

Community CCTV

Legitimate Interests Assessment

Document reference: USCN-LIA-001 | Version: 1.0 | DPO approval: 19 October 2026

Document control	Recorded position
Controller	UK Safety Camera Network Ltd (USCN)
Assessment scope	USCN-owned community CCTV network, including cameras hosted on third-party premises
Proposed Article 6 lawful basis	UK GDPR Article 6(1)(f): legitimate interests
DPO approval scope	Overarching LIA framework and principles only
Camera-specific decisions	Not approved by this document; individual balancing assessments and approved DPIAs required
Implementation status	No community CCTV cameras installed or recording at the time the assessment information was supplied
Public availability	Publish complete overarching LIA with necessary security redactions
Approval authority	Data Protection Officer; approved document provided to Managing Director

Approval limitation. DPO approval of this framework does not establish that Article 6(1)(f) is satisfied for every camera or location. No camera may commence personal-data recording solely on the strength of this overarching document. Each proposed deployment requires evidence, a site-specific balancing outcome, approved DPIA and completed commissioning checks.

1. Assessment status and decision

The DPO has approved the overarching legitimate interests assessment framework and principles on 19 October 2026, as confirmed by USCN. This approval is not a blanket determination that all proposed installations pass the purpose, necessity and balancing tests. The outcome for each individual camera remains outstanding until the relevant location-specific evidence has been reviewed and the DPO has recorded a decision.

The permitted camera-specific outcomes are: approved, approved subject to conditions, or not approved. Conditions necessary for lawful processing must be satisfied before activation. Where significant residual risks remain, the DPO must decide whether the proposed processing can be lawfully redesigned or mitigated; processing must not proceed without a defensible lawful basis and required safeguards.

2. Controller, processing and scope

USCN is the controller and owner of the community CCTV cameras, including cameras installed on privately owned host properties. Hosts provide agreed facilities but do not automatically receive access to recordings or control camera settings. The assessment concerns USCN community CCTV, not commercial CCTV installations or surveillance conducted for hosts' independent private purposes.

Proposed processing consists of motion-triggered video capture in publicly accessible areas such as streets, pavements and car parks. Audio recording is disabled. Footage is stored locally on cameras with encryption at rest, controlled remote access and a routine 31-day retention period, subject to documented and authorised preservation exceptions. Broad object classification may identify people, animals or vehicles. This programme does not use facial recognition, biometric identification, ANPR or cross-camera tracking.

3. Purpose test - legitimate interests

USCN identifies the following interests: preventing and detecting crime; deterring, preventing and investigating antisocial behaviour; promoting public safety and supporting emergency response; preserving and disclosing relevant incident evidence in a controlled manner; and protecting property where connected to an identified community-safety need.

The expected beneficiaries include residents, visitors, businesses, the wider public, relevant police and public-safety agencies, and USCN in pursuing its community-safety mission. CCTV is intended both to deter incidents and to provide evidence after incidents. A general community-safety benefit is insufficient on its own to justify a specific camera.

4. Necessity test - site-specific requirement

Before approving a camera, USCN considers less intrusive responses, including improved lighting, physical security or environmental changes, and community initiatives. Their likely effectiveness and practicality are assessed using available evidence of previous interventions and remaining incidents. A camera is not approved for a purpose if a reasonably effective, less intrusive alternative adequately addresses that need.

Each camera-specific DPIA must record the identified problem, available evidence, alternatives considered, why they are insufficient where applicable, the intended field of view and why the proposed recording is reasonably necessary. Necessity must be reconsidered when relevant circumstances or evidence change.

5. Balancing test - individuals and expectations

Individuals potentially affected include pedestrians, local residents, visitors, children and workers. Although privacy expectations may generally be lower in public areas, public presence does not extinguish privacy rights. The location, activities captured, camera orientation, duration of recording, available alternatives and consequences for affected people must all be considered.

Coverage of potentially sensitive locations is determined individually through the camera-specific DPIA. Unavoidable incidental recording of individuals unrelated to incidents may occur, but must be justified and subject to proportionate access, retention and disclosure controls. Community evidence primarily comes from reports and concerns already received; relevant privacy objections and complaints must also be weighed and are not automatically a veto.

6. Potential adverse impacts

The balancing assessment must consider the nature, likelihood and severity of: recording movements, activities and associations; incidental capture; unauthorised use or disclosure; equipment or data compromise; contextual revelation of sensitive information; chilling effects on lawful activity; and misinterpretation or incorrect inferences from footage.

Severity and likelihood are assessed separately for each proposed camera based on location, field of view, technology and access arrangements. Particular effects on children or vulnerable people must be considered where relevant. Significant residual privacy risks are escalated to the DPO for a recorded case-specific decision. Where a DPIA indicates unmitigated high risk, the requirement for prior consultation with the ICO must be considered.

