CCTV Policy & Procedure

CCTV (Closed Circuit Television) POLICY AND PROCEDURE	
Purpose	This policy sets out how Harrison Housing will manage the operation and use of CCTV systems at its properties.
Applies to	All Harrison Housing Employees, Trustees, Contractors, Consultants, Volunteers, Residents and their Visitors.
Date first implemented	March 2025
Author	Housing Manager
Date first approved by Leadership Team	February 2025
Date first approved by Board of Trustees	March 2025
Review Frequency	Every 3 Years
Service Area	Housing Management
Document Status: This is a controlled document. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local drives but always accessed from the Policy Library.	

CONSEQUENTIAL AMENDMENTS (made prior to full policy revision)		
Amendment Date	**Nature of Amendment**	**Revised by**

VERSION HISTORY			
Revision Date	**Version No.**	**Revised by**	**Approved by**

CURRENT POLICY REVISION	
Date revised	February 2025
Revised by	Housing Manager
LT approval date	February 2025
Board of Trustees Approval date	March 2025
Next revision due	February 2028

1. Policy Statement

1.1 Harrison Housing uses Closed Circuit Television (CCTV) systems at the housing schemes which it owns or manages. Due to its location this provision also covers the Harrison Housing head office building at 46 St James's Gardens, London W11 4RQ.

1.2 This policy sets out how Harrison Housing will manage the operation and use of its CCTV systems.

1.3 We will maintain a balance between ensuring the security of our buildings and safety of both residents and staff, with due respect for the privacy of our residents and staff going about their lawful business. Our use of CCTV will be proportionate to the risks it is intended to mitigate against.

2. Policy Principles

2.1 Harrison Housing has a legitimate business purpose for using CCTV in our schemes and offices. It will be used for the following purposes (list not exhaustive):

2.1.1 To prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime.

2.1.2 To support internal investigations, and law enforcement in the prevention, detection and prosecution of a crime, the apprehension of offenders, and the prevention and detection of safeguarding incidents.

2.1.3 For the personal safety of employees, residents, visitors and other members of the public and to act as a deterrent against crime.

2.1.4 To assist in day to day management, including ensuring the health and safety of employees, residents and other individuals in and around Harrison Housing premises.

2.1.5 To assist in the effective resolution of disputes which may arise during disciplinary or grievance proceedings.

2.1.6 To assist in the defence of any civil litigation, including employment tribunal proceedings; and

2.1.7 To assist our insurers or solicitors to consider issues of liability and indemnity.

2.2 CCTV systems will be used in a manner which is proportionate to the risk which is being mitigated or issue which is being investigated. The

positioning of any cameras will take into account individuals' privacy, in particular in their dwellings and in sensitive locations in communal areas of our schemes or offices, such as around toilet facilities.

2.3 CCTV coverage amounts to personal data which must be processed in accordance with data protection legislation and regulation. Data will be stored securely for the minimum necessary period (usually no more than 30 days), and will only be accessed in accordance with this policy by staff who are authorised to do so. Images will only be downloaded and shared in accordance with clearly defined rules set out herein.

2.4 Failure to comply with this policy will amount to a breach of the staff disciplinary standard, up to and including gross misconduct. In certain circumstances, misuse of information generated by CCTV or other surveillance systems can constitute a criminal offence.

3. Implementation

3.1 All staff will be made aware of this policy through Harrison Housing's internal communication channels, including email.

3.2 Changes to this policy and its associated procedure, if applicable, will be communicated to all staff.

3.3 All staff will be required to read this policy, and to confirm that they have read and understood it.

3.4 This policy will be published to residents through our website and via Resident Engagement Forums.

4. Other Policies, Regulations and Legislation

4.1 This policy should be used in conjunction with the following policies, regulations and legislation:

- ASB Policy
- Complaints Policy
- Data Protection & Confidentiality Policy
- Domestic Abuse Policy
- Equality & Diversity Policy
- Safeguarding Vulnerable Adults Policy

- Data Protection Act 2018
- Information Commissioner's Office (ICO) CCTV Code of Practice
- Home Office Surveillance Camera Code of Practice 2021
- Human Rights Act 1998

- Protection of Freedoms Act 2012
- Regulation of Investigatory Powers Act 2000
- Regulator of Social Housing Neighbourhood and Community Standard (April 2024)
- UK General Data Protection Regulations

5. Responsibility

5.1 Harrison Housing is registered for Data Protection purposes with the Information Commissioner's Office, registration reference Z8927155.

5.2 The Chief Executive Officer (CEO) acting on behalf of the Board of Trustees has overall responsibility for ensuring that Harrison Housing has an appropriate CCTV Policy in place. The CEO is designated the Data Controller for Harrison Housing.

