

The ReConnect Programme – CCTV Policy

OWNERSHIP:	The ReConnect Programme
AUTHORISED BY:	Chief Operating Officer
REVIEW:	August 2027

Purpose

The purpose of this policy is to ensure that Closed Circuit Television (CCTV) and other approved video-surveillance systems used by The ReConnect Programme are necessary, proportionate, secure and operated transparently. CCTV supports safety, safeguarding, security and the prevention and investigation of crime, but does not replace effective staffing, supervision, safeguarding practice or site management.

Scope

This policy applies to all CCTV systems controlled by The ReConnect Programme and to all employees, workers, contractors, volunteers, young people, parents, carers and visitors whose images may be captured. It covers fixed cameras, live viewing, recorded footage, exported stills or clips and any separately approved vehicle, doorbell, body-worn or mobile surveillance system.

Any dashcam, body-worn camera, facial recognition, biometric analysis, automated behaviour detection or other enhanced capability requires separate written approval, a specific assessment and additional operating instructions before use.

Policy Context

AP context (non-school AP): The ReConnect Programme operates as a non-school Alternative Provision (AP). CCTV is used within a setting attended by children and young people, including individuals with SEND, SEMH needs or heightened vulnerability. Camera use must therefore balance safety and safeguarding benefits against privacy, dignity, communication needs and the risk that surveillance could affect trust or behaviour. The ReConnect Programme Ltd is the data controller for CCTV systems it controls.

Policy Statement

ReConnect will operate CCTV in accordance with the UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025 and current Information Commissioner's Office guidance. We also have regard to the principles in the Surveillance Camera Code of Practice as a good-practice benchmark where relevant.

CCTV will be used only for clearly defined purposes. Cameras will not be introduced simply because the technology is available or used for general curiosity, routine observation of young people, excessive staff monitoring, measuring productivity or any purpose incompatible with the stated reason for collection.

POLICY

Purposes of CCTV

CCTV may be used where necessary and proportionate to:

- protect the safety and welfare of young people, staff, contractors and visitors
- support safeguarding and the appropriate investigation of significant incidents or allegations
- deter, prevent and detect crime, trespass, vandalism, theft and unauthorised access
- protect buildings, vehicles, equipment and other assets
- support health and safety, emergency response and investigation of serious accidents or unsafe events
- assist the police or another authorised body with a lawful and proportionate investigation
- establish facts relevant to a complaint, disciplinary matter, insurance claim or legal proceeding where use of footage is fair and consistent with the original purpose or another lawful basis

Footage will not normally be used for a new purpose that people would not reasonably expect. Any proposed new use must be assessed and documented before it begins.

Lawful Basis

ReConnect normally relies on legitimate interests under Article 6(1)(f) UK GDPR for proportionate safety, safeguarding, security, crime-prevention and property-protection purposes. A Legitimate Interests Assessment will document the purpose, necessity, alternatives, expected benefits, impact on individuals and safeguards.

Another lawful basis may apply to a particular disclosure or use, such as legal obligation, vital interests or the establishment, exercise or defence of legal claims. Consent is not normally an appropriate basis for general CCTV because individuals cannot freely avoid the monitoring while using the site.

Where footage reveals special category or criminal offence information and ReConnect intentionally uses it for a decision or investigation, the additional legal conditions will be identified and recorded.

Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) will be completed before a new CCTV system or materially changed deployment begins where the processing is likely to create a high risk. ReConnect will in any event complete and retain a proportionate assessment for its CCTV arrangements.

The assessment will consider:

- the precise problem and evidence that surveillance is needed
- whether less intrusive measures could achieve the purpose
- camera location, angle, field of view, operating hours and image quality
- the impact on young people, staff, neighbours, visitors and public areas

whether audio, zoom, analytics, remote access or cloud storage is proposed
lawful basis, signage, retention, access, disclosure and security
consultation with staff or others where appropriate
measures to reduce privacy and safeguarding risks

The DPIA and Legitimate Interests Assessment will be reviewed when cameras are added, moved or upgraded, purposes change, new technology is enabled, a serious concern occurs or periodic review identifies a need.

