CCTV Policy

Policy Name	CCTV Policy
Effective Date	1st August 2025
Approved By	Harbour Light Board
Approval Date	1st August 2025
Policy Owner/Dept	Information & Data Governance
Policy Author	Peter McEleavey
Review Date	1st August 2028
Version Number	1.0

Version	Date	Changes	Approver

Relevant National Standards or Regulations	• Surveillance Camera Code of Practice (Home Office, under the Protection of Freedoms Act 2012). • British Standard BS EN 62676 – Video Surveillance Systems. • RSH consumer standards relevant to safety/ASB (Home & Neighbourhood and Community Standards). • ICO guidance on video surveillance/CCTV.

Relevant Legislation	• UK GDPR and Data Protection Act 2018. • Protection of Freedoms Act 2012 (framework for surveillance cameras). • Human Rights Act 1998 (Article 8 – privacy). • Crime and Disorder Act 1998 (crime prevention context)

CCTV Policy

1. Purpose

Harbour Light Assisted Living CIC ("the Organisation") operates Closed Circuit Television (CCTV) systems at certain supported housing properties to enhance the safety and security of our tenants, staff, and visitors. The purpose of this policy is to ensure that any CCTV usage is necessary, proportionate, and compliant with relevant laws and regulations. It outlines why we use CCTV, where and how we use it, how footage is stored and handled, and the rights of individuals regarding CCTV images.

This policy aims to strike a balance between security needs and individuals' right to privacy. All CCTV operations will be conducted in accordance with the UK GDPR and the Data Protection Act 2018, as CCTV footage is considered personal data when individuals can be identified. We also adhere to the **Protection of Freedoms Act 2012** (which governs surveillance camera use in public spaces) and the associated **Surveillance Camera Code of Practice** issued by the Home Office. By following this policy, The Organisation ensures compliance with the expectations of our regulators and relevant standards – including the Regulator of Social Housing's standards on tenancy and community safety, and ICO guidance for surveillance systems – while upholding the privacy and dignity of those monitored.

Scope of CCTV Use: This policy covers all CCTV installations and monitoring conducted by or on behalf of the Organisation at its premises. It defines the purposes for which CCTV is used (e.g. security, crime prevention), establishes retention periods for footage, and sets rules for access and disclosure. It also clarifies the rights of tenants, staff, or members of the public who may be recorded on our CCTV.

Joint Controller status: Where CCTV systems are operated across Harbour Light's supported housing schemes in conjunction with the on-site Support Company, Harbour Light Assisted Living CIC and the Support Company act as **Joint Data Controllers** for the processing of personal data captured by the CCTV system, with responsibilities allocated through a written joint-controller arrangement and reflected in our privacy information and site signage.

Status: Since the use of CCTV involves processing personal data and can impact privacy, this policy is deemed **Statutory/Regulatory**. It ensures our CCTV practices meet legal requirements (UK GDPR, DPA 2018) and aligns with best practices such as the Surveillance Camera Code and the Housing Ombudsman's expectations for resident safety and privacy.

2. Scope

This CCTV Policy applies to all CCTV systems operated by The Organisation at any of its housing schemes or offices. It covers all equipment (cameras, recording devices, monitors) and all recorded material generated by those systems. Specifically:

- **Locations Covered:** All current and future sites where the Organisation installs CCTV cameras, typically in communal or external areas of our properties. This can include building entrances, lobbies, corridors, common rooms, parking areas, and building perimeters. **Private areas**, such as inside individual tenants' flats, bathrooms, or staff private offices (excluding the secure rooms where DVR equipment is kept), are **not** subject to CCTV monitoring under this policy. We do not use any hidden or covert cameras except in extreme circumstances permitted by law (and none are in use as of this policy's effective date).
- **Personnel and Users:** The policy governs all staff who have any role in the operation or management of CCTV (e.g. housing managers, maintenance supervisors, security personnel)

as well as any third-party security contractors or installers we might engage. It also informs tenants and the public about how the CCTV is used. All staff with access to CCTV footage must be trained on this policy and related procedures.

- **System Components:** It includes fixed CCTV cameras and any recording devices (Digital Video Recorders, Network Video Recorders, monitors). It currently does not include portable recording devices or body-worn cameras (which we do not use). Should we, in the future, use such devices, this policy would be updated or expanded to cover them.
- **Data Covered:** All images and video recordings captured by our CCTV systems, as well as associated data (such as date/time stamps or camera location labels). Even if the Organisation does not actively monitor the cameras at all times, the captured footage (stored on DVRs) is within scope. The policy also covers live monitoring if that occurs (e.g. staff viewing the live camera feeds).

