CCTV POLICY

1. Purpose

ZAM FM Ltd uses CCTV and other video surveillance systems where appropriate to support the protection of people, property and premises and to assist with the prevention and detection of crime and security incidents.

CCTV footage may constitute personal data where individuals can be identified. CCTV systems will therefore be operated in a lawful, fair, transparent, proportionate and secure manner in accordance with applicable UK data protection requirements.

This policy establishes requirements for CCTV operation, monitoring, access, recording, storage, disclosure, retention, deletion, requests for footage, evidence management, system security and review.

REVISION HISTORY

Issue Number	Review Date	Changes	Signed
01	22/09/2023	Original version (draft)	
01	22/09/2023	Signed off	
01	20/09/2024	Review	
01	19/09/2025	Review	
02	20/05/2026	Address Updated	
02	18/09/2026	Review	

2. Scope

This policy applies to CCTV systems operated or managed by the Company; CCTV systems operated on behalf of clients where the Company's contractual responsibilities include CCTV monitoring or management; security officers and CCTV operators; managers and supervisors; authorised employees and contractors; CCTV recordings, still images and exported footage; remote viewing arrangements; and associated CCTV documentation and records.

Where the Company operates CCTV on behalf of a client, the parties' respective responsibilities as controller, processor or other relevant role shall be determined and documented appropriately.

3. Policy Statement

The Company will only use CCTV where there is a legitimate and clearly defined purpose. CCTV will not be used simply because technology is available. The purpose, necessity and proportionality of surveillance will be considered before a system is introduced or materially changed.

The Company will identify the purpose of each CCTV system, establish an appropriate lawful basis, provide appropriate privacy information, restrict access to authorised persons, protect footage, retain

footage only as long as necessary, respond appropriately to valid requests, maintain relevant records and review arrangements periodically.

4. Lawful Basis and Data Protection

CCTV footage involving identifiable individuals is generally personal data and must be handled in accordance with applicable data protection legislation.

Before CCTV is deployed, the Company or relevant client shall identify and document the appropriate UK GDPR Article 6 lawful basis. Depending on the circumstances, this may include legitimate interests, legal obligation or another lawful basis where applicable.

Consent will not automatically be assumed simply because CCTV is visible. The reason for processing will be documented and CCTV use will be necessary and proportionate.

Where special category data, criminal offence data or particularly intrusive surveillance technologies are involved, additional requirements will be considered.

5. Purpose of CCTV

CCTV may be used, where justified and documented, for protection of employees, visitors and members of the public; protection of client property and assets; prevention and detection of crime; investigation of security incidents; monitoring access and egress; supporting emergency response; assisting law enforcement where lawfully required; monitoring defined security risks; protection against unauthorised access; and supporting contractual security requirements.

CCTV shall not be used for purposes incompatible with the documented purpose without appropriate assessment and authorisation.

6. Camera Positioning and Privacy

Cameras shall be positioned so that they achieve their legitimate security purpose while minimising unnecessary intrusion into individuals' privacy.

The Company shall consider the field of view, areas monitored, privacy expectations, neighbouring properties, public areas, staff areas, private areas, camera functionality and whether recording is necessary.

Cameras should not normally monitor areas where individuals have a heightened expectation of privacy unless there is a clearly documented and lawful justification.

Camera views shall be reviewed following significant changes to premises, system configuration or operational requirements.

7. CCTV Signage and Transparency

Appropriate CCTV signage shall be displayed where surveillance is taking place and positioned so that individuals can reasonably understand that CCTV is operating before entering the monitored area.

Where appropriate, signage should identify that CCTV is in operation and provide information regarding the organisation responsible for the system and how further privacy information can be obtained.

The Company's privacy information shall explain the relevant CCTV processing.

8. CCTV Operators

Only authorised and appropriately trained personnel may operate or access CCTV systems.

Operators shall follow the CCTV operating procedure; maintain confidentiality; access footage only for legitimate work purposes; maintain records; report faults and suspected misuse; protect passwords; follow client assignment instructions; and comply with data protection requirements.

Operators must not access footage for personal reasons, copy footage without authorisation, share footage through personal messaging or social media, photograph screens using personal devices, disclose information to unauthorised persons or allow unauthorised operation.

9. Access Control

Access to CCTV systems shall be restricted according to job responsibilities.

Where technically possible, individual user accounts shall be used; passwords kept confidential; access rights reviewed periodically; former employees' access removed promptly; exported footage access controlled; and access/export logs maintained where available.

Management shall determine who is authorised to access CCTV recordings.

10. CCTV Monitoring

CCTV monitoring shall be conducted in accordance with client requirements, assignment instructions, operating procedures, contractual requirements, data protection requirements and emergency and incident procedures.

Operators shall remain alert to relevant security events and escalate incidents according to applicable assignment instructions.

CCTV monitoring should not replace physical security controls where physical intervention or response is required.

11. Audio Recording

Audio recording can be significantly more intrusive than visual recording. Audio functionality shall only be enabled where there is a documented and justified requirement and the processing has been appropriately assessed.

Where audio is not required, it should be disabled.

12. Recording and Storage

CCTV recordings shall be stored securely using appropriate technical and organisational controls to protect against unauthorised access, accidental deletion, alteration, disclosure, loss and inappropriate use.

Where cloud-based CCTV systems are used, relevant security, contractual and data protection requirements shall be considered.