CCTV System Register

The Data Protection Lead will maintain a restricted CCTV System Register. It will record each camera or device, its location, field of view, purpose, operating hours, whether recording is continuous or event-triggered, whether audio is disabled, storage location, normal retention, system owner, authorised users and date of last review.

The public policy will not normally publish a detailed camera map where doing so could create a security risk. Sufficient privacy information will nevertheless be provided through signs and notices.

Camera Positioning

Cameras will be positioned only where the intended purpose justifies surveillance.

The field of view will be limited to relevant ReConnect premises, entrances, exits, access routes, car parks, boundaries, communal areas and higher-risk operational spaces approved through assessment.

Cameras will be adjusted, masked or privacy-zoned where practicable to avoid neighbouring properties, private gardens, public areas or spaces outside ReConnect's control.

Cameras must provide an image suitable for the stated purpose without capturing unnecessary detail. Portable, hidden, dummy or staff-installed personal cameras are prohibited unless expressly approved under this policy.

Camera locations will be reviewed to ensure that changes to rooms, activities or buildings have not made the surveillance excessive or ineffective.

Areas of Heightened Privacy

Cameras will not be installed in toilets, changing rooms, showers, medical examination areas, counselling rooms or other spaces where there is a strong expectation of privacy. Surveillance will not normally be used in staff rest areas or rooms used for confidential meetings.

Exceptionally, surveillance near a heightened-privacy area may be considered only where there is compelling evidence of a serious risk, no less intrusive option is effective, a specific DPIA is completed, senior approval is recorded, the field of view excludes the private activity and clear additional safeguards are in place. Covert surveillance will never be used in toilets or changing rooms.

Audio Recording

Audio recording is disabled by default. Continuous recording of face-to-face conversations is substantially more intrusive than video and will not be activated as part of ordinary CCTV operations.

Any exceptional proposal to record audio requires a documented and compelling need, confirmation that less intrusive measures are inadequate, a specific DPIA, legal review where appropriate, senior approval, clear notification and tightly limited activation. The same controls apply to audio within vehicles.

Signage and Transparency

Clear signs will be placed before or at entry to monitored areas and, where necessary, within the site. Signs will be visible, readable and accessible and will normally state:

- that CCTV is in operation

- the main purpose of monitoring

- that The ReConnect Programme Ltd is the data controller

- how to obtain further information or contact the Data Protection Lead

Additional privacy information will be available through the ReConnect Privacy Policy, website, parent and carer information and staff privacy information. Young people will receive an age-appropriate explanation where needed.

Roles and Responsibilities

Chief Operating Officer and Directors

- Approve the CCTV purposes, budget, system design and significant changes.

- Ensure that CCTV remains necessary, proportionate and appropriately governed.

- Approve any exceptional covert surveillance or audio proposal after required assessment and advice.

Data Protection Lead

- Maintain the CCTV System Register, DPIA, Legitimate Interests Assessment, authorised-user list and access or disclosure logs.

- Coordinate subject access requests, complaints, disclosures and data breaches.

- Review compliance, retention, signage, processor arrangements and system changes.

- Provide advice and training to authorised users.

System Owner or Site Manager

- Ensure day-to-day system security, maintenance, time and date accuracy and fault reporting.

- Confirm that cameras retain the approved field of view and privacy masking.

Ensure that faults, unauthorised access and security incidents are escalated promptly.

Authorised Users

Access footage only for an approved purpose and only to the minimum extent necessary.

Keep footage and information confidential and never use personal devices to record screens.

Complete the access or disclosure log and follow export, storage and deletion controls.

Report suspected misuse, loss, disclosure or system compromise immediately.

Live Viewing and Recorded Access

Live viewing and playback are restricted to named, trained and authorised roles. Access will be role-based and protected by individual credentials, strong passwords and multi-factor authentication where available. Shared accounts should not be used where the system supports named accounts.

Viewing must take place in a secure location where unauthorised people cannot see the screen. Footage will not be played in front of young people, staff, parents, visitors or other witnesses unless this is necessary, fair and authorised for a specific purpose. Curiosity, informal review or searching for unrelated conduct is prohibited.

