Surveillance Policy

1. Introduction

1.1 This policy sets out the principles that underline our approach to collecting information, the criteria for installing CCTV and how we use it.

1.2 For the purposes of this policy ‘surveillance’ means gathering information that could be used as evidence to support a criminal or civil conviction or obtain a court order. This includes records of incidents, testimonies collected through interviews and information gathered using a surveillance device.

1.3 It should be read and applied in conjunction with the CCTV Procedure. Other policies related to this document include:

- Data Protection
- Antisocial Behaviour
- Information Security
- Service Charges
- Section 20
- Tenant Improvements
- Access Control
- Patching
- Network Security
- Password

2. Scope

2.1 This policy outlines our approach to the use of closed-circuit television (CCTV) and other recording equipment, such as dashboard cameras, sound monitoring equipment, and body worn video (BWV) cameras.

2.2 This policy applies to all properties owned and managed by the Peabody Group, including subsidiaries.

2.3 This policy aims:

- To ensure a consistent and proportionate approach to the use of CCTV and other recording equipment.
- To maintain the safety of our properties and their occupants.
- To ensure that we process recordings with due regard to data protection regulations and respond to requests to access recordings in accordance with the law.

3. Our approach

<u>Our approach to surveillance</u>

3.1 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 or the wider community.

3.2 We combine a range of surveillance methods to give us a greater understanding of incidents and those involved in them. We use surveillance information to make clear, reasonable, evidence-based judgments to maximise benefit for all our residents. Before conducting surveillance, we will set out what we are hoping to achieve and how we intend to achieve it.

3.3 We work closely with partners to gather and share surveillance information. We take an active role in Community Safety Partnerships and other local knowledge sharing initiatives. We establish and follow clear and consistent protocols with public bodies to share information, setting out responsibilities and the assignment of costs where appropriate. We proactively support our partners' surveillance activities, following the principle that our partners' success is our success and expect them to follow the same principle.

3.4 We always consider the value for money of any surveillance we undertake. We ensure that we take a proportionate response to surveillance, balancing its cost against expected outcomes including the cost of not undertaking it. Where appropriate we share costs with other bodies and charge them for using our assets. In making these decisions we will consider the principles of partnership working, the benefit to our residents and the costs incurred or saved.

How we will conduct surveillance

3.5 We recognise that effective surveillance involves collecting information from several sources. We rely on those suffering from anti-social behaviour and witnesses to it, including colleagues or professional witnesses, to record the details of incidents. We will use these records of incidents to:

- Identify the need for surveillance.
- Provide a record of incidents to support legal action.
- Effectively deploy surveillance devices.

3.6 We have a victim-centred approach to ASB. We support those suffering from anti-social behaviour and witnesses to it to keep full and accurate records. We use these to identify if there is a problem and how best to respond to it. We recognise that on occasion we may need to support residents who are too frightened to report or record incidents. Where this is the case, our colleagues can act as professional witnesses to support vulnerable residents to enable us to take action without putting them into real or perceived danger.

3.7 Where appropriate we will use other professional witnesses to support our work. Where partners are taking action to resolve an issue, we will use their evidence to support any action we take. We may also employ professional witnesses where the benefits outweigh costs.

CCTV

3.8 We will only install CCTV in situations where a clear need has been identified relating to the investigation of antisocial behaviour, crime and/or vandalism.

3.9 A decision to install CCTV will only take place where other more cost-effective and less intrusive solutions have been explored.

3.10 Within Care and Supported Housing schemes we may install CCTV to help ensure a safe and secure living environment and to meet care and support service requirements.

Please see the additional guidance document attached to the intranet for the purpose and use of CCTV in Care and Support Schemes. It is titled '**Care and Support CCTV Guidance**'.

3.11 Any decision to install CCTV on existing buildings will be subject to completion of a Data Protection Impact Assessment (DPIA) to evaluate whether its usage is proportionate.