The scope ensures that **any CCTV-related activity by The Organisation** is regulated by this policy. It does not cover CCTV operated by third parties (for example, if a neighbouring property has its own cameras covering nearby areas – those are outside our control). However, if we were to link into or share footage with third-party systems, that would be done under strict agreements consistent with this policy.

Finally, this policy should be read in conjunction with our GDPR Privacy Policy (IDG01) and Data Retention Policy (IDG02), which provide overarching principles for handling personal data and retention schedules, respectively, which also apply to CCTV imagery.

3. Responsibilities

Clear responsibilities are assigned to ensure the CCTV system is managed lawfully and effectively:

- **Data Protection Manager (Mark Adams):** Acts as the CCTV system owner for data protection purposes. The Data Protection Manager is responsible for ensuring that CCTV usage complies with UK GDPR and this policy. He reviews and approves any new CCTV installations or significant changes, conducts Data Protection Impact Assessments (DPIAs) for CCTV when required, and handles any data subject requests (e.g. access to footage). The DPM also arranges periodic audits of CCTV practices and provides training/guidance to staff regarding privacy considerations. Any concerns or complaints about CCTV should be directed to the DPM in the first instance.
- **Joint Controllers:** *At some schemes, CCTV is operated in a manner that means Harbour Light Assisted Living CIC and the on-site Support Company jointly determine the purposes and means of processing CCTV personal data and therefore act as **Joint Data Controllers**. In these circumstances, a written joint-controller arrangement will be maintained which sets out, in a clear and practical way, each party's responsibilities for compliance, including (as applicable): transparency and signage; provision of privacy information; handling and allocation of data subject rights requests (including Subject Access Requests); incident management and personal data breach reporting/notification; retention and deletion; access control and disclosure decisions; and managing processor/contractor access where relevant. The Data Protection Manager is responsible for ensuring that the joint-controller arrangement is in place for applicable sites, is reviewed periodically, and that key information about the arrangement is made available to tenants and other individuals in accordance with data protection requirements. Operational staff must follow the agreed site arrangements and must promptly refer any CCTV rights requests, complaints, or suspected data breaches to the Data Protection Manager.*

- **Operations/Facilities Manager:** (If such a role exists in the Organisation) Responsible for the day-to-day management of the CCTV equipment. This includes ensuring cameras and recording devices are maintained in good working order, arranging repairs or technical support, and controlling physical access to DVR units (which are kept in staff-only secure locations). The Operations Manager ensures that only authorised personnel can access the CCTV system and that signage is correctly installed and maintained.
- **On-site Staff (Housing Officers/Support Staff):** Staff working at properties with CCTV may have access to live camera feeds for immediate security monitoring. They must use this access strictly for the purposes stated in this policy (safety, ASB monitoring, etc.) and not for idle curiosity or any form of surveillance of individuals without cause. On-site staff should report any camera or recording malfunctions and any incidents captured by CCTV that might require further action (such as saving footage for evidence). They are also tasked with ensuring that no unauthorised person (including tenants or visitors) views the CCTV monitors or recordings.
- **IT Support / Security Contractors:** Any third-party contractors or technicians involved in installing or maintaining the CCTV hardware/software must be vetted and sign confidentiality agreements. They should only access footage or systems as needed for maintenance and under supervision if possible. If our IT personnel manage the network aspects of CCTV, they ensure the DVRs are not accessible via insecure connections and that systems are protected against hacking or unauthorised remote access.
- **Senior Management / Board:** The Board of Directors and senior leaders ensure that the decision to deploy CCTV is justified and periodically re-evaluated. They approve the CCTV Policy and any significant expansions of surveillance. They are also responsible for fostering a culture where privacy is respected – ensuring CCTV is used as a security tool, not as a means of unwarranted surveillance on staff or tenants. Senior management will be informed of any serious incidents of CCTV misuse or any data breaches involving CCTV footage.

Every person with responsibility must also be mindful of individuals' rights under data protection law. For example, if a tenant asks who to contact about viewing footage of themselves, staff should direct them to the Data Protection Manager. By clearly delineating these responsibilities, the Organisation ensures accountability in how our CCTV system is operated.

4. Legislation and Regulations

Our use of CCTV is governed by various laws and regulatory frameworks. This policy adheres to the following key legislation and standards:

- **UK General Data Protection Regulation (GDPR)** and **Data Protection Act 2018** – These set the legal requirements for processing personal data, including video footage. They require us to have a lawful basis for CCTV (such as legitimate interests in security), to inform people about the cameras, to secure the footage, and to allow individuals to exercise rights over their data (access, deletion, etc.).
- **UK GDPR (Joint Controllers):** Where Harbour Light Assisted Living CIC and a Support Company are Joint Data Controllers for CCTV processing, we will comply with the UK GDPR requirements for joint controllers by having a transparent written arrangement that sets out respective compliance responsibilities (including for data subject rights and transparency), and by making the essence of that arrangement available to individuals through appropriate privacy information and/or signage. Harbour Light will also have due regard to applicable ICO guidance on video surveillance and joint-controller accountability.
- **Protection of Freedoms Act 2012** – This Act includes provisions on CCTV and led to the creation of the government's Surveillance Camera Code of Practice. It emphasises that CCTV

must be used proportionately and transparently in pursuit of a specified purpose (like crime prevention). We comply with the 12 guiding principles of the Surveillance Camera Code (e.g. having a named responsible person, clear justification, and regular review of CCTV use).

