

UK Safety Camera Network Ltd

USCN-POL-005 - Public Live Viewing & Privacy Review

Document reference	USCN-POL-005
Version	1.0
Status	APPROVED
Approving authority	Data Protection Officer - Bertram Scanlon
Approval date	19 October 2026
Effective date	19 October 2026 - upon formal approval
Publication status	Not confirmed
Policy owner	UK Safety Camera Network Ltd

1. Purpose

1.1. This policy establishes governance, privacy assessment, technical safeguards, public transparency and incident-response requirements for public live viewing of CCTV cameras operated by UK Safety Camera Network Ltd (USCN).

1.2. The intended general model is public access to approved live camera views where lawful, appropriate and technically feasible. Public availability is conditional. USCN may promptly restrict, suspend or withdraw a view where privacy, security, technical or operational concerns arise, including reasonably suspected concerns.

1.3. Public live viewing is distinct from operational CCTV recording. Authorisation to operate a camera for CCTV purposes does not itself authorise publication of live images.

1.4. This policy operates alongside USCN-POL-001 (CCTV Operations, Privacy & Data Protection), USCN-POL-002 (Footage Access, Disclosure & Retention), USCN-POL-003 (Camera Security & Technical Safeguards), USCN-POL-004 (Public Transparency & Accountability), USCN-LIA-001 and each camera-specific Data Protection Impact Assessment (DPIA).

1.5. Applicable law prevails over conflicting policy provisions. Material privacy matters must be referred to the Data Protection Officer (DPO).

2. Scope and responsibility

2.1. This policy applies to all USCN-controlled cameras for which public live viewing is proposed, configured, enabled, restricted, suspended or withdrawn.

2.2. It applies to USCN personnel, authorised technical operators, relevant contractors and service providers involved in public live-view delivery.

2.3. USCN retains responsibility for CCTV processing and public stream authorisation. Property hosts do not acquire authority to publish, administer, redirect or restore streams by providing premises, power or connectivity.

2.4. The DPO reserves authority over camera-specific public live-view approval, material privacy decisions and restoration after privacy-related suspension. Authorised personnel may take immediate precautionary protective action without prior DPO permission.

3. Public live-viewing model

3.1. **Public live viewing is the intended default model**, subject to camera-specific assessment and express DPO authorisation.

3.2. No camera may begin public live viewing merely because it has been installed, connected or configured to record. Its DPIA, additional live-view assessment, safeguards and DPO approval must be completed first.

3.3. Public viewing will ordinarily be free, without registration, authentication or password.

3.4. Where justified, USCN may impose proportionate camera-specific restrictions, including passwords, registered accounts, authenticated viewers, time-based access, reduced resolution or frame rate, and other appropriate limits.

3.5. Restrictions must be proportionately justified and documented. Material privacy changes or departures from an approved live-view arrangement require DPO approval.

3.6. Public viewers must not receive administrative access, remote camera controls, operational recording access or access to internal camera systems.

3.7. Viewing is a **best-efforts service**; USCN does not guarantee continuous availability.

4. Camera-specific privacy assessment and approval

4.1. Before enabling a public view, USCN must complete or update the camera-specific DPIA and separately assess additional risks arising from public exposure of live images.

4.2. The assessment must consider the CCTV purpose and proportionality of publication; camera position, field of view and framing; identification or singling out of people or vehicles; exposure of homes, windows, gardens or private spaces; vulnerable people and sensitive locations; foreseeable misuse; security-sensitive activities or locations; masking, resolution and other mitigations; separation from administration and recordings; signage and public information; and any other material risk identified.

4.3. **The DPO must expressly authorise public live viewing for each camera.** Network-wide or installation approval alone is insufficient.

4.4. Authorisation may be conditional on masking, framing, quality, access restrictions, hours or other safeguards.

4.5. If acceptable privacy and security protections cannot be achieved, public viewing must not be enabled. This does not automatically decide whether separately authorised operational recording may continue.

4.6. Suitability must be reconsidered following relevant complaints, suspected privacy intrusion, material configuration or contextual changes, security incidents or other information calling approval into question.

4.7. Reviews are event-triggered, not tied to a mandatory annual cycle. Prompt action is required where risk warrants it.

5. Public-stream technical safeguards

5.1. Public-stream delivery must be logically separated from restricted camera administration and stored operational footage.

5.2. Public access is view-only: no pan, tilt, zoom or other remote camera controls; no changes to masking, recording or security; no searching, retrieving, exporting or deleting recordings; and no administrative credentials or internal interfaces.

5.3. Secure delivery must minimise exposure of camera credentials, internal network details and administration endpoints.

5.4. USCN may apply bandwidth, connection, resolution, frame-rate or other limits for privacy, security and resource management.

5.5. A visible USCN watermark or camera identifier should appear where supported and appropriate. A watermark does not guarantee image authenticity or prevent misuse.

5.6. Authorised personnel must have a practicable means of disabling a public stream promptly.

5.7. Faults, misuse reports and relevant alerts must be reviewed as resources reasonably permit; this is not a guarantee of continuous monitoring.

5.8. Third-party streaming or delivery services may be used following appropriate technical/privacy assessment and any required DPO approval. They must not provide suppliers with prohibited remote access to operational camera systems.

5.9. Personal data processed through external delivery arrangements, including viewer-related technical data where relevant, must be assessed under applicable data protection and supplier requirements.

5.10. Public delivery must not become cloud-based operational CCTV recording or storage contrary to USCN-POL-003.

6. Immediate suspension and precautionary action

6.1. USCN may promptly suspend a public live view for actual or reasonably suspected concerns. **Conclusive proof is not required before precautionary action.**

6.2. Triggers include suspected privacy intrusion or inappropriate identification; credible complaints; unexpected visibility of private or sensitive locations; misuse, targeting or security-sensitive disclosure risks; failures of masking, framing, resolution or access controls; DPO or authorised direction; and network outages or operational instability.

