

CCTV Operations, Privacy & Data Protection Policy

Community CCTV network | Public policy | Approved version

Document control	Value
Reference	USCN-POL-001
Version	1.0 - approved
Classification	Public
Policy owner	Data Protection Officer (DPO)
DPO	Bertram Scanlon
Approving authority	Managing Director
Approval date	19 October 2026
Effective date	On publication (date not yet recorded)
Review cycle	Following significant operational, technical, legal or privacy changes
Related status register	USCN-REG-001 - Compliance & Implementation Status Register (proposed reference)

Document status. This policy was approved by the Managing Director on 19 October 2026 without conditions. Version 1.0 is approved for publication. It takes effect on actual publication; the publication date has not yet been confirmed. Approval of this policy does not authorise any individual CCTV camera to record. The company registration number should be added only after verification.

1. Purpose and scope

1.1 This policy governs the community CCTV network operated by UK Safety Camera Network Ltd (USCN). It does not govern separate commercial CCTV installation services, customer-owned CCTV systems or future specialist programmes unless expressly brought within its scope.

1.2 Its objectives are lawful and proportionate CCTV operation; transparent processing of personal data; protection of individuals' rights; appropriate evidence handling; and accountable oversight of cameras installed on host premises or elsewhere.

1.3 At the date the operational information for this policy was supplied, the first community camera had not been physically installed and no community CCTV camera was recording. Statements of operational requirements describe the controls to be in place before activation, not proof that a live network is already operating.

2. Governance and accountability

2.1 USCN owns the community CCTV cameras and determines the purposes and means of the associated personal data processing. USCN is the data controller. A host does not become a controller merely by supplying a mounting location, power or internet connection.

2.2 The DPO, Bertram Scanlon, oversees data protection assessments, commissioning authorisation, access and disclosure decisions, preservation extensions, complaints, incidents and relevant records. The Managing Director approves this policy. Any actual or potential conflict affecting the DPO's independence must be assessed and managed under applicable law.

2.3 USCN maintains internal accountability records and a separate public Compliance & Implementation Status Register, proposed reference USCN-REG-001. The DPO maintains and authorises material status updates to that register. The register is intended to identify whether supporting work is proposed, drafting, under review, approved, implemented, suspended or superseded.

2.4 The register does not replace this policy, a lawful basis, or a required assessment. Material changes to the substance or factual accuracy of this policy require a policy revision.

3. Purposes and necessity

3.1 Community cameras may be deployed for crime prevention and deterrence, detection and evidential support, public safety, reduction of antisocial behaviour, protection of property, and support for emergency incidents, insofar as justified for each deployment.

3.2 USCN will document necessity and proportionality for each camera, considering the location, expected public benefit, alternative measures, the extent of personal data captured, and risks to people who may be recorded.

4. Lawful basis and impact assessments

4.1 Legitimate interests under Article 6(1)(f) UK GDPR is the proposed lawful basis for ordinary community CCTV processing. The overarching assessment, USCN-LIA-001 version 1.0, was approved by the DPO on 19 October 2026 as a framework and statement of principles only. It does not establish that legitimate interests is satisfied for any particular camera. A documented camera-specific balancing decision is required before deployment; additional installation-specific assessment is undertaken where necessary.

4.2 The DPO must approve the applicable lawful basis assessment. Processing must not be authorised in a proposed form if the assessment does not establish an adequate lawful basis, unless the concerns are resolved or another valid lawful basis is established.

4.3 A camera-specific Data Protection Impact Assessment (DPIA) is required before activation and when significant changes arise. The first camera DPIA has been completed and documented; its formal approval status is not separately confirmed in this draft. Completion of a DPIA does not itself establish a lawful basis.

4.4 The DPO must authorise commissioning only after the required lawful basis and DPIA work, camera positioning and masking review, security and recording checks, signage and signed host agreement are satisfactorily addressed. Serious privacy concerns may require suspension or withholding of recording.

5. Camera locations and field of view

5.1 Cameras may observe public streets, pavements, publicly accessible parking and other public spaces, frequently from privately owned host properties. A location does not automatically justify unrestricted surveillance.

5.2 USCN approves camera positioning and direction. Field of view and privacy masking are assessed case by case at installation and whenever circumstances change. Unnecessary capture of private spaces or unrelated activity should be reduced through positioning, masking and configuration.

