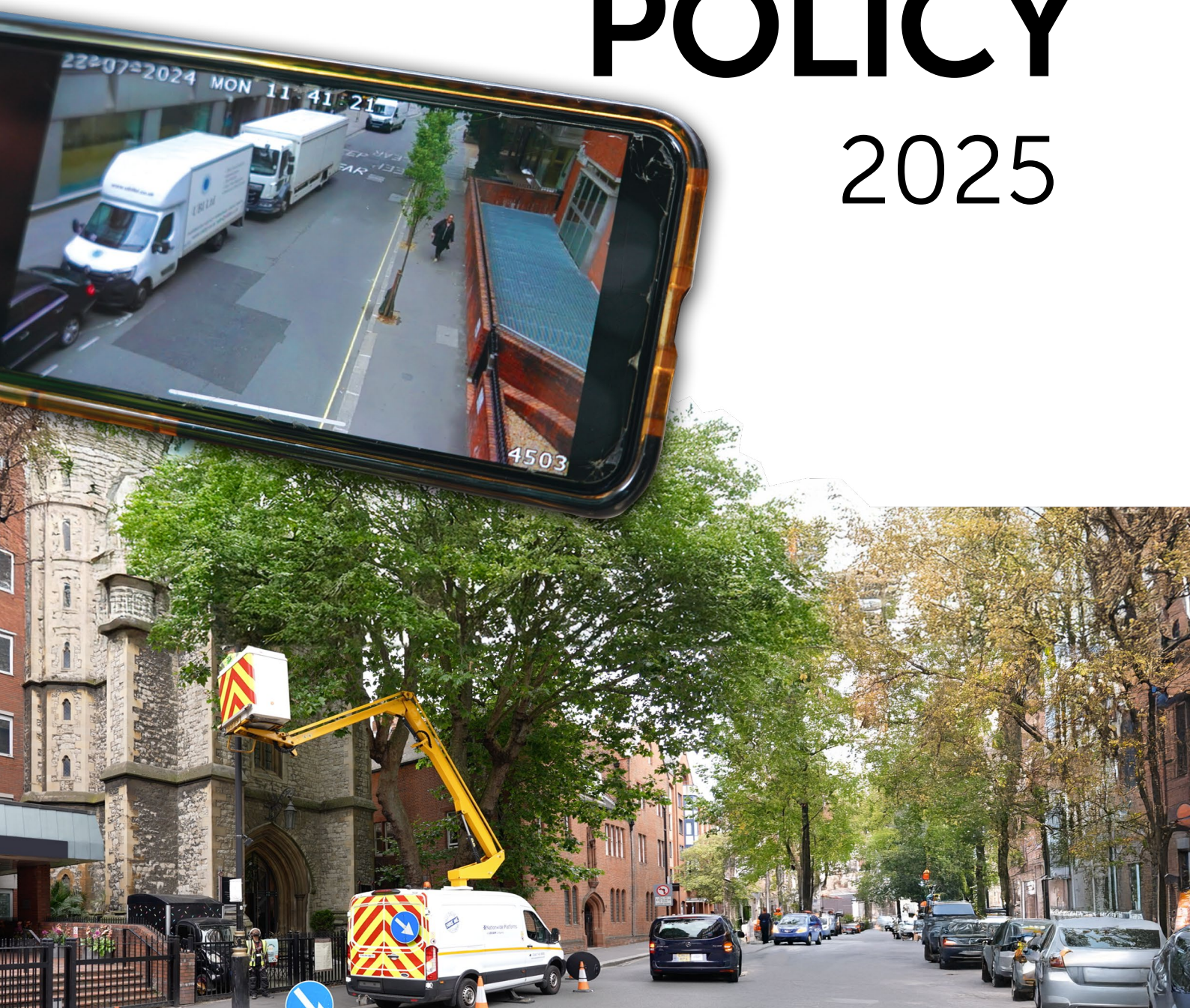
FAIRER WESTMINSTER

City of Westminster

CCTV POLICY 2025



Content

1. Introduction and Key Objectives	3
2. Scope	4
3. Statement of Purpose and Principles	4
4. Legislation and Regulations	5
5. Terms and definitions	6
6. Data Protection and Privacy	7
7. Recording, Retention, and Disposal of Images	7
8. System Monitoring and Maintenance	8
9. Signage and Public Awareness	8
10. Evaluation	9
11. Commissioner: Code of Practice Legislation	9
12. Contact Details Summary Sheet	11
Appendix A – Public Realm	
Appendix B - Housing	
Appendix C – Traffic Enforcement Cameras	