- **Surveillance Camera Code of Practice (Home Office, 2013)** – A code issued under the Protection of Freedoms Act. While not all housing providers are legally required to follow it, we choose to adopt its best practices. It covers issues like the necessity of CCTV, effectiveness, transparency (signage and public awareness), and security of footage.
- **Human Rights Act 1998 (Article 8)** – Although a private organisation like ours is not directly bound by the Human Rights Act in the same way as public authorities, the principles of respecting individuals' privacy apply. CCTV has to be used in a way that does not infringe on reasonable expectations of privacy. Notably, we avoid surveillance in private areas, and we ensure our use is proportional (e.g. focusing on public/communal zones).
- **Regulator of Social Housing Standards** – Particularly the **Neighbourhood and Community Standard** and **Home Standard**, which expect registered providers to keep neighbourhoods safe and collaborate to prevent anti-social behaviour. Our CCTV use supports these standards by deterring and helping address crime or ASB around our properties. We also note the **Tenant Involvement and Empowerment Standard**, which includes respecting the privacy and home of tenants – hence we consulted tenant views (or will do so) if installing cameras in new locations.
- **Housing Ombudsman's Expectations** – While there is no direct Ombudsman policy on CCTV, the Ombudsman's Complaint Handling Code expects landlords to address safety concerns and complaints. Having a clear CCTV policy means tenant concerns about surveillance can be properly handled, and any misuse could be grounds for complaint through the Ombudsman.
- **British Standards (BS EN 62676 series)** – These are technical standards for video surveillance systems. Though mainly relevant to system installers, adherence ensures our equipment meets quality and security benchmarks.
- **CIC Regulatory Requirements** – As a Community Interest Company, we commit to acting in the community's benefit. Using CCTV responsibly to enhance community safety aligns with that mission. The Office of the Regulator of CICs expects us to operate transparently and lawfully; this policy demonstrates our compliance in the context of surveillance.

This policy is therefore built on **Statutory** requirements (Data Protection law, Protection of Freedoms Act) and informed by **Regulatory/Best Practice** standards (RSH guidance, Surveillance Camera Code). We will also consider any guidance issued by the ICO specifically on CCTV (such as the ICO CCTV Code of Practice, which provides practical advice for organisations using CCTV). Compliance with these laws and standards is not optional – it is mandatory and is monitored through internal audits and could be subject to external oversight (e.g., ICO investigations or regulator reviews).

5. Procedures

5.1 CCTV Installation and Operation

Locations of Cameras: CCTV cameras are installed only in communal and external areas of our properties where there is a justified need for surveillance. Typical locations include building entrances and exits, lobby areas, shared corridors or hallways, stairwells, parking lots, and the exterior perimeter of buildings (covering approaches, pathways, etc.). We do **not** install cameras in any private dwelling areas (inside tenant apartments), nor in private spaces like toilets, showers, or areas where people have a heightened expectation of privacy. Additionally, cameras are not placed in staff break rooms or offices (except in the secure room where the recording equipment resides, which is itself a restricted area).

Before any new camera is installed, we assess its field of view to avoid intrusive coverage. Cameras are positioned to monitor only the intended spaces (for example, the entrance door and immediate surroundings) and not to look out onto public streets beyond our property, nor into anyone's private residence (windows of adjacent buildings, etc.).

Signage: We display clear and prominent **CCTV signage** at all sites with CCTV. Signs are typically placed at building entrances and other key locations to inform residents and visitors that CCTV is in operation, the Organisation operating it, and a contact (usually our phone number or office) for more information. This meets our transparency obligation – people must know they are under surveillance. Signs read approximately: "CCTV in operation for the safety of residents and staff. Images are recorded by Harbour Light Assisted Living CIC. For questions, contact 0151 909 5919."

Notification: Tenants are informed about CCTV presence and purposes through tenancy agreements or welcome packs, and via this policy, which is available on request and on our website. If we plan to introduce CCTV to a new location, we will consult or notify affected tenants and staff in advance, explaining the rationale.

