

Fleet Camera Pilot Plan & RFP Checklist

A step-by-step guide for deploying cameras across 20+ vehicles with confidence.

backwatch.co.uk

How to use this checklist

Work through each phase in order. Tick each item when complete. Share this document with your Ops, Safety, IT, HR, Legal and Union stakeholders before starting procurement.

Phase 0 — Prep & Governance (1–2 weeks)

Stakeholders & objectives

- ☐ Appoint a project lead (Operations)
- ☐ Form steering group: Ops · Safety · IT · HR · Legal · Union rep
- ☐ Define measurable objectives (e.g. reduce claims by X%, evidence in <8 hrs)
- ☐ Set false-alert tolerance threshold
- ☐ Agree retention schedule (non-incident: 7–30 days; incidents: 90–540 days)

Procurement requirements document

- ☐ Hardware warranty & spares policy
- ☐ Data encryption standard and retention controls
- ☐ API spec and telematics integration SLA
- ☐ Install SLA and hardware replacement SLA
- ☐ GDPR clauses and DPIA support commitment from vendor
- ☐ Export formats and chain-of-custody requirements

Phase 1 — Pilot (6–12 vehicles, 4–8 weeks)

Vehicle selection

- ☐ 2 high-risk vehicles (urban / city centre)
- ☐ 2 medium-risk vehicles (regional delivery)
- ☐ 2 low-risk vehicles (motorway / rural)
- ☐ Include at least one HGV if applicable

Metrics to collect during pilot

- ☐ Incident capture rate per 1,000 km
- ☐ Time-to-evidence: incident → export (target: <8 hrs)
- ☐ False-alert rate and admin time per alert (hrs/week)
- ☐ Data usage per vehicle (GB/week)
- ☐ Driver feedback score (1–5 scale)

- ☐ Installation time per vehicle (hrs)

Governance during pilot

- ☐ Complete DPIA for pilot vehicles
- ☐ Run driver workshop before installation
- ☐ Driver sign-off forms completed post-install
- ☐ Review pilot data at week 2, week 4 and end of pilot

Pilot Evaluation — Vendor Scoring Matrix

Criteria	Weight	Vendor A /10	Vendor B /10	Vendor C /10
Features & coverage	30%			
Total cost of ownership	25%			
Compliance (GDPR/FORS/DVS)	15%			
Install & support SLA	15%			
References & case studies	15%			
WEIGHTED TOTAL	100%			

Phase 2 — Procurement & Contracts (4–6 weeks)

RFP must-haves

- ☐ Device model, power draw (parking mode), pre-roll seconds
- ☐ Upload latency (seconds from event to cloud availability)
- ☐ API endpoints and sample data export format
- ☐ Cellular carrier compatibility and per-GB pricing
- ☐ FORS / DVS reporting modules (if applicable)
- ☐ GDPR toolkit: DPIA support, role-based access, privacy masking
- ☐ Sample evidence export with chain-of-custody hash

Contract must-haves

- ☐ Firmware update policy and OTA provisions
- ☐ Data ownership and export rights clearly stated
- ☐ Install and hardware replacement SLA (hrs to replacement)
- ☐ Cellular and cloud pricing — caps on overages clearly defined
- ☐ Right-to-audit clause
- ☐ Termination and data deletion procedure

Phase 3 — Fleet-wide Rollout (3–6 months)

Per-vehicle installation checklist

- ☐ Pre-install: confirm VIN, vehicle type, battery topology
- ☐ Install: tidy wiring, label all connectors
- ☐ Photograph completed installation (stored with vehicle record)
- ☐ Note SD card serial number in asset register
- ☐ Post-install: register device on platform

- ☐ Run remote health check (all cameras confirmed active)
- ☐ Driver sign-off form completed and filed

Rollout logistics

- ☐ Wave plan agreed (recommended: 10 vehicles/week)
- ☐ Mobile installers or overnight slots booked
- ☐ 10% spare pool of pre-installed units available for immediate swap
- ☐ Downtime tracking sheet in place

Phase 4 — Ops & Continuous Improvement

Ongoing operations

- ☐ Admin roles & permissions documented (view / export / approve)
- ☐ Evidence retrieval SOP published to ops team
- ☐ Coaching workflow documented (positive-first, escalation tiers)
- ☐ Alert thresholds tuned to reduce false positives
- ☐ Quarterly KPI review scheduled (claims, data cost, admin time)
- ☐ Vendor performance review at 3 months and 12 months

Key red flags to watch for

- Separate cellular and cloud contracts — you may pay twice for connectivity.
- No DPIA or vague retention policy — a GDPR liability.
- Vendor cannot provide signed export or chain-of-custody metadata.
- Surprise installs without driver communication — creates trust issues.
- Hundreds of low-value alerts per week — alert fatigue kills adoption.
- Long RMAs with overseas-only repair — fleet downtime risk.