3.12 CCTV will only be used to record images of properties which we own or manage. We will not use CCTV to record an individual's private property without their written consent.

3.13 Where sites are agency-managed, the managing agency must seek our permission prior to installation. Where we are the managing agent of a property, we will seek permission from the landlord prior to installation.

3.14 Where a partner organisation manages our CCTV system, responsibilities should be documented in a Management Contract or Service Level Agreement.

3.15 Consultation principles for permanent CCTV installation:

- We will consult with affected residents prior to installing permanent CCTV, unless we feel the situation is exceptionally high risk or the property is part of a short-stay care and supported housing scheme.
- Where we choose to consult, we will inform residents of the potential impact this may have on their service charges.
- Consultations will require a 50% response rate, with at least 66% responding in favour of CCTV being installed.
- Residents will be informed of the outcome of the consultation.

Please refer to the Service Charges Policy for detailed guidance on this requirement.

3.16 Where leaseholders, shared owners or freeholders will be affected, this will be subject to formal leasehold consultation in line with our Section 20 Policy.

3.17 We will have a management agreement or service level agreement in place if a partner organisation manages our CCTV system. Any third party carrying out this service must have a Security Industry Authority (SIA) licence; it is an offence not to do so.

3.18 CCTV cameras will typically be sited in relevant communal areas (e.g., External doors, hallways, stairwells, exits, bin stores, bike stores, car parks, lifts) and will be accompanied by clear and prominent signage identifying the data controller and contact details.

3.19 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.

3.20 We will take all reasonable steps to ensure that CCTV equipment is always secure from unauthorised access.

3.21 We will not use "dummy" or "fake" CCTV in any circumstances.

3.22 We may install temporary CCTV where we feel this is necessary to obtain evidence or identify the perpetrators of ASB in the absence of clear supporting evidence. This will only be installed after other options have been exhausted and its usage will be reviewed monthly.

3.23 We will not carry out covert surveillance. We may allow the police to carry out covert surveillance on our estates where appropriate.

<u>CCTV System Design and Installation Standards</u>

3.24 The CCTV systems installed must allow authorised colleagues or third parties the option of either secure remote or physical viewings of footage or both as and when required.

3.25 Systems must have individual unique user accounts with the ability for users to control the level of access other users have. Shared accounts are forbidden and must not be used.

3.26 The system must be able to capture good quality images that can be used in the court of law.

3.27 The system must have a variable coverage and quality of images for context. For example, estate wide, car parks, a camera at the entrance of every block, one in the landing, one looking over mailboxes, bins store, gardens, etc.

3.28 For future proofing, cameras must not be installed in a place where future plans for scheme may render it unhelpful (e.g., in a place where a tree will grow and block out the view).

3.29 The CCTV system must be able to retain footages for a minimum of 4 weeks.

3.30 The system must not be defined by size (GB/TB), but should be determined by the number of cameras and duration we need footage accessible for.

3.31 Systems that are not actively monitored MUST be able to detect motion (software that highlights when an incident was triggered)

3.32 The system installed must comply with our IT systems and environment, such as Citrix, and must be logically separated from the Peabody network.

3.33 CCTV system and design must adhere to security and privacy by design.

3.34 All CCTV suppliers must be GDPR compliant and process data within the UK or EU.

3.35 All CCTV Systems that are connected to the internet must be pen tested before made live. If there are any existing CCTV systems installed that have internet connectivity as a functionality, these must also be pen tested before that functionality is enabled.

3.36 CCTV systems that are accessible from the internet must be scanned for vulnerabilities, it is the CCTV requestor's responsibility to inform the Information Security Team so they can setup appropriate scanning and monitoring.

3.37 The CCTV system must conform to all information security policies, standards and requirements including, but not limited to, the below:

- Access Control Policy
- Patching Policy
- Network Security Policy
- Password Policy

3.38 CCTV systems should be reviewed as part of a business unit's Business Continuity plans and Recovery Time/Recovery Point Objective set, if relevant.