System Operation: CCTV cameras generally operate continuously, 24 hours a day, recording video footage to the DVR (Digital Video Recorder) system. We do not routinely have personnel monitoring live feeds in real-time, except where on-site staff may occasionally view monitors to check on an ongoing incident or at certain times (e.g., night wardens glancing at screens to see if any disturbance in common areas). The system is primarily recording for post-incident review.

Cameras are fixed focus (we do not operate any pan-tilt-zoom (PTZ) cameras). A small number of our cameras have audio recording capability; where audio is enabled, this will only be for clearly defined security and safety purposes, and we will ensure this is proportionate, transparent, and reflected in site signage and privacy information. Access to live and recorded CCTV (including any audio where present) is restricted to authorised staff only, and any access/use is appropriately controlled. We do not use facial recognition or automated analytics capabilities on our CCTV systems; it is used for security and incident investigation purposes only.

The CCTV system is configured with date and time stamps on footage. We ensure the system clock is maintained accurately (adjusted for BST/GMT changes) as accurate timestamps are important for investigations.

Regular checks are performed (e.g., weekly) to ensure cameras and recording devices are functioning (no lens obstructions, adequate lighting, and DVR recording properly). If a camera is found to be faulty or out of alignment, we aim to repair it promptly. During downtime, we may put up a notice if appropriate and inform tenants if the outage is prolonged and affects security.

5.2 Purposes of CCTV Use

CCTV is deployed by The Organisation for specific, limited purposes. We list these purposes clearly, and all use of CCTV must fall under one or more of these objectives:

- **Safety of Tenants and Staff:** The primary purpose of our CCTV is to help ensure the safety and security of people in and around our properties. Cameras serve as a deterrent to those who might cause harm and provide reassurance to residents that there is an additional layer of security. In the event of incidents (e.g., an intruder or a threat to a resident), CCTV can provide real-time visibility and recorded evidence to respond effectively.

- **Monitoring and Addressing Anti-Social Behaviour (ASB):** Our supported housing schemes, at times, may face issues like vandalism, graffiti, loitering, or other anti-social behaviour in communal areas. CCTV is used to monitor such behaviour, assist in identifying those responsible, and support appropriate action (such as warnings, tenancy enforcement, or involving authorities). It also helps us provide factual evidence when responding to complaints about ASB from residents.
- **Crime Prevention and Detection:** We aim to prevent crimes such as theft, burglary, or trespassing on our properties. Visible cameras act as a deterrent to criminal activity (like breaking into the building or cars in the car park). If a crime does occur, the recorded footage can aid in detecting and investigating the incident – for instance, by providing images of suspects to the police or documenting the sequence of events.
- **Property Protection:** CCTV helps us protect the Organisation's property (the buildings, equipment, etc.) from damage. For example, if there is illegal dumping of rubbish or damage to fire equipment, the cameras might capture who was responsible, allowing us to take follow-up action. This protects the safety of the environment and can save costs on repairs.
- **Supporting Staff in Incident Response:** In supported housing, staff sometimes need to attend incidents (e.g., a tenant's medical emergency in a corridor, or a conflict between residents). CCTV can support staff by allowing a quick assessment of a situation remotely (on a monitor) before physically intervening, thus promoting staff safety. After an incident, management can review footage for debrief and to improve future responses or training.

Explicit Exclusions: We do **not** use CCTV for general monitoring of staff performance or tracking staff movements. Footage is not analysed to evaluate staff work habits or tenant routines. The only time staff behaviour might be reviewed is if there is an allegation of misconduct or an incident involving staff – and even then, any review must be justified and limited to that investigation. This is in line with ensuring CCTV use remains proportionate and focused on security, not everyday surveillance.

We also do not use CCTV to enforce tenancy terms unrelated to safety. For example, we wouldn't normally use cameras to check if someone has an unapproved pet or a guest (unless that issue manifests as a security concern or ASB, like a disruptive visitor).

By clearly defining the purposes above, we maintain **purpose limitation** – meaning footage collected will only be used to fulfil these security and safety objectives and not for any incompatible purpose. If a new purpose arises, we would need to update this policy and potentially inform tenants (for instance, if we ever considered using cameras to monitor parking compliance, we would treat that as a separate purpose requiring notice).

5.3 Data Retention and Storage of Footage

All CCTV footage recorded is stored in a secure manner to prevent unauthorised access or tampering. Our practices for retaining and storing CCTV recordings are as follows:

- **Storage Medium and Location:** CCTV footage is recorded and stored on local Digital Video Recorders (DVRs) or Network Video Recorders (NVRs) physically located on-site at each scheme where cameras are installed, typically within the Support Company's staff-only offices or locked communications rooms. Routine CCTV footage is not stored in cloud storage as part of the normal recording process.
- **Remote Access:** Where enabled, the DVR/NVR may be accessed remotely by authorised Harbour Light and/or Support Company personnel using secure credentials and controlled access arrangements.