1. Introduction and Key Objectives

1.1. The Council acknowledges the role of Closed-Circuit Television (CCTV) in promoting public safety, preventing crime, detect motoring offences and safeguarding assets. CCTV systems, when deployed appropriately, can assist in deterring crime, addressing anti-social behaviour, protecting assets, and promoting the safety and well-being of residents, visitors, and Council staff. This policy outlines the Council's framework for the responsible deployment of CCTV, ensuring a balance between the benefits of surveillance and individuals' privacy rights.

1.2. The primary objectives of CCTV systems used by the Council are as follows:

• Enhance Public Safety - Use CCTV to help manage and monitor public spaces to enhance public safety as well as enforce moving traffic regulations, ensuring safe public space and road use.

• Help deter and detect crime and anti-social behaviour – Use CCTV to act as a deterrent and to assist in investigations of criminal activity and anti-social behaviour.

• Protect Council Assets - Use CCTV to help manage Council-owned properties, assets, and facilities from theft, vandalism, and unauthorised access and use.

• Support Wider Strategic Objectives - Where appropriate, responsibly use anonymised metadata generated by CCTV systems, including those with AI-powered analytics, to support the Council's broader objectives such as town centre planning, partnership working, and initiatives that enhance local economic growth. All such data will be anonymised and handled in compliance with data protection principles.

1.3. The Council recognises that 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 for ongoing monitoring of individuals or groups. The use of cameras to undertake covert surveillance will only happen when the law permits.

2. Scope

2.1. This policy applies to all types of surveillance systems deployed by the Council across multiple settings, including but not limited to:

• Public Realm: CCTV in public areas (owned by the Council) such as town centres, and streets, aimed at enhancing public safety, deterring crime, anti-social behaviour, environmental crime and protecting Council assets.

• Housing: Surveillance in and around council-owned housing stock's communal areas, to help with prevention of anti-social behaviour and crime.

• Moving Traffic Enforcement: CCTV is primarily used to monitor and enforce moving traffic regulations, with limited enforcement of static parking contraventions, such as bus stops, School Streets (Pedestrian and Cycle Zones) and school keep-clear markings, ensuring safe road use in compliance with legislation., ensuring safe road use in compliance with legislation.

2.2. This policy does not apply to any other private CCTV systems, such as those operated by private organisations or individuals or CCTV systems used by Metropolitan Police Service (MPS). This includes "Ring Doorbells" and similar installations fitted by homeowners. In such situations homeowners are expected to comply with local policies where applicable, and with the Data Protection Act 2018.

3. Statement of Purpose and Principles

3.1.The purpose of this policy is to give clear guidelines on the Council's use of CCTV and how the systems can be accessed by partner agencies and the public, in line with legislative provisions and guidance. This policy outlines the Council's approach to the following:

• the installation and removal of any CCTV systems.

• the management of existing systems and other surveillance tools.

• the specific use and management of CCTV systems on housing estates, ensuring alignment with Council housing policies and legal provisions.

• the specific use and management of traffic enforcement cameras used by the Council ensuring adherence with relevant legislation.

3.2. The three objectives of this policy are as follows:

A. To outline the responsibilities of those involved in the Council's CCTV system.

B. To state the purposes for which the CCTV system was installed and should be used.

C. To set out the process of how the systems can be accessed by partners and the public, and of how images can be obtained.