The system or accompanying log will record, so far as practicable:

- date and time of access

- name and role of the person accessing footage

- reason and lawful purpose

- camera, time period and footage viewed

- any export, disclosure, redaction or deletion action

Safeguarding and Allegations

CCTV may support a safeguarding enquiry but must not delay an immediate response. Any person who sees or becomes aware of a safeguarding concern must report it promptly to the Designated Safeguarding Lead in accordance with the Safeguarding and Child Protection Policy. The DSL will coordinate with the Data Protection Lead and Head of Provision regarding preservation and controlled access to relevant footage.

Where an allegation concerns a member of staff, access will be restricted to those who need it and the matter will be managed under the allegations procedure, including referral to the appropriate external authority where required. Footage must not be shown to the subject of an allegation, witnesses or colleagues in a way that could contaminate evidence or compromise welfare.

A young person's distress, disability, SEND, communication style or behaviour will be considered when interpreting footage. Video may show what occurred but not always the context, intent, sensory experience or events outside the camera's field of view.

Staff Monitoring and Employment Matters

Staff will be told about the nature and purpose of workplace CCTV. Security footage will not routinely be repurposed to monitor productivity, minor performance matters or general compliance where staff were not informed that this was a purpose.

Footage may be used in a disciplinary, grievance, complaint or health and safety investigation where the use is necessary, proportionate, fair, within the stated purpose or supported by a documented compatible purpose, and the individual's rights have been considered. Relevant HR and staff privacy procedures will be followed.

Recording, Storage and Security

Footage will be stored only on approved, secured equipment or services.

Recording units, administrator consoles and network equipment will be physically and technically protected.

Remote access will be disabled unless required and specifically secured.

Exports will use encrypted or otherwise approved storage and be tracked from creation to deletion.

Footage will not be sent through personal email, consumer messaging services or unapproved cloud storage.

Suppliers with system access will be subject to due diligence, confidentiality and an Article 28 processor contract where applicable.

Security updates, backups, account reviews and maintenance will be managed proportionately to system risk.

Retention and Preservation

Recorded CCTV footage will normally be retained for no longer than 30 days and will then be automatically and securely overwritten or deleted. A shorter period will be used where it adequately meets the purpose. The exact period for each system will be recorded in the CCTV System Register and privacy information.

Relevant footage may be preserved for longer when required for a specific safeguarding matter, incident, complaint, disciplinary process, police request, insurance claim, legal proceeding or rights request. A preservation record will identify the reason, footage, owner, access restrictions, review date and final deletion decision. Preserved footage will not be kept indefinitely.

Exporting Footage

Only authorised users may export a clip or still image. The export must be limited to the relevant camera and time period, checked for third-party information, securely named and stored, and entered in the export log. Where evidential integrity matters, the original should be protected from alteration and a working copy used for review or redaction.

Subject Access Requests

A person may request access to CCTV footage containing their personal information. Requests may be verbal or written and should be sent promptly to the Data Protection Lead. To help locate footage, we may ask for the approximate date, time, location, clothing or other identifying information and may verify identity or authority.

We will respond within the applicable legal timeframe. Where clarification is reasonably required, the response period may be paused in accordance with current law until the requested information is received. Footage involving other people will be redacted, masked or withheld where necessary to protect their rights, unless disclosure is otherwise lawful. Applicable exemptions, including crime-prevention and safeguarding exemptions, will be considered and documented.

Requests on behalf of a child will be considered in light of the child's competence, best interests, parental responsibility and safeguarding circumstances. A parent or carer does not automatically have an unrestricted right to footage of a child or other people.

Requests From Police and Other Authorities

Police and statutory requests will not be treated as automatically valid. The Data Protection Lead or authorised senior manager will confirm the identity of the requester and obtain a written request or reliable record stating the purpose, legal basis, incident, date and time range, cameras required and urgency.

Disclosure will be limited to footage that is necessary and proportionate. An audit record will document the recipient, authority, purpose, footage released, method, date and decision-maker. Emergency disclosure may be made where necessary to protect life or respond to an immediate serious risk, with the rationale recorded as soon as practicable.

Other Disclosures

Footage may be disclosed to insurers, legal advisers, courts, safeguarding partners, regulators or another third party only where a clear lawful basis applies. Court orders will be complied with, subject to verification and legal advice where appropriate. Footage will not be released for entertainment, social media, informal circulation, commercial use or publication unless there is an exceptional and lawful reason supported by senior approval.