- **Exported Evidence Copies:** Where footage is required for an investigation, safeguarding, complaint handling, legal action, or disclosure to a competent authority (for example, the Police), a specific clip may be extracted from the DVR/NVR and stored securely as an "evidence copy" within Harbour Light's approved secure environment (for example, within Microsoft 365). Exported copies are handled under strict access controls and retained only for as long as necessary for the relevant purpose.
- **Retention Period:** Recorded footage is retained for a maximum of 30 days. Our standard configuration aims for approximately one month of rolling storage. The exact retention within that range can vary depending on the DVR's storage capacity and the number of cameras (e.g., a busy camera might overwrite a bit sooner if the hard drive fills). However, under normal conditions, we do not exceed 30 days for routine footage. Footage older than 30 days will be automatically overwritten or securely deleted. We consider a 30-day retention to be sufficient for security purposes, as incidents are typically noticed and acted upon within that timeframe.
- **Automatic Overwrite:** The DVRs are set to auto-delete/overwrite old footage once the retention period is reached or the disk space is full. This means the system continuously records new images over the oldest ones. There is no indefinite accumulation of footage. This automated process ensures obsolete data does not linger beyond the set period without manual intervention, supporting compliance with the GDPR storage limitation principle.
- **Extended Retention for Incidents:** If a particular segment of footage is needed for an investigation or evidence (for example, a tape of a crime or a serious incident), we will **securely extract and save that specific footage** before it is overwritten. Such extracted footage may be retained longer than 30 days solely for the purposes of the investigation or any ensuing legal action. Once it has served that purpose and is no longer needed (e.g., the case is closed), it will be deleted. Any extended retention is documented, including reasons and duration.
- **Access Security:** The DVR units and any network equipment are password-protected. Only authorised personnel have login credentials to access the recorded footage. There are tiers of access – for instance, on-site management may be able to view live feeds on a monitor but not access archives without approval. Full administrative access (to change settings or export footage) is limited to designated senior staff or IT support. We do not permit remote access to the CCTV system for non-authorised persons. Where remote access is enabled for operational purposes, it is restricted to authorised Harbour Light and/or Support Company personnel, protected by strong authentication and passwords, and limited to legitimate purposes set out in this policy. Remote access settings are reviewed periodically and removed where no longer required.
- **Integrity and Backup:** While footage is only stored locally, the integrity of recordings is important. The system records in a tamper-evident format (watermark or checksum) where possible, to ensure that any attempt to alter footage would be detectable. We do not make regular backups of CCTV footage (since it's short retention), but if footage is exported for evidence, copies are handled carefully (e.g., on an encrypted USB drive) and logged. The exported copies themselves are kept secure and subject to the same retention considerations. Where evidence copies are stored electronically (for example, within Microsoft 365), access is restricted to named recipients, sharing is time-limited where possible, and a record of disclosure is retained.

In summary, routine CCTV footage is recorded and stored securely on-site and retained for no more than 30 days, unless a specific clip is extracted and retained as an evidence copy for a defined incident purpose.

5.4 Access and Disclosure of Footage

Access to CCTV footage is strictly controlled. Not everyone can view or retrieve CCTV recordings – only those with a legitimate need and authorisation. The following rules apply to access and disclosure:

- **Internal Access:** Internally, only designated staff can access the CCTV recordings. Typically, this includes the Data Protection Manager, relevant Operations/Security managers, and senior management if required. On-site housing staff may have access to live feeds but **not** the ability to replay or export footage on their own. If they become aware of an incident and believe footage needs to be reviewed, they must request this through an authorised person (e.g., request the Data Protection Manager or a manager to review the footage). The CCTV systems in use across Harbour Light schemes may not provide a comprehensive automated audit trail of user access, playback, or export activity. Harbour Light therefore controls access by limiting remote and on-site access to authorised personnel only, using secure credentials and role-based permissions where available.

  Where footage is exported or disclosed (for example, for safeguarding, investigations, complaints, legal proceedings, or disclosure to a competent authority such as the Police), Harbour Light will retain an appropriate record of the disclosure. This record may include the reason for export/disclosure, date and time, the footage reference (camera/date/time range), the recipient, and the method of transfer (for example, secure link or encrypted media). Records may be held within incident files, email correspondence, case management records, or other secure organisational systems.