5.3 Locations involving children or vulnerable people are considered within each camera DPIA, including necessity, proportionality, positioning, masking and alternative deployment options. Incidental capture of children does not remove their UK GDPR protections.

6. Recording and analytics

6.1 The community network uses motion-triggered video recording. Audio recording is disabled. Basic object classification may distinguish broad categories such as a person, vehicle or animal for motion-based recording decisions.

6.2 The community network does not use facial recognition, biometric identification, automatic number plate recognition (ANPR), or automated tracking of individuals between cameras. Object classification must not be represented as identification of a particular person or vehicle.

6.3 Only functions necessary for the documented monitoring purpose may be enabled. Any proposed new analytical capability requires a documented privacy assessment and DPO approval before activation. A distinct future programme involving ANPR or other identification technology would require its own legal and governance review and is not authorised by this policy.

7. Live viewing and transparency

7.1 Public live viewing is disabled until further notice. Authorised USCN personnel may use restricted live access for legitimate operational purposes.

7.2 Any proposal to introduce public live viewing requires a separate, documented assessment of lawful basis, necessity, proportionality, privacy impact and safeguards, with DPO approval before activation. The separate balancing assessment is in progress and is intended to be published when appropriate.

7.3 Appropriate CCTV signage must be provided for each camera or monitored area, stating essential information and directing individuals to fuller privacy information online. USCN and the host share practical signage responsibilities as set out in the host agreement.

8. Retention, preservation and deletion

8.1 Recordings are stored locally on each camera, normally for 31 days, and are automatically deleted or overwritten at the end of that period unless a justified preservation hold applies.

8.2 The DPO authorises preservation beyond the normal period where needed for an investigation, dispute, rights request or other justified purpose. Preservation records identify the footage, reason, authoriser, dates, review and deletion outcome. Holds are reviewed when their justification changes or ends.

8.3 When preservation is no longer justified, the relevant material must be securely deleted unless another lawful basis requires continued retention. Before decommissioning, transfer or disposal of a camera, recordings and credentials must be securely erased or otherwise protected.

8.4 Ancillary service records have separate retention schedules. Where applicable, telephone call recordings are normally retained for eight months, subject to justified extensions; this is not the retention period for CCTV footage.

9. Access controls and confidentiality

9.1 Only designated USCN personnel formally authorised by the DPO may access CCTV footage. Access must be limited to legitimate duties and recorded in access logs. Camera hosts have no automatic entitlement to live or recorded footage; exceptional access requires separate assessment.

9.2 Personnel must receive relevant privacy, security and footage-handling training before access is granted and must be subject to written confidentiality obligations. Access permissions are reviewed when responsibilities change or relevant security concerns arise and are promptly withdrawn when no longer required.

9.3 Local recordings are encrypted at rest. Remote access is secured and restricted, individual credentials are used, and firmware/security updates are applied as needed in response to maintenance requirements and identified vulnerabilities.

10. Footage requests, disclosures and evidence

10.1 Requests from police, other authorities, hosts and third parties are assessed individually. The DPO authorises external disclosures after considering the requester, purpose, legal justification, necessity, proportionality and rights of other people captured.

10.2 Disclosure records must identify the requester, legal justification, footage, recipient, date and authoriser. Secure transfer arrangements are selected according to the circumstances. No request creates an automatic entitlement to footage.

10.3 Camera clocks are automatically synchronised with a reliable time source. Where necessary, original recordings are preserved and working copies used for review or disclosure. Exports are logged with camera, date, person and reason; recordings are checked for apparent completeness and integrity before disclosure.

10.4 Transfers and custody of evidential footage are documented. This policy does not claim that cryptographic hashing is routinely used as an integrity check.

11. Individual rights and complaints

11.1 Individuals may exercise applicable UK GDPR rights and submit privacy enquiries through the designated email, online form, data protection telephone contact or another appropriate channel published by USCN. The DPO oversees responses.

11.2 USCN will verify identity where reasonably necessary, assess the rights and privacy of others, and apply redaction or other appropriate safeguards where disclosure could affect third parties. Requests will normally be answered within one calendar month, subject to applicable legal extensions and exceptions.

