

CCTV and Video Surveillance Policy

October 2026

1. Policy statement

Realise Training Group and its subsidiaries ("the Company") recognises that CCTV and other video surveillance systems can play a legitimate role in maintaining a safe and secure environment for employees, learners, apprentices, visitors and members of the public. The Company also recognises that surveillance may affect individuals' privacy and behaviour.

Images and other information relating to identifiable individuals are personal data. The Company will operate surveillance systems lawfully, fairly, transparently, securely and only where their use is necessary and proportionate for a defined purpose.

Misuse of surveillance information is prohibited and may constitute misconduct, a breach of data protection law or, in some circumstances, a criminal offence.

2. Scope

This policy applies to the Company's overt CCTV and video surveillance systems and to all employees, contractors and officers who specify, approve, operate, maintain, access, export, disclose or otherwise process surveillance information on the Company's behalf.

It applies to fixed cameras, live viewing, recorded video, still images and any associated system used at Company-controlled premises. Any proposal to use other technologies, including audio recording, automatic number plate recognition, body-worn video, drones, facial recognition, biometric identification, portable cameras or live streaming, must be approved through the process in section 12 before use.

This policy does not authorise covert surveillance. Any exceptional proposal for covert monitoring requires specific legal and data protection advice and separate senior approval before implementation.

This policy does not form part of any individual's contract of employment or terms and conditions. The Company may amend it from time to time.

3. Definitions

Term	Definition
CCTV	Fixed or moveable cameras and associated equipment used to view or record images for surveillance purposes.
Controller	The organisation that determines the purposes and means of processing personal data. The Company is the controller for surveillance it operates for its own purposes.
Data subject	An identified or identifiable living individual whose personal data is processed.
Personal data	Information relating to an identified or identifiable living individual, including recognisable video images and still pictures.
Processing	Any operation involving personal data, including collection, viewing, recording, storage, retrieval, export, disclosure, restriction and deletion.

Term	Definition
Processor	A person or organisation that processes personal data on behalf of the Company and under its instructions.
DPIA	A Data Protection Impact Assessment used to assess necessity, proportionality, risks to individuals and mitigating controls.
LIA	A Legitimate Interests Assessment documenting the purpose, necessity and balancing tests for reliance on legitimate interests.
Surveillance information	Live or recorded images, stills, metadata, access logs, exports and associated records generated by a surveillance system.

4. Governance and responsibilities

4.1 Chief Executive Officer

- Has overall executive responsibility for this policy and the lawful operation of the Company's surveillance systems.
- Approves exceptional or materially intrusive surveillance where escalation is required.

4.2 Data Protection lead

- Advises on lawful basis, transparency, individual rights, DPIAs, LIAs, disclosures and personal data breaches.
- Reviews high-risk or novel surveillance proposals and determines whether prior consultation with the Information Commissioner is required where high residual risk cannot be mitigated.
- Maintains oversight of the relevant record of processing activities and privacy information.

4.3 Chief People Officer

- Advises on workplace-monitoring fairness, employee consultation, investigations and employment implications.
- Ensures that footage is used in employee matters only where necessary, proportionate and consistent with the stated purposes and applicable procedures.

4.4 Facilities lead

- Has day-to-day operational responsibility for approved CCTV systems, including camera positioning, signage, maintenance, retention settings and authorised access.
- Maintains the CCTV Asset Register and operational logs required by this policy.
- Ensures faults, unauthorised access and security incidents are reported promptly.

4.5 Authorised users

- Access surveillance information only for an approved business purpose and within the permissions granted.
- Keep information confidential and use approved methods for viewing, export, transfer and deletion.
- Complete relevant training and maintain accurate records of access and disclosure.

4.6 Deputies and contact route

Current role holders, nominated deputies and contact details must be maintained in an access-controlled CCTV Contact Register. CCTV signage and the Company privacy notice must provide a current route for questions and individual-rights requests without publishing unnecessary personal contact details in this policy.

5. Purposes and lawful basis

The Company may use CCTV where necessary and proportionate for one or more of the following specified purposes:

- Preventing and detecting crime and protecting premises, assets and systems from theft, damage, disruption or vandalism.
- Protecting the safety and security of employees, learners, apprentices, visitors and members of the public.
- Supporting law-enforcement activity where disclosure is lawful and proportionate.
- Supporting the investigation of accidents, incidents, safeguarding concerns and health and safety events.
- Supporting the fair investigation and resolution of disciplinary, grievance or other internal matters where the use is compatible with the notified purpose and is necessary and proportionate.