4. Legislation and regulations

4.1. In addition to Council policies and procedures, the operation of CCTV systems is subject to legislation under:

- The UK GDPR and Data Protection Act 2018 ("DPA 2018")
- The Human Rights Act 1998 ("HRA 1998")
- The Freedom of Information Act 2000 ("FOIA)
- The Regulation of Investigatory Powers Act 2000 ("RIPA 2000")
- The Protection of Freedoms Act 2012 ("PoFA 2012")
- Criminal Procedures and Investigations Act 1996 ("CPIA 1996)
- Criminal Justice and Public Order Act 1994 ("CJPO 1994")
- Equalities Act 2010 ("EA 2010)

4.2. The Human Rights Act 1998 gives effect in the UK to the rights set out in the European Convention on Human Rights (ECHR) Article 8 provides for a person's right to respect for their private and family life, home and correspondence, and is one of the qualified rights within the Act. Surveillance that may interfere with such a right should only be carried out where it is necessary and proportionate and lawful to do so.

4.3. The purpose of this policy is to ensure that the above legislation is always complied with when operating CCTV, and to ensure compliance with the codes of practice as outlined below.

4.4. The Council acknowledges the UK Government's concerns regarding surveillance technologies manufactured by companies owned or influenced by foreign government. The Council is aware that legacy surveillance systems, including installations within Housing and Corporate sites, may contain devices from these manufacturers and are recognised as requiring enhanced security oversights. To address these concerns, the Council has conducted a comprehensive audit of its CCTV infrastructure, with the findings informing future procurement and deployment strategies.

4.5. The Council is committed to reviewing existing systems on a regular basis, prioritising replacements to align with national security standards and ensuring all new CCTV systems comply with government recommendations.

5. Terms and definitions

CCTV: means Closed Circuit Television. It means dedicated fixed and re-deployable cameras designed to capture and record images of individuals and property.

Council: means Westminster City Council

We: means Westminster City Council

Data: Information which is stored electronically. In respect of CCTV, this generally means video images. It may also include static pictures such as screen shots.

Data subjects: means all living individuals about whom the Council hold personal information because of the operation of our CCTV (or other surveillance camera systems). This includes employees, councillors, contractors or members of the public.

Personal data: means data relating to a living individual who can be identified from that data (or other data in our possession). This includes video images of identifiable individuals and vehicles.

Data controllers: The people who, or organisations which, determine the manner in which any personal data is processed.

Data users: Those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV, cameras and other surveillance camera systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy

Data processors: means any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier who handles our data on our behalf).

Processing: is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, or destroying it. Processing also includes transferring personal data to third parties.

Surveillance camera systems: Any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

Data Protection Impact Assessment [DPIA]: is a process to systematically and comprehensively analyse any processing, and help identify and minimise data protection risks. A DPIA must describe the nature, scope, context, and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks. A DPIA may cover a single processing operation or a group of similar processing operations. A DPIA is an ongoing process that is subject to regular review. The Surveillance Camera Commissioner's DPIA will be used for all installations.

6. Data Protection and Privacy

6.1. The Council is committed to respecting individuals' privacy rights in accordance with the Data Protection Act 2018 (DPA), UK GDPR, and Article 8 of the European Convention on Human Rights. All activities will be conducted in a manner that ensures the least intrusion necessary to achieve the stated purpose.

6.2. A DPIA must be undertaken to cover all surveillance system deployments, depending on service's requirement or significant changes to existing systems. The DPIA will evaluate the necessity, proportionality, and potential privacy risks of the system and outline appropriate mitigation measures. A copy of completed DPIAs will be maintained and reviewed annually.

6.3. Access to recorded data will be strictly controlled and limited to authorised personnel. The Council will implement safeguards to prevent unauthorised access or misuse of data. Appendices related to specific Council services will include further details about data access protocols for those services.

6.4. Each appendix will specify the data protection and privacy practices unique to the specific service area, including DPIA processes and privacy impact considerations.

7. Recording, Retention, and Disposal of Images

7.1. CCTV images and recordings will be collected and used solely for the purposes stated in this policy. Data will not be repurposed without appropriate justification, assessment and consultation.

7.2. Data retention periods will align with the stated purposes of the surveillance system. Standard retention will not exceed 30 days unless required for ongoing investigations or legal proceedings. Retention periods for specific service areas will be detailed in each relevant appendix.

7.3. When no longer required, data will be securely deleted, over-written or destroyed in line with Council's data disposal procedures.