- **Live Monitoring:** Live CCTV monitors, where present (such as a screen in an office showing camera feeds), are positioned so that they are only visible to staff, not to the general public or unauthorised viewers. Staff should ensure that if they leave the office, the office is locked. We treat the live feed with the same sensitivity as recorded footage.
- **Disclosure to External Parties:** We will only disclose CCTV footage to external third parties in a few specific circumstances, and always in compliance with data protection law:
    - **Law Enforcement:** If the police or other law enforcement agencies formally request CCTV footage for the investigation or prosecution of a crime, we will cooperate and provide the relevant footage. Typically, the police will provide a request identifying a time window or incident. We will verify their credentials and ensure the request is documented (e.g., a form or written request). We may also initiate sharing if we have captured evidence of a serious crime (e.g., burglary); in such cases, we would contact the police proactively, following legal guidelines.
    - **Legal Proceedings:** In response to a court order or in preparation for legal proceedings, footage may be disclosed to solicitors or courts. For example, if there is a personal injury claim or an anti-social behaviour injunction case where CCTV is evidence, we will provide copies as required through the proper legal process. Only footage relevant to the case will be disclosed.
    - **Regulatory Bodies:** If a regulatory body such as the Regulator of Social Housing or the Housing Ombudsman or the ICO legitimately needs to see footage (for instance, investigating a complaint or data breach), we will grant access as required by law.
    - **Insurance Companies:** We generally do not share footage with insurance companies or any private entities unless it is necessary in relation to a claim that involves the Organisation (for example, if a contractor claims they were injured on our property,

and our insurer needs evidence). Even then, we ensure only relevant footage is shared and that the recipient will handle it securely.

- **No Unauthorised Disclosure:** We do **not** permit disclosure of CCTV images to the media, other tenants, or the public at large, unless there is an exceptional reason and a lawful basis. For instance, we wouldn't release footage to the media for publicity or to shame someone. In some cases, police might release images of suspects to the public, but that would be their decision under their legal powers, not ours directly. We also do not allow staff to use or circulate footage informally (no screenshots sent around, no posting on social media, etc.). Any misuse of footage in this way would be a disciplinary matter.
- **Third-Party Viewing:** Occasionally, an individual (non-police), such as a victim of a crime, might request to view footage to identify a perpetrator. Our usual practice is to handle such matters through the police. We would not show raw footage to private individuals, both for privacy reasons and chain-of-evidence reasons. Instead, we'd advise them to file a police report or a subject access request (if they themselves are in the footage).

All disclosures are made in line with the GDPR's rules on data sharing – ensuring we have a legal basis (such as legal obligation or legitimate interests) and that we redact or limit footage to what's necessary. For example, if we share footage externally, we might blur or redact images of other individuals not relevant to the request to protect their privacy (see next section on individual rights).

In summary, **access to CCTV footage is limited to authorised personnel** for legitimate purposes, and **external disclosure is tightly controlled**. We treat all recordings as sensitive personal data and handle them accordingly.

5.5 Individual Rights and Subject Access Requests (SARs)

People whose images are recorded by our CCTV cameras have rights under the data protection law. The Organisation acknowledges these rights and has procedures to facilitate them:

- **Right of Access (Subject Access):** Individuals have the right to request access to personal data that we hold about them, including CCTV footage in which they appear. If a tenant, staff member, or visitor believes they were captured on our CCTV and wants to see the footage, they can submit a Subject Access Request (SAR) to us. They should provide details like the date, time, location, and a description of themselves to help identify the relevant footage.
    - We will verify the identity of the requester (especially if it's a tenant or someone we don't know well) to ensure we don't release footage to the wrong person.
    - Once we have sufficient information, we will search for the footage. If footage is found and it contains the requester, we will arrange for them to view it, or we will provide still images, **except** we will **redact** (blur or obscure) images of other individuals in the footage for privacy, unless those individuals have consented or it is otherwise fair to disclose (rare). This means if others are clearly identifiable in the same frame, we may pixelate them or use techniques to hide their identity. If redaction is not feasible (e.g. it would take disproportionate effort or render the footage useless), we may invite the requester to view the footage in a controlled setting rather than giving a copy.
    - We will respond to CCTV access requests within **one calendar month**, as per GDPR timelines. If a request is complex (for example, covering a long-time span or multiple cameras), we may extend by up to 2 further months, but we will inform the requester of this within the first month.
    - We do not charge for SARs of CCTV footage, but if a request is manifestly unfounded or excessive (for instance, someone asking to see "all footage of me ever" without

narrowing it down), we reserve the right to refuse or charge a reasonable fee. We will work with requesters to clarify overly broad requests (e.g. asking them to specify a date/time). Vague or very broad requests that require unreasonable effort (like searching weeks of footage without a clear timeframe) may be refused on proportionality grounds, but we will explain why and try to assist in refining the request.

