

Remote Fleet Monitoring: Operator SOP Checklist

Reference checklist for fleet remote monitoring operators — covering pre-deployment setup, alert configuration, incident response, and compliance review cycles.

backwatch.co.uk

Pre-Deployment Setup

- ☐ Define who is responsible for monitoring (dedicated role vs. shared responsibility)
- ☐ Document which alert types require immediate action vs. log-only vs. review queue
- ☐ Write and distribute written escalation protocol with named contacts and order
- ☐ Confirm platform access for all monitoring operators (logins, vehicle groups, alert views)
- ☐ Define the standard event log format (timestamp, vehicle ID, GPS, description)
- ☐ Establish footage download and evidence preservation procedure before first incident

Alert Configuration

- ☐ Set g-force thresholds by vehicle class (7.5t, HGV, LGV, coach) not a single global value
- ☐ Configure tiered alert levels: Level 1 (immediate), Level 2 (daily review), Level 3 (weekly coaching)
- ☐ Review false positive rate weekly for first month after any threshold change
- ☐ Set geofence boundaries accounting for GPS drift (minimum 50m buffer from actual boundary)
- ☐ Configure camera health alerts separately from driving behaviour alerts
- ☐ Suppress maintenance/diagnostic alerts outside of shift hours if no overnight operator

Incident Response Protocol (5 Steps)

- ☐ Step 1 — VERIFY: Access auto-uploaded event clip, confirm genuine incident vs. false positive
- ☐ Step 2 — CHECK: View live feed to confirm vehicle status; attempt driver contact by radio/phone
- ☐ Step 3 — LOG: Record timestamp, vehicle ID, GPS coordinates, driver, and footage description NOW
- ☐ Step 4 — ESCALATE: Notify correct contact (transport/fleet manager/emergency services) per severity
- ☐ Step 5 — PRESERVE: Flag footage for download; export GPS data ± 10 minutes around event
- ☐ Target: complete all 5 steps within 5 minutes of alert confirmation

GDPR & Access Control

- ☐ Restrict live view access to named roles only (transport manager, fleet manager, compliance)
- ☐ Confirm platform automatically logs: user ID, vehicle accessed, session time, footage downloads
- ☐ Define footage retention periods in policy and confirm platform settings match (min. 30 days)
- ☐ Confirm all drivers have received written notification of camera and monitoring policy
- ☐ Complete DPIA (Data Protection Impact Assessment) before deploying driver-facing cameras
- ☐ Review and re-sign driver monitoring policy when new camera types are added to fleet

Review Cadence

- ☐ Weekly: Review alert volume — Level 1 true positive rate; adjust thresholds if needed
- ☐ Weekly: Check footage preservation log — any expired clips before download?
- ☐ Monthly: Incident log audit — correctly identified/escalated vs. missed
- ☐ Monthly: Driver coaching review — patterns, conversations documented, targets agreed
- ☐ Quarterly: Operator competency check — platform navigation + 5-step protocol drill
- ☐ Annually: Full DPIA review and monitoring policy update signed by all operators