The Company's usual Article 6 UK GDPR lawful basis for these purposes is legitimate interests under Article 6(1)(f). The Company must document those interests, necessity and the balance against individuals' rights in an LIA and, where required, a DPIA. A different lawful basis must be identified and documented where legitimate interests is not appropriate.

CCTV must not be used for a new and incompatible purpose merely because the technical capability exists. It must not be used routinely to measure employee productivity, attendance or performance unless a separate, lawful, necessary, proportionate and transparent assessment has been completed and approved.

If a proposed use actively processes special category data, biometric data for unique identification, or criminal offence data, the Data Protection lead must identify and document all additional UK GDPR and Data Protection Act 2018 conditions and safeguards before processing begins.

6. Necessity, proportionality and camera placement

- Less privacy-intrusive alternatives must be considered before installing or extending surveillance.
- Cameras must be positioned and configured to capture only areas necessary for the approved purpose. Privacy masking or restricted fields of view must be used where appropriate.
- The field of view must avoid private homes, gardens and other areas outside Company control where reasonably practicable.
- Cameras must not normally be installed in toilets, changing rooms, rest areas or other locations where individuals have a heightened expectation of privacy.
- Continuous monitoring of a particular individual is not permitted except under a separately approved and lawful process.

- Image quality, date and time settings must be sufficient and accurate for the stated purpose and checked periodically.

Current use is limited to monitoring the exterior of the relevant building and the main entrance 24 hours a day, with authorised live monitoring during working hours. Any material change to locations, operating hours, fields of view or monitoring arrangements requires review under section 12.

7. Transparency and signage

- Clear, visible and readable signs must be positioned before an individual enters a monitored area and repeated where necessary.
- Signs must identify the Company as the operator where this is not obvious, state the purpose of monitoring, and provide a current contact route or link to further privacy information.
- The Company must maintain layered privacy information explaining the lawful basis, purposes, categories of data, retention, recipients, rights, complaints and contact details.
- Employees, contractors and other regular site users must receive appropriate information about the nature and extent of workplace surveillance.
- Where monitoring may materially affect employees, learners or apprentices, the Company must consider appropriate consultation and safeguarding implications as part of the DPIA.

8. Operation, access and security

- Live feeds and recordings may be viewed only by authorised users whose duties require access.
- Recorded footage must be viewed in a secure location or through an approved secure connection that prevents unauthorised observation.
- Access must be role-based, use individual accounts where technically available, and be removed promptly when no longer required.
- Administrative and remote access must be protected by appropriate authentication and logging.
- Exports must be limited to the minimum necessary, protected during transfer and storage, and deleted when no longer required.
- Portable media must not be used unless specifically authorised, encrypted where supported and recorded in the disclosure or evidence log.
- The system, connected devices and supporting software must be securely configured, maintained and updated.
- The Company must retain an access and disclosure audit trail where the system supports it, and otherwise maintain a manual log. Logs must be reviewed periodically by the Facilities lead and any anomalies escalated.
- Cloud storage or other processors may be used only following appropriate due diligence, a compliant written contract, security assessment and international-transfer assessment where relevant.

9. Audio recording and advanced technologies

Audio recording is more intrusive than visual recording and must be switched off by default. It may be enabled only in exceptional circumstances where a specific evidenced need cannot reasonably

be met by less intrusive means, and only after an approved DPIA, lawful-basis assessment, enhanced transparency and senior approval.

Facial recognition, biometric identification, behavioural analytics, automatic number plate recognition, automated decision-making and artificial intelligence functions must not be enabled by default. Any proposal requires separate assessment of purpose, necessity, proportionality, lawful conditions, accuracy, bias, security, individual rights and safeguarding before implementation.

10. Retention, preservation and secure deletion

Routine CCTV recordings will be retained for 30 days from the date of recording and then permanently and securely deleted, unless a shorter setting is appropriate for a particular system or specific footage must be preserved for an approved purpose.