6.3. **Authorised USCN personnel may suspend immediately** without prior DPO approval when warranted.

6.4. Privacy-related suspensions and material incidents must be escalated to the DPO as soon as practicable under relevant internal incident procedures.

6.5. Public-stream suspension does not automatically suspend operational recording. Recording ordinarily continues under its existing authorisation unless the DPO directs otherwise or law or mandatory safeguards require different action.

6.6. Where underlying recording may itself be unlawful or unsafe, promptly escalate; nothing in this policy requires unlawful processing to continue.

6.7. **A privacy-suspended stream must remain offline until the DPO expressly authorises restoration** after assessment and sufficient mitigation.

6.8. Ordinary technical recovery may be handled operationally where no privacy suspension or DPO restriction remains. Automatic recovery must not override an outstanding privacy suspension.

6.9. Material suspensions and resolutions must be recorded proportionately, including reason, assessment, corrective action and any restoration approval.

7. Public information and transparency

7.1. USCN must provide clear, accessible public live-view information through its established transparency arrangements.

7.2. The central resource is **transparency.uscn.org.uk**, with camera-specific links incorporating the unique camera ID. **datahandling.uscn.org.uk** may be linked where appropriate.

7.3. Camera-specific information must explain availability, purpose, nature of the view, limitations, access restrictions, privacy safeguards, reporting routes, status where practicable, and appropriate warnings about copying, redistribution or misuse.

7.4. USCN need not disclose detailed security architecture, internal network information or other sensitive material where disclosure creates disproportionate risk.

7.5. Public availability does not authorise unlawful misuse of images. Notices should not falsely imply USCN can prohibit every lawful use of publicly accessible material.

7.6. Signage and transparency information must be consistent with approved viewing arrangements and USCN-POL-004.

8. Public concerns, complaints and privacy review

8.1. The public must have a practical route to report concerns about field of view, identification, private spaces, misuse or inappropriate availability.

8.2. Credible concerns require prompt assessment and, where warranted, precautionary suspension before investigation concludes.

8.3. The DPO oversees material privacy concerns, reassessment and restoration of privacy-suspended streams.

8.4. Remedies may include changed framing, masking, resolution, access restrictions, viewing hours, public information or other controls. Viewing may remain withdrawn where mitigation is inadequate.

8.5. Complaints and statutory rights requests follow applicable law and related USCN policies. Routine enquiries are handled proportionately within available resources.

8.6. Where practicable, provide the complainant with an acknowledgement or proportionate outcome without disclosing confidential, personal or security-sensitive information.

9. Records and accountability

9.1. USCN must maintain proportionate records of significant public live-view decisions and actions.

9.2. Records should cover assessments and DPO approvals; material restrictions; significant complaints; material suspensions and reasons; reassessments and corrective measures; and DPO restoration authorisations.

9.3. Every transient outage, viewer interaction or minor status change does not require a separate formal decision record solely under this policy.

9.4. Records must be appropriately protected, access-controlled and retained in line with relevant USCN requirements.

9.5. The DPO may review material decisions and require further mitigation, restriction, suspension or withdrawal.

10. Responsibilities and decision-making

10.1. **DPO:** Approves each camera's live view; reviews DPIAs and live-view risks; decides material privacy restrictions; oversees significant complaints and reassessment; approves restoration after privacy suspension; approves this policy and material privacy amendments.

10.2. **Authorised USCN personnel:** Implement approved controls; maintain separation from restricted systems; promptly suspend where warranted; escalate significant matters; document significant decisions; and operate within DPO authorisations.

10.3. **Property hosts:** Meet agreed physical, connectivity, signage and reporting duties; they may not independently grant access, alter arrangements or restore suspended streams.

10.4. **External providers:** Act within approved technical and contractual arrangements. USCN retains controller responsibility and reserved privacy decisions.

11. Mandatory safeguards and exceptions

11.1. Mandatory requirements are: (a) camera-specific DPIA and live-view assessment before enabling; (b) express DPO authorisation for each camera; (c) immediate precautionary suspension authority for designated personnel; (d) DPO approval before privacy-related restoration; (e) separation of public viewing from administration and recordings; (f) camera-specific transparency and concern-reporting route; and (g) proportionate records of significant assessments, suspensions, complaints and restorations.

11.2. Routine operational discretion cannot waive mandatory safeguards.

11.3. Operational variations in quality, access, delivery or availability are permitted within this policy and applicable DPO authorisations. Material privacy changes require DPO approval.

11.4. If a mandatory safeguard cannot be met, public viewing must not begin or must remain suspended until appropriately resolved.

12. Implementation and review

12.1. This policy became effective **19 October 2026 upon formal DPO approval**, independently of its publication date.

12.2. It applies to all new public live-view proposals.

12.3. Existing or planned live-view arrangements must be reviewed for compliance before being enabled or permitted to continue; prior configuration is not an exemption.

12.4. Camera-specific approvals, public information and operational controls must be consistent with this policy before public viewing is authorised.

12.5. Review is required when material legal, technical, operational or privacy developments warrant it; no mandatory annual review cycle is imposed.

12.6. Material amendments affecting privacy safeguards or DPO-reserved decisions require appropriate DPO approval.

13. Approval and document control

13.1. **Formal approval:** Approved by Data Protection Officer Bertram Scanlon on 19 October 2026.

13.2. **Effective date:** 19 October 2026, immediately upon formal approval.

13.3. **Publication:** Not confirmed. Formal approval and public publication are distinct events.

13.4. **Next review:** On material change or identified need.

End of approved policy - USCN-POL-005 version 1.0.