11.3 Privacy complaints may be made by email, online form or telephone. USCN aims to acknowledge complaints within seven working days and will investigate issues such as positioning and masking individually. Internal escalation is available, but individuals may contact the Information Commissioner's Office (ICO) directly without first exhausting USCN procedures.

12. Incidents and personal data breaches

12.1 Personnel and hosts must report suspected privacy or security incidents promptly to the DPO. Hosts must report camera theft or loss within 24 hours of becoming aware of it and report other damage or security concerns promptly.

12.2 All suspected breaches, including those not requiring regulatory notification, must be documented. The DPO assesses risk and any duty to notify the ICO, normally within 72 hours of awareness where the statutory threshold is met, and affected individuals where a high risk arises.

12.3 A formal written incident response procedure is being developed; its status will be reflected accurately in the Compliance & Implementation Status Register.

13. Community hosting and maintenance

13.1 A signed host agreement must be in place before activation. Hosts provide electricity and internet connectivity, allow agreed reasonable access for installation, maintenance and removal, cooperate with signage, and notify USCN of relevant property changes.

13.2 Hosts must not reposition, tamper with, disconnect or change settings without USCN approval, except where necessary for safety or other compelling circumstances. Hosts should take reasonable steps to maintain power and connectivity and, where reasonably practicable, give at least a few hours' notice before planned router changes, internet maintenance or power disconnection.

13.3 Faults may be identified through host reports, scheduled maintenance and authorised checks. USCN prioritises remedial work by severity, risk and available resources. Internet interruption does not necessarily stop local recording where power and storage remain functional; remote access may require reconfiguration after router changes.

13.4 Host arrangements terminate in accordance with the signed agreement. USCN retains responsibility for camera configuration, access permissions, recordings and appropriate decommissioning safeguards.

14. Service providers and international transfers

14.1 USCN may use external providers for websites, communications, online forms, customer/issue management, chat and telephony. Providers previously identified for review include HubSpot, tawk.to, FreeCX (service name to be verified), VoIPline Telecom UK, Google/Gmail and Microsoft services. Their inclusion does not imply that each processes CCTV footage.

14.2 Data processing agreements and relevant international data transfer arrangements have not yet been fully assessed or verified. USCN must complete the applicable supplier and transfer reviews before relying on arrangements requiring them; current progress is tracked through the status register.

15. Records, publication and review

15.1 USCN maintains, as applicable, camera-specific DPIAs, lawful basis assessments, records of processing activities, access/export logs, disclosure and preservation records, breach and incident records, and privacy complaints and outcomes.

15.2 USCN intends to publish this policy, applicable privacy notices and contact information, the separate public live-viewing assessment when appropriate, and non-sensitive DPIA summaries where suitable. Full DPIAs and sensitive operational/security records remain internal unless disclosure is otherwise appropriate or legally required.

15.3 Supporting assessment and implementation statuses are published separately in USCN-REG-001. The register is updated whenever a material status changes under DPO oversight. Its status labels must not be interpreted as authorisation for processing unless the relevant legal and operational approvals are complete.

15.4 The Managing Director approves this policy. It takes effect on publication after approval and is reviewed following significant operational, technical, legal or privacy changes. Revised versions must identify their version and approval/publication details.

16. Pre-activation conditions

16.1 Before any community CCTV camera begins recording, USCN must confirm an adequate lawful basis and approved relevant assessment(s), the camera-specific DPIA and DPO commissioning decision, suitable signage, signed host agreement, appropriate security configuration, access and training controls, and retention/deletion arrangements.

16.2 Approval of USCN-LIA-001 covers overarching principles only; camera-specific balancing conclusions and other outstanding implementation work must not be concealed by referring to the status register. No live recording is authorised merely because this policy or the overarching LIA has been approved or published.

17. Related documents and version history

17.1 Related documents include USCN-REG-001 (Compliance & Implementation Status Register), camera-specific DPIAs, USCN-LIA-001 (DPO-approved overarching framework) and any installation-specific LIAs, privacy notices, host agreements, and future specialist policies covering footage handling, technical safeguards, transparency, public live viewing and camera deployment.

Version	Status / change
0.1	Initial draft prepared from confirmed USCN operating requirements; pending formal approval.
1.0	Approved by Managing Director on 19 October 2026 without conditions; updated LIA status and pre-activation wording.

Approval record

Approving authority	Approval date	Publication / effective date
Managing Director	19 October 2026	On publication - date pending