RLT CCTV Policy

Adopted: Spring Term 2026

Review period: Annually

Statutory: No

Required on website: No

THE ROWAN LEARNING TRUST

Policy Document Version Control

Version 1

Responsibility for Policy:	Data Protection Officer
Policy approval/date:	Summer term 2026
Frequency of Review:	Annual
Next Review date:	Summer term 2027
Related Policies:	Data Protection Policy Records Management & Retention Policy Information Security Policy Cybersecurity Policy Freedom of Information (FOI) Policy Data Breach Management Policy Acceptable Use Policies (Staff, Pupils, Governors) Online Safety Safeguarding & Child Protection Policy Behaviour Policy Staff Code of Conduct Whistleblowing Policy Health & Safety Policy Premises Management Policy
Minor Revisions:	
Major changes	
Full re-write	This policy is new. It is an overarching RLT policy that ensures that our schools are compliant with all relevant related policies and current legislation. All processes will sit at school level.

1. Policy Aim

This policy mandates that all CCTV systems operated across the Rowan Learning Trust (RLT) are deployed and managed in a manner that is *lawful, necessary, proportionate and accountable*. It establishes a Trust-wide framework ensuring that surveillance activities:

- uphold and evidence full compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, including the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation and security as set out in the ICO's statutory guidance on video surveillance systems
- align with and operationalise the Home Office Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012, ensuring that every deployment meets the Code's expectations of clear purpose, robust governance, proportionality, transparency and continual review
- support RLT's safeguarding duties, ensuring that CCTV contributes directly to creating a safe and secure environment for pupils, staff and visitors, in line with statutory obligations under the Department for Education's safeguarding framework
- respect the rights and freedoms of individuals, particularly the Article 8 right to private and family life under the Human Rights Act 1998, by ensuring that surveillance is never excessive, intrusive or unjustified, and is always subject to documented necessity and proportionality assessments

Through this policy, RLT ensures that CCTV is used only where it is the least intrusive and most effective security and safeguarding measure available, supported by rigorous governance, Data Protection Impact Assessments (DPIAs), clear accountability structures, secure technical controls, and transparent communication with data subjects. The policy establishes the standards by which all staff must operate to maintain public trust, safeguard community members, and protect the Trust's estate while ensuring legal and ethical compliance at all times.

CCTV operation must be considered alongside the Trust's wider safeguarding responsibilities, including managing risks associated with online safety, digital harms, disinformation and cyber-security as identified in KCSIE latest version.

2. Executive Summary

The Rowan Learning Trust (RLT) operates Closed Circuit Television (CCTV) as a critical safeguarding, security and governance control. Its purpose is to ensure the safety and welfare of pupils, staff and visitors; to protect Trust property and infrastructure; and to support the prevention, deterrence and detection of crime and misconduct. These functions align directly with the expectations set out in the ICO's guidance for organisations operating video surveillance systems, which emphasises the need for lawful, transparent and accountable processing of personal data.

All CCTV deployments across RLT must be demonstrably necessary, proportionate, justified and risk-assessed. No system may be installed, expanded or materially altered without a completed and approved Data Protection Impact Assessment (DPIA) that evidences the legitimate purpose of the deployment, evaluates less intrusive alternatives, defines clear operational boundaries, and sets out appropriate technical and organisational safeguards in accordance with the UK GDPR's data protection by design and default requirements.

CCTV operation within RLT forms a core component of the Trust's wider safeguarding and security framework. Accordingly, the Trust is committed to ensuring that all CCTV use is subject to robust governance, including strict access controls, secure configuration, auditable oversight, and regular performance/relevance reviews, ensuring each system continues to meet the regulatory expectations for accountability and necessity.

3. Policy Statement

RLT shall operate CCTV in accordance with:

- UK GDPR and Data Protection Act 2018 – adhering to the principles in Article 5(1) (lawfulness, fairness & transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity & confidentiality; accountability) and implementing appropriate technical and organisational measures
- ICO Video Surveillance (CCTV) Guidance – governance, DPIA, signage, access, disclosure, retention and security requirements for controllers using CCTV
- Surveillance Camera Code of Practice (Home Office), issued under PoFA 2012 – applying the 12 guiding principles (necessity, proportionality, transparency, governance, data quality and security)
- Human Rights Act 1998 (Article 8) – ensuring any interference with the right to respect for private and family life is lawful, necessary and proportionate to the risk being addressed
- DfE safeguarding expectations – KCSIE (2025) – ensuring a safe environment and strong leadership oversight of monitoring/safeguarding systems (including alignment with DfE digital standards for filtering/monitoring where relevant to wider safeguarding governance)

Lawful basis. RLT will only process CCTV data where a lawful basis applies—normally Article 6(1)(e) UK GDPR (public task/official authority) for maintained/academy trusts and, where appropriate, Article 6(1)(f) (legitimate interests)—and will record this in the Record of Processing and privacy notices. Where special category data is incidentally captured, an Article 9 condition will be identified and documented.