Covert Surveillance

Covert surveillance is highly intrusive and will be considered only in exceptional circumstances where there are reasonable grounds to suspect serious criminal activity or comparably serious misconduct, informing people would prejudice the investigation, and no less intrusive measure is effective.

Before covert surveillance begins, ReConnect must complete a specific DPIA, define the exact purpose, people or area, duration, authorisation, access controls, review point and deletion arrangements, and obtain written approval from a Director. Legal or specialist advice will be obtained where appropriate. Surveillance will be targeted, time-limited and stopped immediately when the purpose is achieved or it is no longer justified.

Covert monitoring will not be used in toilets or changing rooms and will not be used to capture private communications except where lawful, strictly necessary and supported by exceptional justification and advice.

System Maintenance and Quality

The system owner will complete and record proportionate checks of:

- camera operation, obstruction, damage and field of view
- recording, playback, storage capacity and overwrite function
- date and time accuracy
- signage and privacy masking
- user accounts, remote access and security settings
- image quality sufficient for the approved purpose
- faults, repairs and changes

A fault that materially affects safety, security, privacy or evidential integrity will be escalated promptly. Temporary alternative controls will be considered until repair is complete.

Data Breaches and Misuse

Loss, unauthorised viewing, sharing, copying, alteration, hacking or accidental disclosure of footage is a personal data incident and must be reported immediately under the Data Breach Procedure. ReConnect will contain and investigate the incident, assess risk, preserve evidence and notify the Information Commissioner's Office or affected people where legally required.

Misuse may result in withdrawal of access, disciplinary action, termination of contract, safeguarding referral, police report or other legal action. Staff must not photograph CCTV screens or share clips through personal devices or accounts.

Complaints

Concerns about CCTV should be raised with the Data Protection Lead through admin@reconnect1-1.com or 07599 035520 and may also be progressed under the Complaints Policy. Individuals may complain to the Information Commissioner's Office at www.ico.org.uk or 0303 123 1113. Safeguarding concerns must be reported immediately and must not wait for the complaints process.

Monitoring and Review

This policy and each CCTV deployment will be reviewed at least annually. Review will consider whether the original problem still exists, whether the cameras remain effective and proportionate, complaints, requests, incidents, disclosures, system security, retention, signage, changes in law or guidance and whether a less intrusive measure is now available. Cameras that are no longer justified will be removed or deactivated.

Appendix A: CCTV Access and Disclosure Log

Field	Record required
Request or access date	Date and time received or accessed.
Requester / authorised user	Name, role, organisation and verified identity where relevant.
Purpose and lawful basis	Specific reason, authority and necessity.
Footage	Camera, location, date and exact time range.
Action	Viewed, preserved, exported, redacted, disclosed, refused or deleted.
Recipient and method	Person or organisation receiving footage and secure transfer method.
Decision	Approver, rationale, restrictions and any exemption.
Review / deletion	Preservation review date and confirmed deletion date.

Appendix B: CCTV Signage Minimum Content

CCTV is in operation.

Purpose: safety, safeguarding, security and prevention or detection of crime, as applicable to the location.

Data controller: The ReConnect Programme Ltd.

Contact: admin@reconnect1-1.com or 07599 035520.

Further privacy information: www.reconnect1-1.com.

Appendix C: Legal and Organisational Framework

UK General Data Protection Regulation

Data Protection Act 2018

Data (Use and Access) Act 2025

Protection of Freedoms Act 2012 and Surveillance Camera Code of Practice, where applicable or adopted as good practice

Human Rights Act 1998

ICO guidance on video surveillance and monitoring workers

ReConnect Privacy Policy, Data Protection Policy, Data Breach Procedure, Information Security Policy, Safeguarding and Child Protection Policy, Staff Code of Conduct, Complaints Policy and Records Retention Schedule

VERSION CONTROL

We will review our documentation regularly and we reserve the right to amend our policies and

procedures at any time.

Version	Date	Change Summary	Author/ Reviewer	Approved by:
1	29/08/2026	Initial Version	Naomi Hamer	Director