7.4. Appendices will detail retention schedules and disposal protocols specific to each service area, considering operational requirements and legal obligations.

8. System Monitoring and Maintenance

8.1. All surveillance systems will be reviewed and maintained to ensure they operate effectively and meet the intended purposes. Monitoring will include regular reviews of system performance, image quality, and compliance with this policy.

8.2. Systems will undergo routine maintenance to ensure reliability and security. Maintenance schedules will be documented, and any system faults will be logged and resolved promptly.

8.3. All systems will meet or exceed relevant technical standards for surveillance systems, including those related to cybersecurity and physical security.

8.4. Each appendix will specify the monitoring and maintenance protocols applicable to the unique requirements of each service area, including any advanced or specialised surveillance technologies.

9. Signage and Public Awareness

9.1.The Council will ensure that all surveillance systems are operated transparently. Signage will be placed in areas under surveillance to inform the public of the presence and purpose of surveillance systems.

9.2.Signage, depending on the service, must include:
- A statement indicating that CCTV is in operation.
- The purpose of the surveillance.
- Contact details for further information or to lodge complaints i.e. the owner of the system.

9.3. For Moving Traffic Enforcement will display the legend 'City of Westminster' accompanied by a standard traffic enforcement symbol (box brownie). There is no requirement to include contact information on the signage itself, as all relevant details are provided within the associated documentation, including Postal Penalty Charge Notice (PCN), Notice to Owner (NtO), and other official literature.

9.4. Information about the Council's CCTV policy, including this document and associated appendices, will be made publicly accessible through the Council's website and other appropriate channels.

9.5. Appendices will outline specific signage and public awareness practices for unique service areas, such as bespoke communication strategies for sensitive locations or high-privacy settings.

10. Evaluation

10.1. The council will regularly evaluate the effectiveness of its CCTV systems to ensure they meet the objectives stated above.

10.2. Evaluation metrics will include, but will not be limited to:

- Changes in crime and anti-social behaviour rates in monitored areas.
- The effectiveness of systems in resolving incidents and addressing environmental issues.
- Public perceptions of safety, assessed through mechanisms such as the annual City Survey.
- Compliance with moving traffic regulations such as improved road safety, reduced congestion and decreased pollution levels.

10.3. Where feasible, cost-benefit analyses will be conducted to evaluate the return on investment and prioritise areas with the greatest need.

10.4. Any minor reviews or changes to the policy or the appendices are subject to approval by the relevant service director. If the review process identifies a need for substantial amendments, these recommendations will be escalated for consideration by the appropriate Executive Director or Cabinet Member.

10.5. Any incidents involving data breaches will be addressed in accordance with the Council's official Incident Management Procedures.

11. Surveillance Camera Commissioner: Code of Practice Legislation

11.1. Westminster City Council is a relevant authority as defined by The Protection of Freedoms Act 2012 (POFA) and it recognises that it must have regard to the Surveillance Camera Commissioner's Code of Practice when exercising any of the functions to which the code relates. This policy recognises the importance of the 12 guiding principles of the Code (outlined below). All employees and contractors must adhere to these principles in conjunction with the lawful operation of all CCTV systems used by the Council. The following principles are designed to provide a framework for operators and users of surveillance camera systems so that there are proportionality and transparency in the Council's use of surveillance.

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be securely deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

12. Contact Summary Sheet

Service Area	Contact
Housing	The Director of Housing, Westminster City Council, 64 Victoria Street, London SW1E 6QP. housing.enquiries@westminster.gov.uk Queries or concerns around the processing of personal data by our CCTV systems, will be managed through the WCC Information Management Team. dataprotection@westminster.gov.uk
Public Realm	Operational queries or concerns and requests for footage and exercising of above rights will be managed through the LBHF VSS. vssinfo@lbhf.gov.uk Queries or concerns around the processing of personal data by our CCTV systems, will be managed through the WCC Information Management Team. dataprotection@westminster.gov.uk
Traffic Enforcement Cameras	For Parking Services parkingservices@westminster.gov.uk Queries or concerns around the processing of personal data by our CCTV systems, will be managed through the WCC Information Management Team. dpo@westminster.gov.uk