13. Retention of CCTV Footage

There is no single statutory CCTV retention period that applies to every CCTV system. Retention shall be determined according to the purpose for which footage is processed and footage retained only for as long as necessary.

As a general operational starting point, the Company may use a defined retention period such as 31 days, subject to client requirements, system capacity, documented assessment and applicable law.

Where footage is required for an investigation, complaint, insurance matter, disciplinary proceedings, legal proceedings or law enforcement request, it may be preserved beyond the normal retention period where lawful and necessary.

14. Deletion

At the end of the approved retention period, footage shall be securely deleted or automatically overwritten where the system is configured to do so.

Footage preserved for a specific investigation shall be reviewed and securely deleted when no longer required.

15. Disclosure to Police and Other Authorities

CCTV footage may be disclosed to the police or another competent authority where there is a lawful basis for disclosure.

Requests should normally be verified, recorded, made by an appropriately authorised person, limited to information reasonably required and handled securely.

The Company shall maintain a CCTV Disclosure / Footage Release Log for significant disclosures.

16. Requests for CCTV Footage

Individuals may have rights under data protection legislation concerning their personal data, including rights relating to access.

Requests for CCTV footage shall be referred to the Data Protection Lead or other authorised person.

The Company shall assess the identity of the requester, date/time, location, whether footage exists, whether other individuals are visible, whether disclosure is permitted, whether redaction is required and applicable statutory requirements.

The Company shall not automatically release footage simply because a person asks for it.

17. CCTV Incident Management

Suspected misuse, unauthorised disclosure, loss, theft or compromise of CCTV footage shall be reported immediately to management.

Examples include unauthorised access, footage sent to the wrong person, lost exports, unauthorised copying, inappropriate viewing, system compromise, accidental disclosure or deliberate misuse.

The Company shall assess whether the incident constitutes a personal data breach and take appropriate action.

18. CCTV Export and Evidence

Where CCTV footage is required as evidence, the relevant date/time and camera shall be identified; footage exported using an authorised process; the original protected; the export securely stored; disclosure or transfer recorded; and an audit trail maintained.

Where evidence is provided to another organisation, the receiving organisation and date of transfer should be recorded.

19. Body-Worn Video

Where security personnel use Body-Worn Video (BWV), separate operating instructions shall apply.

BWV shall only be used where authorised and where appropriate lawful basis, operational purpose, information/signage, retention, access controls, activation requirements, incident procedures and staff training have been established.

20. CCTV Maintenance

CCTV equipment shall be maintained to ensure it remains suitable for its intended purpose.

Records should cover system faults, repairs, maintenance, camera failures, recording failures, date/time accuracy, storage capacity, system testing and corrective action.

Faults that materially affect security coverage shall be reported promptly.

21. Training and Competence

Personnel responsible for CCTV shall receive appropriate training relevant to their role.

Training may include CCTV operation, data protection, confidentiality, incident management, evidence handling, access controls, disclosure procedures, subject access requests, information security, client requirements and emergency procedures.

Training records shall be retained. Where a CCTV operator role is subject to SIA licensing requirements, applicable licensing requirements shall be met.

22. Monitoring and Review

The Company shall periodically review CCTV arrangements to ensure the system continues to meet its stated purpose; cameras remain appropriately positioned; retention remains appropriate; access rights remain appropriate; signage remains adequate; security controls remain effective; operators remain trained; incidents and complaints are reviewed; and the system remains necessary and proportionate.

23. Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) shall be considered before introducing surveillance likely to result in a high risk to individuals.

This is particularly important for more intrusive systems or large-scale monitoring, including certain workplace surveillance arrangements.

27. Review

This policy shall be reviewed at least annually or sooner where there are significant changes to legislation, ICO guidance, surveillance technology, contractual requirements, client requirements, Company operations or identified risks.

The policy owner shall verify the current regulatory and guidance position at each review.

24. Responsibilities

Managing Director: Approves this policy, ensures resources are available, allocates responsibilities and reviews significant CCTV issues.

Data Protection Lead: Monitors data protection compliance, advises on lawful CCTV use, handles data protection requests, reviews disclosures, supports DPIAs and investigates relevant incidents.

Operations Manager: Ensures CCTV procedures are implemented, operators follow assignment instructions, performance is monitored and significant issues are reported.

CCTV Operators / Security Officers: Follow authorised procedures, maintain confidentiality, use CCTV only for legitimate purposes, report incidents and faults, protect credentials and never misuse or disclose CCTV information.

25. Records

- CCTV System Register
- CCTV Camera Location Register
- CCTV Maintenance Log
- CCTV Operator Training Records
- CCTV Access Log
- CCTV Footage Request Log
- CCTV Disclosure / Release Log
- CCTV Incident Log
- CCTV Export / Evidence Log
- Retention and Deletion Records
- Data Protection Impact Assessment (DPIA)
- Legitimate Interests Assessment, where applicable
- CCTV Privacy Notice

- CCTV Signage Records
- CCTV Review / Audit Records

26. Related Documents

- Data Protection Policy
- Privacy Notice
- Information Security Policy
- Data Retention Policy
- Incident Management Procedure
- Subject Access Request Procedure
- CCTV Operating Procedure
- CCTV Footage Release Procedure
- CCTV Maintenance Procedure
- Staff Confidentiality Policy
- Disciplinary Procedure
- Assignment Instructions

Managing Director

Name: DANISH IFTIKHAR

Sign: 

Dated: 22-09-2023