Sound Monitoring Equipment

3.39 We may use sound monitoring equipment, including the Noise App, in cases of persistent and high-level noise nuisance complaints or cases which involve verbal abuse. Sound monitoring

equipment will only be used where other solutions have been exhausted. Further information is contained in our Antisocial Behaviour Policy.

Body Worn Video (BWV)

3.40 Our colleagues may use BWV cameras where appropriate. We will advise an individual that they are being recorded and will not use them for continuous recording purposes.

Dashboard Cameras

3.41 We reserve the right to use dashboard cameras on vehicles used by our colleagues. These must only be used during working hours and any individual must be informed of their presence when entering a vehicle in which they are used. They should not record audio inside the vehicle.

Domestic CCTV

3.42 It is not unlawful for our residents to install CCTV equipment, including a doorbell system, provided they comply with legislation and the ICO guidance. However, we are not responsible for their actions in this regard, nor are we able to monitor whether they are legally compliant in the use of these cameras.

3.43 If a resident wishes to install their own CCTV equipment, then they can submit their request to their Neighbourhood Manage by letter or email under the Tenant Improvements Policy.

Storage and Access to Recordings

3.44 We will own the copyright of all images and recordings made using the CCTV, BWV and sound recording equipment in use on properties we own and manage, unless there is a management agreement in place stating otherwise.

3.45 We will not retain any images or recordings from CCTV, sound monitoring or BWV cameras for more than one calendar month unless one of the following circumstances apply:

- we are otherwise advised by police.
- we believe that the footage may be required to evidence anti-social behaviour, a crime, or the civil litigation process.
- we have received a request to disclose the footage as part of a subject access request.

All other information will be deleted beyond this point.

3.46 All recordings will remain secure and encrypted at rest with access restricted to relevant colleagues (i.e., those involved in the investigation of an ASB or safeguarding case), unless we have been requested to provide information to the police, prosecuting agencies or legal representatives where it relates to the prevention, investigation, detection or prosecution of a crime.

3.47 The media may also be provided with footage if the police decide this is necessary to identify the perpetrator of a criminal incident.

3.48 Third party images will be obscured where there is an unfair intrusion into a person's privacy, or where disclosure may cause unwarranted harm or distress, unless we have the consent of the third party to disclose the images.

3.49 Individuals may only access recordings of themselves through making a subject access request. Under data protection legislation, we are required to respond to such requests within one

calendar month from the date the request is received. Recordings will be made available to the subject via a suitable format, unless we are advised not to by the police.

3.50 Individuals may request that we delete recordings about them. We will respond to such requests within one calendar month, explaining whether we intend to comply with the requests and the reasons why.

3.51 Individuals making such requests must provide identification details through which we can identify them as being the subject of the information.

4. Legislation and Regulation

4.1 Key legislative and regulatory requirements affecting this policy:

- Data Protection Act 2018
- UK General Data Protection Regulation 2021
- Environmental Protection Act 1990
- Human Rights Act 1998
- Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice
- ICO Guidance on Video Surveillance (including CCTV)

5. Responsibilities

5.1 The Managing Director of Customer Operations South London has overall responsibility for the delivery of, and compliance with, this policy.

5.2 Community Safety Managers have operational responsibility for the delivery of this policy, ensuring data is held and disclosed appropriately and approving surveillance in areas. They also ensure the Community Safety team manages surveillance in accordance with the ASB policies. The Head of Centre of Excellence for Community Safety is responsible for training, communicating to residents, and monitoring and reviewing the policy.

5.3 Heads of Service and Assistant Directors in other departments (such as Neighbourhoods) may also make decisions about data and external surveillance where appropriate. In their absence, decisions for these areas must be made by the relevant Director or Executive Director.

5.4 Colleagues take an honest appraisal of the situation and make appropriate responses on a case-by-case basis using the ASB Policies to guide them.

Approval

Version number	1
Effective from	*27 February 2023*
Policy owner	Managing Director South London Customer Operations