Annual assurance. The DPO will conduct an annual compliance review covering necessity/proportionality, DPIA currency, signage, logs, access controls, retention, disclosures and training, reporting findings to the Trust's governance committees.
RLT shall undertake an annual, Trust-wide self-assessment against the 12 guiding principles of the Home Office Surveillance Camera Code of Practice.
The assessment will use the Home Office's "Guide to the 12 Principles" framework and shall evaluate necessity, proportionality, transparency, governance, data quality, security and continued justification for each CCTV deployment.

A publishable summary of the assessment will be made available on the RLT website to support transparency and public accountability. Outcomes, required improvements and implementation deadlines shall be reported to the Audit & Risk Committee and retained for audit.

4. Scope

This policy applies to the operation, governance, monitoring, maintenance, oversight and use of all fixed CCTV systems deployed by the Rowan Learning Trust (RLT) across all Trust-managed sites, buildings, external grounds, learning environments, satellite facilities, and any location where Trust-owned CCTV equipment is installed or used. It governs the full lifecycle of CCTV processing, including recording, viewing, access, disclosure, retention, deletion, security controls, and DPIA-driven change management. This aligns with the ICO's requirements that organisations ensure CCTV operations are subject to clear, comprehensive and transparent governance arrangements.

The policy applies to all Trust employees, contractors, authorised third-party service providers, and any individual acting on behalf of RLT who has responsibility for the deployment, operation or oversight of CCTV systems. This includes IT, estates, safeguarding, leadership and compliance functions, in line with the need for clearly defined roles and responsibilities within the operation of surveillance systems.

The policy includes all static, fixed-installation cameras, associated network video recorders (NVRs), servers, software platforms, storage devices, and any integrated security systems used for capturing or processing CCTV footage. It also extends to relevant signage, system documentation, viewing terminals, and the operational processes attached to them.

Exclusions and Boundary Clarifications

This policy does not apply to:

- web-conferencing, classroom camera, or audio-visual equipment used for teaching, learning, hybrid meetings or remote engagement, where such equipment is not used for surveillance or monitoring. The ICO differentiates clearly between video conferencing technologies and surveillance systems, and only the latter fall under CCTV governance
- online filtering and digital monitoring systems used to safeguard pupils' online activity or ensure compliance with digital standards. These are governed separately under RLT's IT Security, Online Safety, and Filtering & Monitoring Standards, in line with Department for Education guidance on
- digital monitoring technologies
- ad-hoc, personal or temporary recording devices, including mobile phones or portable cameras, unless formally designated as part of an authorised CCTV deployment

Authority and Applicability

All systems, processes and decisions covered by this policy must comply with:

- UK GDPR / DPA 2018 governance requirements for surveillance systems
- The ICO's Video Surveillance Guidance on lawful, fair and transparent processing
- The Home Office Surveillance Camera Code of Practice (necessity, proportionality, transparency, governance and review)
- RLT's safeguarding, security, estates and data protection frameworks

No CCTV activity is permitted outside this scope without explicit DPO approval, an updated DPIA and formal authorisation from Trust leadership.

5. Roles and Responsibilities

Effective governance of CCTV systems requires clearly defined responsibilities, robust oversight, and a demonstrable accountability framework. The following roles carry non-delegable obligations to ensure that all surveillance activities across the Rowan Learning Trust (RLT) meet statutory, regulatory and ethical standards.

a) Trust Board / Audit & Risk Committee (Strategic Governance & Oversight)

The Trust Board and its Audit & Risk Committee shall provide strategic oversight and independent assurance that the deployment and ongoing operation of CCTV systems remain necessary, proportionate, transparent and compliant with the Home Office Surveillance Camera Code of Practice's governance principles.