- **Right to Erasure:** A person can ask us to delete CCTV footage of them, but this right is not absolute. Typically, if the footage has not yet been overwritten and the individual appears, we might consider erasing or blurring them if the footage isn't needed. However, if the footage is being retained for a lawful reason (e.g., it captured a crime and is evidence), we will likely refuse erasure as we have a compelling reason to keep it. In practice, most CCTV is overwritten in 30 days, so by the time we get an erasure request, the data might be gone. If not, we handle such requests case by case, balancing the individual's rights with our necessity for the footage.
- **Right to Object:** Individuals generally have a right to object to processing based on our legitimate interests. If someone objects to being recorded by CCTV (for instance, a resident has concerns), we'll consider their objection. We may decide that our legitimate interest in running CCTV for safety overrides the objection, but we would document the reasoning. If possible, we might offer compromises (like adjusting a camera angle) if it's a reasonable request and doesn't undermine security. However, outright exclusion of someone from being filmed in common areas is usually not feasible if they use the space, since cameras can't practically be turned off for one person.
- **Complaints:** If anyone believes our CCTV is excessive or not in compliance with laws, they can raise a complaint to the Data Protection Manager. We will investigate and respond. They also have the right to complain to the ICO if they're unsatisfied. We note this in our publicly available privacy information. For example, a tenant concerned about CCTV intrusiveness can go to the ICO if they feel we're misusing cameras. We strive to address issues internally first.

The Organisation will **never retaliate or discriminate** against an individual for exercising their privacy rights. We treat requests confidentially and professionally. We also ensure that staff know how to recognise a request: for instance, if a tenant says, "I want to see the camera footage of me in the lounge last week," that is a valid SAR and should be forwarded to the Data Protection Manager immediately.

We keep records of all SARs and outcomes, including CCTV requests, as part of our GDPR compliance logs.

In conclusion, individuals **have the right to request access to CCTV images of themselves**, and we have a clear process to respond within legal timeframes, balancing that with others' privacy. We aim to be transparent and fair in handling these rights.

5.6 Security of CCTV Systems and Audit

Maintaining the security of the CCTV system itself is a key part of this policy (protecting the data from unauthorised access, alteration, or loss):

- **System Security:** The DVRs are located within the Support Company's on-site offices. Those rooms are leased to, and controlled by, the Support Company, who therefore manage day-to-day physical security and access arrangements. Harbour Light retains access (including keys where applicable) for oversight and essential operational purposes, however physical access control to those rooms is primarily exercised by the Support Company. Harbour Light requires

that DVRs are kept within secure, locked environments and that access is restricted to authorised personnel only, with appropriate records maintained where feasible.

- Logical and system security controls are applied to the extent they are within Harbour Light's control: systems are protected by strong passwords, default manufacturer credentials are changed at setup, and passwords are updated periodically and whenever an individual with access leaves their role. Where CCTV is connected to a network, segmentation from general networks is used where possible to reduce exposure. Firmware on cameras and recording units is kept up to date to address known security vulnerabilities.
- **Access Controls (Footage Viewing and Export):** Our current CCTV recording equipment does not provide automatic user audit trails, and we do not maintain a manual access log. To ensure accountability and appropriate governance, access to live or recorded footage is restricted to authorised personnel only and permitted solely for defined, legitimate purposes (for example, the investigation of incidents, crime prevention, safeguarding, or responding to lawful requests). Any viewing, downloading, copying, or disclosure of footage must be approved in advance by the Data Protection Manager (or an authorised deputy) and will be handled in accordance with our data protection procedures, including maintaining appropriate records where required (for example, where footage is disclosed externally or relied upon for decision-making).
- **Regular Audits:** The Data Protection Manager (or an appointed auditor) will conduct periodic audits of CCTV use. This includes checking that signage is in place, that retention rules are being followed (no old footage beyond 30 days), and that any issues or complaints were handled. The audit might also review whether cameras remain justified – if a camera consistently shows no incidents and residents find it intrusive, we could evaluate removing or repositioning it. A full review of whether CCTV is still needed at each site will occur at least at policy review time (every three years) or sooner if circumstances change (for instance, if a building becomes a lower-risk environment, maybe CCTV could be reduced).
- **Data Breach Protocol:** If there is any suspicion that CCTV footage has been accessed by an unauthorised person or disclosed improperly (for example, a stolen DVR or a leaked video), this is treated as a **data breach**. We will follow our Data Breach Response procedures: contain the breach, investigate, notify the ICO within 72 hours if it meets the reportable threshold, and inform affected individuals if there is a high risk to them. We will also take corrective action to prevent recurrence (e.g., improving security, disciplining staff involved in misuse).
- **Maintenance and Repairs:** When service or repairs are needed, only authorised contractors are used. We supervise where possible. If a device must be removed for repair, we check that no footage remains on it, or we get assurance from the repair service about confidentiality. End-of-life equipment that stores footage (like an old hard drive) is destroyed or wiped.
- **Integration with Other Systems:** Currently, our CCTV is a stand-alone system. If in future we integrate it with other systems (like linking to door entry systems, or alarms that trigger cameras), we will evaluate any new privacy impacts. This policy will be updated accordingly, and staff will be trained on the new usage rules.