7. Safeguards and effectiveness

Control	Required approach
Coverage and minimisation	Appropriate positioning, field-of-view restrictions and masking where justified; motion-triggered recording; no audio.
Retention and security	Encrypted local storage; routine 31-day retention with automatic overwrite; documented preservation exceptions; secured remote access.
Personnel access	DPO-authorised trained personnel, confidentiality requirements and appropriate access records; no automatic host access.
Transparency	Appropriate signs near covered areas and accessible privacy information.
Disclosures	Case-specific lawful review, authorisation, secure transfer and evidential handling records.
Analytics restrictions	No facial recognition, ANPR or cross-camera tracking under this programme.
Verification	Relevant safeguards checked at commissioning before recording is authorised.
Failure and residual risk	Safeguard failures referred to DPO; effectiveness and remaining risks documented in each camera-specific DPIA.

These are the safeguards USCN has selected for its framework. Their selection does not prove that any uninstalled camera has been configured or tested. Commissioning evidence must verify the relevant controls before activation.

8. Balancing methodology and decisions

USCN uses a documented qualitative assessment. The DPO considers the strength and evidence of the location-specific public-safety interest, whether recording is necessary, reasonable expectations of individuals, likely adverse effects, available safeguards and remaining risks. Available local evidence informs the expected benefit; neither the existence of crime nor USCN's general mission automatically establishes proportionality.

The camera-specific conclusion must explain why the legitimate interests are not overridden by affected individuals' interests, rights and freedoms, or why approval must be withheld. Relevant complaints and objections must be considered. The DPO formally records the decision, conditions, supporting rationale and date.

9. Purpose limitation and secondary processing

This LIA covers the stated community-safety purposes only. Routine employee monitoring, customer profiling and private host surveillance are excluded. Any materially different purpose requires a prior assessment of purpose compatibility, necessity, lawful basis and privacy implications, together with any necessary approvals.

Public live viewing and public publication of identifiable footage are not authorised by this LIA; each requires separate assessment, legal justification and approval. New technologies or materially different analytics must be assessed and approved before processing begins. Lawful requests for incident footage are reviewed under the applicable access and disclosure controls.

10. Special category and criminal offence data

USCN does not intend to collect or analyse special category data, but incidental capture may arise. Whether Article 9 UK GDPR applies depends on the nature and purpose of the particular processing; the DPO assesses any required additional conditions before that processing. Sensitive locations and restrictions are assessed in individual DPIAs.

Footage or incident records may involve criminal offence information. The DPO must assess Article 10 UK GDPR and applicable Data Protection Act 2018 conditions where required. Article 6(1)(f) alone does not dispense with additional legal requirements. Where concerns remain unresolved, relevant processing must be restricted, redesigned or suspended pending assessment.

11. Review and ongoing necessity

USCN reviews this framework or associated camera assessments when material changes or new evidence arise, without a fixed annual review interval. Selected triggers include the availability or effectiveness of less intrusive alternatives, technological changes, significant complaints and legal or regulatory developments. Material new evidence affecting necessity or privacy must also be considered, even if not within a listed trigger.

Continued justification may be evaluated using available incident trends, camera usefulness and effectiveness of alternatives, without attributing changes in crime automatically to CCTV. Where a camera is no longer necessary or proportionate, USCN may reposition it, reduce coverage, suspend recording or remove it. Location-specific findings are recorded in the DPIA or linked review record; the overarching LIA is revised when necessary.

12. Records, transparency and accountability

USCN retains records of the purpose, necessity reasoning, balancing analysis, safeguards, residual risks and DPO decisions. Evidence is held in this overarching LIA, camera-specific DPIAs and linked supporting records. The complete overarching LIA is intended for publication, subject to necessary security redactions; such redactions must not misrepresent the nature or legal status of the processing.

The DPO approves and records the overarching LIA. The Managing Director receives the approved document. The approval and implementation status of related documents and camera deployments should be accurately reflected in the relevant compliance records; approval of this document must not be represented as commissioning approval.

13. Mandatory steps before any camera records

- Document the identified location-specific safety problem, evidence and realistic less intrusive alternatives.
- Complete the camera-specific purpose, necessity and balancing assessment and obtain an approved DPIA.
- Resolve any applicable Article 9, Article 10, Data Protection Act 2018 or other legal requirements.
- Confirm the field of view, privacy masking where appropriate, audio disabled, motion settings, encryption, retention and access controls.
- Install and verify signage and accessible privacy information.
- Complete commissioning checks, obtain required DPO authorisation and record any conditions as satisfied.
- Do not activate recording if an essential safeguard or lawful-basis requirement remains unresolved.

14. Approval record and limitations

Approval field	Recorded information
Document reference	USCN-LIA-001
Version	1.0
Approval date	19 October 2026
Approving role	Data Protection Officer
Approval confirmed by	USCN instruction supplied for document finalisation
Approved scope	Overarching legitimate interests framework and principles
Excluded from approval	Individual camera balancing outcomes, camera-specific DPIAs, commissioning and public live viewing
DPO signature / independent approval record	Not supplied for inclusion in this document

Formal conclusion: The DPO-approved overarching framework sets out the method and controls for assessing reliance on Article 6(1)(f) UK GDPR for USCN community CCTV. It does not itself conclude that the legitimate interests test passes for any particular proposed camera. Each camera-specific balancing conclusion remains outstanding until documented and approved. No personal-data recording is authorised by this document alone.

Document-control note: Version 1.0 reflects the approval of the overarching framework reported by USCN, dated 19 October 2026. No DPO signature or independent approval evidence was provided for attachment.