5.3 The Data Controller has overall responsibility for the management and operation of the CCTV systems and the implementation of this policy. This will include arranging for training for all staff who have access to the CCTV systems on their operational use and the requirements of this policy.

5.4 The Data Controller will ensure that the CCTV systems are operated according to this policy and that regular audits are carried out to ensure that the relevant procedures are complied with.

5.5 The Housing Manager is responsible for monitoring the use of and access to CCTV systems in the housing schemes, and for providing guidance to the team of Scheme Managers on appropriate use.

5.6 The Housing Manager will assess the potential need for additional CCTV and make recommendations to the Data Controller, using a Data Protection Impact Assessment (DPIA) (Appendix A).

5.7 Where necessary the Housing Manager will initiate disciplinary investigation if misuse of the CCTV systems is suspected.

5.8 Scheme Managers will be responsible for complying with this policy at all times in their use of CCTV systems at their schemes, for reporting faults and for advising residents of the purpose and limitations of the CCTV system where queries arise. Scheme managers should also draw to the attention of the Housing Manager any concerns about the existing systems, and set out their proposals for improvements, amendments or additions.

6. Installation of CCTV

6.1 A proposal to install CCTV at one or more of our schemes may arise from a proposal from staff, a request from residents, or a recommendation from law enforcement services including the police.

6.2 The potential reasons for installing a CCTV system are listed above in paragraph 2.1.

6.3 Any decision to install a CCTV system will be based on a Data Protection Impact Assessment completed by the Housing Manager and approved by the Data Controller. This will consider:

6.3.1 The scale of any problem which has given rise to the proposal. Installation of CCTV systems must be proportionate to the risk we are seeking to mitigate.

6.3.2 The potential for intrusion on the privacy of individual residents, and employees going about their lawful business. We will also consider the potential intrusion on the privacy of members of the public or people in neighbouring properties.

6.3.3 The estimated cost of installing and maintaining the proposed equipment, in proportion to the size of the scheme and the likely impact on residents' service charges.

6.3.4 The layout of the building concerned and any planning restrictions which might apply e.g. for listed buildings.

6.3.5 Consultation with residents in the scheme, seeking feedback on the factors listed immediately above.

6.4 Cameras will usually be located to cover the main entrance and exit points of the scheme, and external communal areas. Cameras will not be located in such a way as to cover the entrance to individual residences, or where this is difficult to achieve, the relevant section of the coverage will be obscured or blurred. We will not usually set cameras to capture sound recordings.

6.5 They will be located so as to ensure their security and protection from vandalism. Cameras which record continuously will be recording 24 hours a day, every day of the year. Motion activated cameras will be capable of being activated 24 hours a day every day of the year.

6.6 Where CCTV systems are in use, signs will be displayed to alert residents and other people on our premises to the existence of the CCTV system. Such signs will identify Harrison Housing as the organisation operating the system, the purpose for using the system and who to contact for further information.

6.7 We will only make use of covert recording (without signage) in very exceptional circumstances, and in liaison with law enforcement agencies. This will only usually happen in the event of a serious criminal offence being suspected. We will only do this where other less intrusive methods have been considered first, and will follow the completion of an additional Data Protection Impact Assessment, and approval by the Data Controller for Harrison Housing.

6.8 Dummy CCTV cameras or signage are strictly prohibited. Their use can result in risk to life of individuals and leave the organisation open to litigation.

6.9 The control units and monitors for any CCTV system will be located so that this hardware is secure and not on general display (e.g. locked in a cupboard or situated in a lockable office with the monitor switched off unless being accessed securely by a Harrison Housing employee).

6.10 Scheme managers will be expected to make a weekly check via the monitor displaying live recording that the system is functioning. It is not an expectation that scheme managers will routinely access the CCTV system to check recordings unless one of the circumstances listed in paragraph 7.3 applies.

6.11 Our CCTV systems will be maintained regularly under a service contract to be set up by the Asset Management Team. Faults will be reported by Scheme Managers or Property Services staff in accordance with the terms of the service contract.

7. Storage and Retention of CCTV coverage

7.1 CCTV footage will be stored securely, and retained for no longer than 30 days where no need to download or disclose such footage exists.

7.2 Where CCTV coverage is to be reviewed or downloaded, each instance will be recorded on a central log by the staff member who has accessed the CCTV system (usually the Scheme Manager or Housing Manager).

7.3 In agreement with the Housing Manager, the Scheme Manager may review (but not download) existing footage in the event of one of the following circumstances:

7.3.1 A potentially criminal incident has been reported to the Scheme Manager by a resident, colleague or member of the public.

