

Personal Data Breach & Security Incident Response Procedure

USCN-PRO-001 • 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.

Intake and containment

Report suspected loss, unauthorised access, disclosure, tampering or outage immediately to the DPO/security lead via verified internal channel [TO BE SET].

Significant incidents must be escalated internally promptly and no later than 24 hours, per approved safeguards. Preserve evidence, restrict access, isolate affected components as proportionate; do not destroy logs.

Assessment and notification

Record discovery time, occurrence window, affected systems/people/data, likelihood and severity of risk, mitigation, evidence and DPO decision.

Where a personal data breach is notifiable, notify ICO without undue delay and where feasible within 72 hours of becoming aware; record reasons for any delay.

Notify affected individuals without undue delay where high risk requires it, unless a lawful exception applies. Record decisions even where no notification occurs.

Supplier contracts must require prompt breach notification and assistance; processor notification to USCN does not replace controller assessment.

Closure

Maintain incident log, remedial actions, evidence of completed fixes, lessons learned, review and DPO closure date.