Specific footage may be retained beyond 30 days where necessary for:

- Evidence relating to a crime, security incident, accident, safeguarding matter or health and safety event.
- A disciplinary, grievance, complaint or other internal investigation.
- A subject access request, legal claim, litigation hold, court order, insurance matter or lawful request from a competent authority.

A preservation record must identify the reason, responsible owner, review date, access restrictions and final disposal decision. When footage is no longer required, it must be deleted securely and the deletion recorded. Physical exports, still images and printed copies must be disposed of as confidential waste when no longer required.

The Facilities lead must conduct periodic checks to confirm that configured retention periods and deletion controls are working as intended.

11. Disclosure and sharing

Surveillance information must not be disclosed unless the disclosure is lawful, necessary, proportionate and consistent with the documented purpose, or otherwise required by law.

- Requests from law-enforcement bodies must be verified and recorded. Disclosure should be limited to relevant footage and made securely.
- Disclosures to group companies, legal advisers, insurers, courts, regulators or other third parties require an appropriate lawful basis and documented approval.
- A disclosure log must record the requester, authority or purpose, footage disclosed, approver, date, method and any restrictions.
- Footage must not be posted online, shared through personal accounts or disclosed to the media. Any exceptional external publication requires specific legal, data protection and executive approval.
- Processors may access footage only under written instructions and appropriate contractual, confidentiality and security safeguards.

12. DPIAs, changes and the CCTV Asset Register

Before installing a new system or materially changing an existing system, the Company must assess the proposed processing. A DPIA is required where the processing is likely to result in a high risk to individuals, including workplace monitoring, large-scale monitoring of publicly accessible areas, advanced analytics, biometric processing, audio recording or monitoring in circumstances of heightened privacy risk.

The assessment must address the purpose, lawful basis, reasonable expectations, necessity, proportionality, less intrusive alternatives, data minimisation, transparency, security, retention, sharing, individual rights, safeguarding, consultation and residual risks. Processing must not start until required approvals are complete.

A review is also required when cameras are added, removed, moved or re-aimed; recording hours or retention change; the system is upgraded; new analytics, audio, cloud storage or integrations are introduced; or the purpose changes.

The Facilities lead must maintain a CCTV Asset Register containing, as a minimum:

- Site, camera or system identifier, location, field of view and operational status.
- Purpose, lawful basis, LIA or DPIA reference and responsible owner.
- Recording and live-monitoring hours, audio status and advanced features.
- Retention setting, storage location, processor and relevant transfer position.
- Authorised roles, access-control method, signage location and privacy-notice link.
- Maintenance, review, test and decommissioning dates.

13. Individual rights and subject access requests

Individuals may exercise applicable data protection rights in relation to surveillance information, including the right of access and, in appropriate circumstances, objection, restriction or erasure. Requests must be sent through the Company's approved data rights process and handled in accordance with the Data Protection Policy and Subject Access Request procedure.

- The Company may ask for sufficient details to locate relevant footage, such as the date, approximate time, location and information needed to identify the requester.
- The Company must conduct a reasonable and proportionate search and respond within the applicable statutory timeframe.
- Images of other people must be redacted, obscured or otherwise protected where required, taking account of their rights and any applicable exemption.
- Original footage must be preserved where needed while a request is being handled.
- Any refusal, exemption, extension or fee must be decided and documented by the Data Protection lead in accordance with applicable law.

This policy does not rely on automated decision-making. Any future proposal to make solely automated decisions producing legal or similarly significant effects requires separate assessment and approval.

14. Personal data breaches and incidents

Loss, unauthorised access, disclosure, alteration, destruction, inability to access required footage, compromised credentials or other security incidents involving surveillance information must be reported immediately through the Company's approved data breach and IT incident routes.

- Preserve relevant logs and evidence without unnecessarily increasing access to the footage.
- Contain the incident, revoke inappropriate access and prevent further disclosure where practicable.
- Inform the Data Protection lead promptly so that risk to individuals and any notification obligations can be assessed.
- Record the facts, effects, decisions and remedial action, whether or not external notification is required.
- Coordinate communications with the Facilities lead, IT, People team, safeguarding, legal advisers and senior management as appropriate.

15. Complaints and concerns

Questions or concerns about CCTV should be raised with the individual's line manager, the Facilities lead or the Data Protection lead using the contact route in the privacy notice or CCTV signage. Employees may also use the relevant Company complaint or grievance procedure.

