FAIRER WESTMINSTER

City of Westminster

Appendix B

# Housing Estates CCTV Cameras




## CCTV POLICY
2025

**This appendix is to be read in conjunction with Westminster City Council's overall policy and will outline the additional considerations and policies that would apply specifically to cameras operated by Westminster Housing Services (WHS).**

WHS manages CCTV systems located across the housing stock. In 2024 WHS conducted a comprehensive audit of all its CCTV systems to ensure that their deployment aligns with the Council's strategic objectives. WHS is reviewing its options to upgrade its CCTV systems in the light of the findings of this audit. This document explains how the current service is managed. It details the additional purpose, use, management and monitoring of the various CCTV systems that are currently installed and operated by WHS across the housing stock and sets out the policy for new installations.

# 1. Purpose and Objectives

1.1. The key CCTV objectives are set out in the Council's Main CCTV Policy. In addition, the following objectives apply specifically to the operation of CCTV within the Housing Service.

1.2. The Housing Service aims to ensure that all CCTV systems are operated fairly, proportionately and in full compliance with the law. All staff and contractors who use or access Westminster Housing Services (WHS) CCTV systems must adhere to these principles and relevant data protection legislation.

1.3. CCTV systems managed by WHS are installed to support the effective management and security of the Council's housing estates, properties, and public spaces. The primary purposes of these systems are to:

- Prevent and detect crime and disorder in and around Council housing estates.
- Tackle anti-social behaviour (ASB) by residents, visitors, or third parties.
- Reduce the fear of crime and provide reassurance to residents and visitors.
- Promote public safety for all who live, work, trade, or visit WHS properties.
- Monitor and ensure the proper use of WHS amenities and communal areas.
- Support enforcement activity, including addressing tenancy/lease breaches and other appropriate legal or regulatory action.
- Ensure effective oversight of WHS contractors and service delivery, providing value to residents.

# 2. New Systems Installation Policy

2.1. In accordance with (1.3) Main Policy - CCTV is a limited resource and is deployed only in circumstances where it is deemed appropriate and necessary to achieve the objectives outlined in this policy. CCTV is primarily a deterrent and part of a broader set of tools used to address crime, anti-social behaviour and public safety concerns. It is not intended to continuously monitor individuals or specific communities.

2.2. Accordingly, it is the policy of Westminster Housing Services (WHS) to ensure that new CCTV systems are only installed in appropriate circumstances where there is evidence that it can assist with the overall management of its public and communal spaces
on its estates and properties.

2.3. When considering any new proposal for CCTV the service will first look at less intrusive options for the identified purpose before committing to any new investment. This is because the service must carefully consider any option to install CCTV alongside its broader toolbox of measures that may be deployed to manage its stock. CCTV is part of a broader suite of measures employed by the service to enhance safety and manage its public spaces in and around its housing stock.

2.4. The service requires that any new installation meets a rigorous "test of appropriateness" TOA, with confirmed funding.

2.5. Any new installation must be approved by the CCTV Governance Group.

# 3. Test of Appropriateness

It is WHS's policy that every camera it installs meets an agreed Test of Appropriateness. This test requires:

• That CCTV cameras are deployed only when there is evidence of an identified pressing need in that location and the use of CCTV is the most effective and appropriate intervention to meet that need. This is in line with the Surveillance Camera Commissioner's Code of Practice, Guiding Principles 1-12 and the UKGDPR principles.

• That final decisions are made by the CCTV Governance Group.

• In urgent cases (risk to harm/life) verbal agreement can be given by a director or nominated deputy.

# 4. Cameras and operational coverage

4.1. All new cameras from the date of this policy will be capable of digital privacy masking to ensure that no collateral intrusion occurs.

4.2. The positions of the cameras are determined during the planning stage of any new installation and must be based on the specific defined operational requirement for that camera (e.g. an internal static camera facing entrance to a block is designed to capture the ID of anyone entering the building and therefore should be capable of meeting this requirement). These positions may only be altered by an officer authorised by the System Manager.

4.3. There are various live-view monitoring points across WHS which include Concierge's offices/positions, housing offices, and other locations identified for that purpose. Only authorised staff, specifically delegated by the System Manager, will carry out monitoring operations using CCTV. The live-view monitoring points are only situated in secure office locations and only accessible by authorised staff.

4.4. The CCTV systems are checked and maintained on a periodic basis as part of planned preventative maintenance (PPM) and reactive repairs carried to ensure it is working effectively and remain fit for purpose in accordance with our obligation under Security Cameras Code of Practice.

4.5. All footage requests must be made within the first 25 days to allow for at least five working days for WHS to secure any possible footage. This is to consider any technical requirements to confirm the appropriateness and availability of the data. Exceptions will be considered on a case-by-case basis.

4.6. The showing of recorded CCTV material to members of the public is prohibited except where permitted by law and the overall Policy. In limited circumstances, still images may be shared publicly to help identify unknown offenders or support community safety, following a documented risk assessment and approval by the relevant Council officer in consultation with the Corporate Data Protection Team or the Police. Demonstrations of the CCTV system for residents or partner groups may also be carried out for educational or engagement purposes, provided no personal or identifiable data is shown.

4.7. Under specific circumstances, for example, where a serious event may trigger the requirement for police to manage a potential public order incident, the police may make a request to take control of part of the System to facilitate live monitoring. Any member of the police accessing the System must comply with the Data Protection Legislation and the principles set out in this Policy. Only requests made on the written authority of a police officer, of minimum rank of Inspector, will be considered for this purpose. Any such request will be considered by the Governance Group. There may be occasions where a verbal request will be accepted due to the circumstances of the incident.

# 5. Third Party Data Requests

5.1. An individual who believes that their personal data (that is their identifiable image) has been recorded by the System has the right to make a subject access request for that data only, this may result in the redaction of footage in all other elements of the scene.

5.2. Once a request has been made to the Data Controller, the Systems Manager will be instructed to immediately set aside the relevant Recorded Material from the 30-day rotation system and label it accordingly.

5.3. The Council follows the corporate procedure for handling subject access requests. This includes applicants providing verification proof to confirm entitlement. The Council reserves the right to reject a request where this requirement has not been met. Where appropriate exemptions will be applied to requests for a number of reasons, for example if it would prejudice an investigation.

5.4. Under data protection legislation other DP rights are also managed by the corporate Data Protection Team.

5.5. The Data Controller can also refuse a request for access if searching for the information would require disproportionate effort or if the request is considered vexatious. Any such exemptions shall be considered on a case-by-case basis.

5.6. All requests relating to Legal Proceedings and Insurance (Schedule 2, Part 1, Paragraph 5) must be managed through the Council's Information Management Team. Each request will be assessed on a case-by-case basis to ensure compliance with applicable law.

# 6. Roles and responsibilities

The Data Controller of the WHS Systems is Westminster City Council
64 Victoria Street, London SW1E 6QP.