:	Octavia Williams
Version:	1

Contents

Introduction.....	2
Objectives.....	2
Equality and diversity statement (fair access).....	2
Legal Framework.....	2
Purpose of the CCTV system	3
Our CCTV systems	3
Installing CCTV	4
Storage, retention and disposal of images	4
Sharing of CCTV footage with external agencies.....	4
Access to an image by a subject	5
Residents video doorbell guidance.....	6
Monitoring and continuous improvement	7

Introduction

This Policy outlines our approach to the use of residential closed-circuit television (CCTV) and other video surveillance systems. It sets out how Dolphin Living collects, uses, and stores CCTV images and information. It covers:

- Residents who have a tenancy agreement with us
- Third-party suppliers who install, maintain, operate, or remove CCTV on our behalf
- Existing and future installations of overt (visible) systems.
- Existing and future domestic CCTV systems and smart camera doorbells installed by our residents.

This Policy does not cover:

- The use of 'dummy' or non-operational CCTV systems, as no images or information will be processed.
- CCTV systems installed or proposed by third parties (e.g. commercial premises owners or operators, owners or agents of residential blocks or estates and/or similar) in areas (such as their buildings and/or on their land) they control and/or over which we have no responsibility or control even if there is an obligation to contribute to such systems if they arise.

Objectives

The aim of this policy is to ensure Dolphin Living complies with all relevant data protection legislation and guidance at all stages of using CCTV, including resident guidance on the installation of video doorbells.

The policy covers the installation and use of CCTV surveillance equipment and the gathering, storage, use and disposal of digital images and how we communicate to people about digital images. This policy applies to all staff employed by Dolphin Living, our Managing Agent, external contractors, and other partner agencies who may have access to the system from time to time. Where a partner organisation manages our CCTV system, responsibilities should be documented in a management contract or service level agreement.

The CCTV system should not be used for any other purpose. It is not the intention to use any of the measures to intrude on the privacy of areas where people have expectation of privacy or to monitor or record minor indiscretions.

Equality and diversity statement (fair access)

Dolphin Living is committed to ensuring fair access to all its services. The organisation believes in valuing diversity and promoting inclusion. We promote equality of opportunity for all our residents and stakeholders, regardless of their race, gender, age, religious belief or non-religious belief, ethnic origin, disability, marital status or sexual orientation. In addition to any statutory responsibilities under the Equality Act 2010 (and any other relevant legislation).

Legal Framework

- Data Protection Act 2018
- Data (Use and access) Act 2025
- Human Rights Act 1998
- Regulator of Social Housing Regulatory Standards
- Protection of Freedoms Act 2012

- UK Government: Home Office Surveillance Camera Code of Practice (2013)
- Information Commissioner Office- CCTV Code of Guidance
- General Data Protection Regulation (2018)

Purpose of the CCTV system

We use surveillance as a tool to support our activities as a landlord. Specifically, it allows us to take a positive approach to combating anti-social behaviour (ASB) and illegal activities that adversely affect our residents. We will install systems with the primary purpose of maintaining the safety of our residents and their homes, of reducing the threat of crime generally, and improving public safety.

These purposes will be achieved by monitoring the system for:

- Prevention of crime
- Training
- Service/maintenance purposes
- Detection of crime – e.g. a request from the Police
- Reduce the threat of ASB
- Deter fly-tipping
- Facilitate the identification, apprehension, and prosecution of offenders in relation to crime and community safety.

The system will not be used:

- For any purpose other than laid out above
- To provide recorded images for the internet
- To record sound
- For any automated decision taking

Systems should be able to record good quality images, of the appropriate standard to be used for the reasons the CCTV is in place.

CCTV cameras will typically be sited in relevant communal areas (e.g. external doors, hallways, stairwells, exits, bin stores, car parks, lifts) and will be accompanied by clear and prominent signage identifying the data controller and contact details. Cameras will be positioned to allow areas of interest to be filmed unobscured, but to ensure that areas that are not of interest or should not be filmed, such as private homes, are not filmed. If the cameras cannot be sited in a way that avoids filming private areas, technical solutions should be used to obscure the private areas.

We will maintain a central register of CCTV systems in operation on our properties, including details of the location and type(s) of device in use.

We will take all reasonable steps to ensure that CCTV equipment is always secure from unauthorised access. No camera will be hidden from view, and all will be prevented from focusing on private areas.

Our CCTV systems

- We hold a CCTV register that covers each site with CCTV in operation.
- No camera will be hidden from view.

Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage. We will monitor and review footage for the purposes set out above.

Installing CCTV

For new build developments, Dolphin Living will consider installation on a case-by-case basis, ensuring that a proposed scheme meets the aims set out above relating to preventing antisocial behaviour and crime and creating a safe environment.

Please also refer to the Data Protection Policy Section 9 - Use of monitoring and surveillance technology.

Whether planning the installation of a new system or modifying an existing system, a site risk assessment and Data Protection Impact Assessment (DPIA) undertaken. The consideration will include but not be limited to:

- Area(s) that the system will cover
- Detail required in the resulting images, normally expressed using defined industry terms like 'identity' and 'recognise'
- Reason for that coverage including the target and activity
- Provides an explicit and mutually agreed instruction to the designer/service provider
- Ensures that the designer/service provider takes responsibility for design and product selection
- Process of user acceptance and confirming that the designed and installed system meets the brief
- Provides instructions on privacy and cyber-security requirements.

Dolphin Living may, on occasion, choose to install or upgrade service chargeable CCTV systems as part of a health & safety-based risk assessment if:

- There is a specific need that cannot be met through other reasonable methods
- A Privacy Impact Assessment is carried out
- There is a robust business case

Signage will be installed to ensure staff, residents, visitors and members of the public are aware they are entering an area that is covered by CCTV. The signage will include the Dolphin Living logo and the relevant contact details.

Dolphin Living does not have the legal powers required to use covert CCTV. There may be some circumstances when the Police or other law enforcement agency ask for our co-operation with a covert surveillance exercise, which we will consider on a case-by-case basis.

Storage, retention and disposal of images

All captured images are recorded and securely stored. Recorded images will be stored for a maximum of 30 days in line with GDPR, unless required for evidential purposes, or as part of a Subject Access Request (SARS). Images will automatically be deleted after this period.

Images will be time and date stamped.

Images will be stored either onsite or off-site with data transmitted via internet safe servers.

Images required for an investigation shall be retained for no longer than a period of 2 years following the end of the investigation.

Sharing of CCTV footage with external agencies

All requests for access to CCTV footage will be considered in line with GDPR Principles. The GDPR Principles:

- Purpose limitation – only using data for specific purposes.
- Data minimisation – only collecting and using minimum data.
- Accurate and up to date data.
- Storage limitation – only retaining data as long as necessary.
- Security – keeping data secure, in storage and when being accessed or shared.
- Accountability – meaning being able to demonstrate compliance with the other requirements of the legislation.

The GDPR Rights of Individuals that are applicable to CCTV include:

- The Right to Access – giving people access to their own data, which is the footage that they appear in.
- The Right to Erasure – allowing people to ask for it to be erased. Note: Some exemptions do apply when responding to these requests.

The GDPR requires specific controls to be in place whenever 'Data Processors' are used. A third party who operates CCTV on behalf of Dolphin Living is a Data Processor, and Dolphin Living is responsible for: selecting companies who provide sufficient guarantees that they will comply with data protection legislation; including GDPR compliant clauses in the contract; continuing to manage and review the contract.

All requests for access to CCTV footage will be considered in line with GDPR Principles as above. It is key to identify a lawful basis for sharing, to meet the first principle of 'lawful, fair and transparent processing'.

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded may assist in criminal enquiry and/or prevention of terrorism and disorder.
- Prosecution agencies
- Relevant legal representatives
- Emergency services in connection with the investigation of an accident
- Residents will not be given access to CCTV footage unless as below they are the subject or it is part of a civil or insurance case

Access to an image by a subject

CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in the Act. We will only share images if the images are appropriate and in line with our Subject Access Request (SAR) process.

Under data protection law, you have the right to access and receive a copy of your personal data; this may include images and information captured by any overt CCTV system we have in place if it can identify you as an individual. This is called the right of access and is commonly known as making a Subject Access Request or SAR. We cannot release images or information of other people to you and so you may receive only part of the information you asked for.

Images can only be provided if they will not be prejudicial to criminal enquiries or proceedings. We will obscure third parties where appropriate.

A person whose image has been recorded and retained and who wishes to have access to the data must apply in writing to the Data Protection Officer. They need to give the following information to enable us to find their image:

- Location
- Time

- Date
- Photograph of the subject so we can identify them in the footage

The Data Protection Officer will then arrange for a copy of the data to be made and given to the applicant. Dolphin reserves the right to charge a fee to secure a copy of this data. The Data Protection Act gives the Data Protection Officer the right to refuse a request for a copy of the data particularly where such access could prejudice prevention or detection of crime or the apprehension or prosecution of offenders.

All such requests will be referred to the Data Protection Officer.

If it is decided that a data Subject Access Request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

At times we may provide data to individuals for their use in civil or insurance claims, but only if it is justifiable and does not put others' safety at risk. If others can be identified we will not provide this data.

We hold a Data Request Register that outlines:

- Date of request
- Who requested the data?
- Why they requested the data
- Our response

Residents video doorbell guidance

Residents are legally entitled to install CCTV or a smart camera doorbell for your domestic use only and you do not need to contact us where you intend to do so, provided:

- Your tenancy or rental agreement states you can make any adaptations to your property without our express permission
- The installation of a smart camera doorbell can be done without causing any damage to the structure of the building or compromising the fire-safety integrity of the building
- Dolphin Living's lease with the freeholder states our residents can make adaptations to properties.
- You comply with the relevant legislation listed above.

If you are in any doubt about the requirements of installing a camera doorbell, please contact Managing Agent- Touchstone. Any breach of these stipulations may result in the removal of the doorbell camera and you being charged for any repair work required.

Residents must be aware that if their recording device captures images beyond their property boundary, then the use of the system is subject to data protection laws. Residents can still capture images but will need to comply with legal obligations as a data controller under the data protection laws. These include:

Telling people that you are recording, e.g. display signs.
Regularly or automatically deleting footage and you must also ensure security of the footage.
Stop recording a person if they object to it e.g. restrict your camera coverage area or point in different direction as appropriate. You may have to provide some of your recordings if asked by a person whose images you have captured.

The domestic use of smart camera doorbells and such recording devices could be challenged if their use amounted to harassment, under the Protection from Harassment Act 1997. The relevance of the legislation would depend on the specific circumstances.

Monitoring and continuous improvement

This policy will be monitored in several ways:

- An annual review will be carried out to ensure the systems remain necessary, proportionate, and effective in meeting their stated purpose.
- Resident feedback will be included in the monitoring of the systems.