7.3.2 A safeguarding concern has been raised in respect of a resident where an incident may have occurred in an area of the scheme covered by CCTV.

7.3.3 Damage has occurred to a part of the building or its facilities covered by the CCTV system. This does not apply to trivial damage or misuse such as littering.

7.4 This footage must be viewed in a secure setting and is only for the purpose of establishing if we may have relevant coverage of an incident.

7.5 Footage may only be downloaded and disclosed to law enforcement agencies by a member of the Leadership Team, usually the Housing Manager. It is not a given that a request from the police must be complied with at all times.

7.6 Disclosure will be actioned following a formal written request from the relevant law enforcement agency, stating the specific date, time and location of the CCTV coverage sought and the legal powers being relied upon (e.g. Article 6 of the UK Data Protection Regulations of Section 10 of the Data Protection Act 2018). The Housing Manager, in consultation with the Data Controller will consider the reasonableness and proportionality of such a request before proceeding. In the event that a warrant or court order is provided, then the request will be complied with on this basis.

7.7 Where a disclosure is compelled by warrant or court order, or approved based on a specific written request, it will usually be the Housing Manager who downloads the coverage. In the absence of the Housing Manager the Data Controller will delegate this to another member of the Leadership Team. This data will be transferred securely to the law enforcement officer responsible for the disclosure request.

7.8 Details of the coverage disclosed, to whom and for what purpose will be recorded on the central log (Appendix B) by the member of the Leadership Team who has carried out this process, usually the Housing Manager.

7.9 An anonymised report of any CCTV coverage disclosures and refusals will be covered in the Housing Manager's quarterly report to the Trustees. This will state the date of the incident being investigated and the scheme where this has occurred, but not the details of the incident being investigated or any individual residents involved.

7.10 An annual review of the effectiveness of our current CCTV systems and any proposed amendments will be carried out by the Housing Manager and Data Controller, taking into account any access requests recorded in the preceding year. Any recommendations for new or improved systems which arise will be assessed using the Data Protection Impact Assessment contained at Appendix A.

8. Use of CCTV Cameras by Residents

8.1 If a resident wishes to use any form of CCTV system in or around their own flat, we will consider the following factors:

8.1.1 The installation of any fixtures or fittings for a CCTV system requires the written permission of Harrison Housing. The resident concerned will need to put their request in writing to the Head of Operations, setting out where they wish to put any camera, and the purpose for doing so.

8.1.2 We will not unreasonably withhold permission.

8.1.3 Where permission is sought to install a CCTV camera inside the property, this will usually be permitted so long is this is done by a competent qualified person, does not interfere dangerously with the electricity supply to the flat, and does not have any camera coverage of communal areas outside the flat. The resident will be expected to put up a notice at their front door to alert anyone entering the flat that they may be on CCTV.

8.1.4 Where a resident seeks permission to put up a video enabled doorbell, permission will only be given if this can be located in such a way as not to interfere with the privacy of other residents. The doorbell would have to be positioned so as only to cover the immediate front door area and not any communal spaces where other residents may legitimately be going about their lawful business.

8.1.5 We will not usually give permission to mount CCTV cameras, other than a small video enabled doorbell, on the outside of any dwelling.

8.1.6 Any CCTV system installed by a resident, will be their responsibility to maintain, and any damage caused to walls or decorations by such fixtures will be that resident's responsibility to make good.

8.2 Permission may be withdrawn if a CCTV system is found to have breached any of the principles set out above.

9. Equality, Diversity, and Inclusion

9.1 For Harrison Housing, diversity is about respecting people's individual differences and ensuring that all people that come into contact with us have access to the same high standards of behaviour and service.

9.2 We are committed to ensuring that no resident or team member will be treated less favourably because of their protected characteristics.

Appendix A - *DPIA template*

This template should be used record your DPIA process and outcome. It follows the process set out in the DPIA guidance of the Information Commissioner's Office (ICO), and should be read alongside that guidance.

You should start to fill out the template at the start of any major project involving the use of CCTV, or if you are making a significant change to an existing CCTV system. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for new or amended CCTV systems.

Step 2: Describe the processing

Describe the nature of the processing: how and where will you collect, use, store and delete CCTV images? Will you be sharing data with anyone? What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the CCTV coverage, and will it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Example: CCTV camera will cover an area which includes individual from doors	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Example: Individual properties covered	Relocate cameras Blur or mask front door areas in any remaining coverage	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix B – Record of CCTV access requests

Scheme		Year			
Date of request:	**Reason for request (include details of any police officers making a request for access):**	**Accessed by:**	**Viewed only or downloaded?**	**Approved by Housing Manager or Data Controller?**	**Date approved**

Reviewed by Data Controller: _____ (name and signature)

Date: