

Camera-Specific Data Protection Impact Assessment

USCN-DPIA-T01 • Version 0.1 working template • Prepared 19 October 2026

Document status	WORKING TEMPLATE — not formally approved or executed
Controller	UK Safety Camera Network Ltd (USCN)
Data protection contact	data.protection@datahandling.uscn.org.uk
Postal contact	124 City Rd, Islington, London, EC1V 2NX
Source policies	USCN-POL-001 to 006; USCN-LIA-001 (approved 19 October 2026)
Important	No operationally commissioned cameras confirmed. No supplier processor status or international transfers verified.

Identity and screening

Camera ID []; proposed site []; host []; assessor []; version/date []; planned coverage map/photo reference [].

Status: proposed / physical installation only / commissioned []; no commissioning is permitted on the strength of this template alone.

Explain whether likely high risk, systematic monitoring of publicly accessible areas, vulnerable persons or sensitive locations; justify DPIA scope.

Processing description and necessity

Public safety objective and evidence []; persons likely recorded []; hours/motion triggers []; boundaries/angles [].

Data types: video imagery, timestamps and incident metadata; confirm no audio, ANPR, facial recognition, behavioural profiling or unrestricted PTZ.

Article 6 basis: legitimate interests as applicable; link overarching LIA and perform site-specific balancing [].

Potential criminal-offence data: assess Article 10/DPA 2018 Schedule 1 condition, safeguards and APD requirement separately [].

Alternatives considered (lighting, signage, narrower field, masking, no camera) and reasons [].

Data flows and safeguards

Encrypted local SD/NVR; no operational cloud recording. Map access routes, network isolation, maintenance and any temporary disclosure copies [].

Routine footage auto-overwritten no later than 31 days; DPO-authorized holds documented under POL-002.

Signs in place before recording, QR to camera-specific page on transparency.uscn.org.uk; link to datahandling.uscn.org.uk.

Host no admin access; supplier remote access to live operational camera systems prohibited.

Risk assessment

Risk 1: capture of private premises or sensitive areas — likelihood [] impact [] mitigation masking/repositioning [] residual [].

Risk 2: over-collection or unjustified monitoring — likelihood [] impact [] mitigation motion zones/coverage [] residual [].

Risk 3: unauthorised access or loss — likelihood [] impact [] mitigation encryption/access logging [] residual [].

Risk 4: inadvertent disclosure/retention — likelihood [] impact [] mitigation DPO review/31-day overwrite [] residual [].

Risk 5: public live viewing — assess separately under POL-005; do not treat this DPIA as stream approval.

Decision and authorisation

Consultations and host/public feedback []; technical checks []; outstanding actions []; residual high risk [].

If high risk cannot be mitigated, assess need for prior ICO consultation before processing.

DPO DPIA decision: approve / conditional / reject []; rationale []; signature []; date [].

Operational commissioning requires separate signed USCN-FRM-001; DPIA approval alone is insufficient.