Individuals may complain to the Information Commissioner's Office. The Company encourages individuals to raise concerns with the Company first so that the matter can be investigated and, where appropriate, resolved promptly.

16. Training, monitoring and review

- Authorised users must receive role-appropriate training before access is granted and periodically thereafter.
- Training must cover purpose limitation, confidentiality, secure handling, disclosures, subject rights, incident reporting and misuse.
- The Facilities lead must periodically review access permissions, logs, signage, camera positioning, time accuracy, retention and deletion controls.
- The Data Protection lead must support periodic review of LIAs, DPIAs, privacy information, records of processing and processor arrangements.
- The continued need for each surveillance system must be reviewed at least annually. Systems that no longer meet a necessary and proportionate purpose must be changed, suspended or removed.
- This policy must be reviewed at least annually and sooner following a material change, complaint, breach, legal development or significant audit finding.

17. Related documents and records

- Data Protection Policy and privacy notices.
- Subject Access Request and Request for Information procedure.
- Personal Data Breach Procedure and IT incident response arrangements.
- Records Retention Schedule.

- CCTV LIA, DPIA, Asset Register, Contact Register, access logs, disclosure logs and preservation records.
- Processor contracts, security assessments and international-transfer documentation where applicable.
- Safeguarding, Health and Safety, disciplinary, grievance and complaints procedures.

Appendix A - Operational control checklist

Control	Owner	Evidence
Approved purpose and lawful basis documented.	Data Protection lead / system owner	LIA and, where required, DPIA
Camera location and field of view remain necessary and proportionate.	Facilities lead	Asset Register and review record
Signage is visible before entry to the monitored area.	Facilities lead	Site check and photographs
Audio and unapproved analytics are disabled.	Facilities lead / IT	Configuration check
Access is restricted and current.	Facilities lead	Access list and log review
Date, time and image quality are accurate.	Facilities lead	System check
Thirty-day routine retention and secure deletion operate correctly.	Facilities lead	Configuration and deletion test
Exports and disclosures are minimised, authorised and logged.	Authorised user	Disclosure or evidence log
Processor, cloud and transfer controls remain appropriate.	System owner / Data Protection lead	Contract and assessment
Incidents and rights requests are escalated promptly.	All authorised users	Case record
Annual necessity and effectiveness review completed.	Policy owner	Annual review record

Appendix B - Change log

Section	Issue	Amendment	Priority
1-2	Scope and status required clearer coverage.	Clarified overt-surveillance scope, audiences, technologies and exclusion of covert monitoring.	High
4	Responsibilities were distributed but escalation and deputies were not explicit.	Defined governance roles, operational ownership, authorised-user duties and controlled contact register.	High

Section	Issue	Amendment	Priority
5	Lawful basis was not expressly documented.	Added Article 6(1)(f) legitimate interests, LIA requirement and controls for sensitive processing.	Critical
6-7	Necessity, placement and layered transparency needed strengthening.	Added less-intrusive alternatives, privacy-sensitive locations, consultation and privacy-notice requirements.	High
8-9	Access, audit, audio and advanced technology controls were incomplete.	Added role-based access, audit logs, secure exports, audio default-off and approval for analytics or biometrics.	High
10	Retention was stated but preservation governance needed detail.	Retained 30-day period and added preservation, review and deletion evidence.	Medium
11	Disclosure controls required a clearer audit trail.	Added verification, approval, secure transfer and disclosure-log requirements.	High
12	PIA terminology and system accountability were outdated.	Replaced PIA with DPIA and added LIA, change triggers and CCTV Asset Register.	High
13	Individual-rights handling needed fuller operational detail.	Added search, redaction, preservation and decision requirements.	High
14	No explicit surveillance breach process.	Added immediate reporting, containment, evidence and risk-assessment requirements.	High
16	Review and training frequency were not operationally specific.	Added role-based training, periodic controls and annual necessity and policy reviews.	Medium

Policy control

Version Control Number	Realise-08-PD-105
Version	V3
Last Review Date	01/10/26
Next Review Date	01/10/27
Policy Owner	Patrick Richter IT Manager
Signed by Managing Director	 Gregg Scott Realise Managing Director