By rigorously securing and auditing our CCTV operations, we ensure that the system remains a tool for safety and does not become a risk in itself. This reinforces trust among our tenants and staff that CCTV is managed responsibly.

5.7 Complaints and Compliance

Anyone with concerns or complaints about our use of CCTV can raise them, and we will address them promptly:

- **Internal Complaint Process:** Tenants or staff who feel that CCTV is being misused, or who have a complaint (for example, "a camera points at my window" or "staff are looking at cameras when they shouldn't"), should contact the Data Protection Manager (Mark Adams). Contact can be made via email at cctv**@harbourlight.org.uk**, by phone at **0151 909 5919**, or by writing to our office at 71 Linacre Road, Litherland, Merseyside, L21 8NP. We will treat complaints seriously and confidentially. The Data Protection Manager or a designated officer will investigate the issue, speaking with relevant staff, and checking camera configurations. We will aim to respond with findings and any corrective actions within a reasonable time (usually 20 working days). If a complaint requires urgent action (for example, a camera causing a clear privacy intrusion), we will act immediately to mitigate the issue while the investigation is ongoing.
- **Escalation:** If the complainant is not satisfied with the internal resolution, they have the right to escalate their concerns. Tenants may escalate to the Housing Ombudsman Service if it's affecting their housing rights (though typically the Ombudsman would ensure our internal process is exhausted first). Any individual (tenant, staff or public) may also lodge a concern with the **Information Commissioner's Office (ICO)**, which regulates data protection compliance. The ICO can be contacted through **ico.org.uk** or by telephone. We inform individuals of this right in our responses. The ICO can investigate how we use CCTV and can issue enforcement or require corrective measures if we are found non-compliant.
- **Regulatory Oversight:** We acknowledge that improper use of CCTV could also draw scrutiny from the Regulator of Social Housing or the Office of the CIC Regulator under governance or tenant treatment standards. We therefore commit to full cooperation with any external reviews.
- **Staff Compliance:** Compliance with this CCTV Policy is mandatory for all Harbour Light staff and contractors with CCTV-related duties. Any breach of this policy by staff (e.g., unauthorised viewing or sharing of footage, or misuse of cameras) may result in disciplinary action, up to and including termination of employment or contract. Staff are made aware of this, and of the importance of respecting privacy. We include CCTV policy review in staff induction for those working on sites with cameras, and periodic refreshers in training.
- **Community Engagement:** We remain open to feedback from our residents about CCTV. We understand some people may feel uncomfortable with cameras. While safety is our priority, we try to engage residents (for example, in resident meetings) about where cameras should be and how the footage is used. This transparency and involvement can itself prevent complaints by addressing concerns proactively.

By providing clear channels for complaints and ensuring accountability, we maintain trust and ensure that our CCTV usage continues to meet its intended goals without overstepping reasonable boundaries.

6. Review and Updates

This CCTV Policy will be reviewed every **three years**, or sooner if required due to changes in relevant legislation, regulatory guidance, or the operational needs of the Organisation. The next scheduled review will occur by **June 2028** (three years from the effective date of this version).

The review process will include evaluating whether the use of CCTV is still achieving its intended purposes and whether those purposes remain justified. We will consider technological changes, changes in the law, and any feedback or complaints received during the period. For example, if new data protection laws or updated ICO codes of practice on CCTV are introduced, we will update this policy to reflect those. If we expand CCTV to new sites or add new capabilities (like audio recording or

integration with alarms), we will conduct a fresh Data Protection Impact Assessment and update the policy accordingly.

Any revisions to this policy will be approved by senior management. The version number will be incremented, and a summary of changes will be recorded in the policy document control. We will communicate major changes to tenants and staff, especially if the changes impact how CCTV operates or individuals' rights (for instance, if we decided to use cloud storage or increase retention, which we currently do not – such a change would be clearly communicated and likely require consultation).

Version History:

- **Version 1.0** – Effective 1st August 2025. Initial standardised CCTV Policy covering all key aspects (purpose, scope, responsibilities, etc.) aligned with GDPR and regulatory standards.

Future versions (e.g., 1.1, 2.0) will be noted here with dates and a brief description (e.g., "Updated to include new site installations" or "Amended retention period following law change").

By keeping this policy up to date, The Organisation ensures continued legal compliance and effective, fair use of CCTV as part of our commitment to providing a safe living environment in our supported housing schemes. All staff and relevant parties will be expected to familiarise themselves with the latest version of the policy and act accordingly to remain in compliance.