Their responsibilities include:

- Approving the overarching CCTV governance framework and ensuring it integrates with safeguarding, risk, estates and data-protection strategies.
- Reviewing annual assurance reporting from the DPO and the Director of Risk

& Compliance.

- challenging deployments that lack a clear purpose, DPIA justification or evidential benefit.
- ensuring leadership sets the tone for lawful and ethical surveillance practice.

b) Chief Executive / Director of Risk & Compliance (Policy Owner & Senior Responsible Officer)

The Chief Executive and Director of Risk & Compliance act as Senior Responsible Officers for CCTV governance. They shall:

- ensure effective implementation of this policy across all academies and services
- allocate appropriate resources, training and technical capability to maintain compliance
- ensure prompt corrective actions when non-compliance or governance gaps are identified
- oversee reporting to the Board and external regulators, where required

c) Data Protection Officer (DPO) - Statutory Compliance Lead

The DPO provides independent oversight of CCTV processing, in accordance with the UK GDPR and ICO Video Surveillance Guidance.

The DPO shall:

- advise on and approve lawful bases, DPIAs, signage content and transparency measures
- maintain the CCTV Asset Register, including all camera locations, system purposes, and related DPIA records
- Maintain and audit the Authorised Viewers Register, ensuring strict role-based access
- maintain a Processing & Disclosure Log documenting all footage access, downloads, disclosures and justifications
- monitor compliance with retention periods and security controls, escalating risks or breaches
- provide independent advice on necessity, proportionality, and governance reviews

d) Headteachers / Principals (Operational Accountability at Site Level)

Headteachers and Principals hold operational responsibility for ensuring that CCTV systems at their site are used lawfully, securely and in accordance with this policy.

They shall:

- implement local Standard Operating Procedures (SOPs) consistent with Trust requirements
- ensure that only authorised and trained staff access or view CCTV footage, and that all access is fully logged and auditable
- ensure signage is correctly placed, accurate and maintained

- respond appropriately to safeguarding, behaviour, security and welfare incidents requiring CCTV review
- report any suspected misuse, security incident or non-compliance to the DPO immediately
- each academy shall complete the ICO CCTV self-assessment checklist annually and following any significant system change. The completed assessment must be submitted to the DPO, who will review findings, document remedial actions and track closure to completion
- this process evidences compliance with ICO expectations around DPIAs, signage, public awareness, retention, image quality, access controls, governance and security. Results form part of the Trust's annual CCTV assurance report to the Audit & Risk Committee

e) Safeguarding Governance Alignment

CCTV governance and assurance shall be integrated into the academy's wider safeguarding oversight. Headteachers/Principals and the DSL must coordinate CCTV assurance with compliance against DfE filtering and monitoring standards, ensuring governors receive a single, coherent safeguarding assurance picture.

This alignment reflects national expectations for leadership oversight of monitoring technologies, risk management and safeguarding systems, as emphasised in DfE digital safety guidance and contemporary best practice surrounding monitoring and access control oversight. This includes alignment with KCSIE latest version, expectations regarding cyber-security, filtering & monitoring oversight, and the management of digital harms and misinformation as safeguarding risks.

f) IT & Site Teams / Approved Contractors (Technical & Physical Security Leads)
IT and Site Teams, along with approved contractors, provide the technical and physical controls that secure CCTV systems, in alignment with data-security requirements under UK GDPR Article 32 and ICO operational expectations.

They shall:

- install, configure and maintain all CCTV hardware and software to Trust standards, ensuring system integrity and reliability
- implement and enforce role-based access control, multi-factor authentication (where supported), encryption at rest and in transit, and

robust audit logs

- ensure that all systems are patched, updated and protected against unauthorised access or tampering
- maintain secure storage environments for servers/NVRs and ensure environmental risks (e.g., overheating, moisture) are controlled

- record all maintenance, configuration changes and technical incidents in the CCTV Technical Log
- notify the DPO and Director of Risk & Compliance of any security vulnerabilities or failures

g) All Authorised Staff (Responsible Users & Custodians of Access)
All staff authorised to access or review CCTV footage carry personal accountability for safeguarding the confidentiality, integrity, accuracy and lawful use of recorded images.

They shall:

- access CCTV systems only for legitimate purposes defined within this policy
- complete mandatory training on CCTV governance, lawful processing, security expectations and incident reporting
- prevent any form of unauthorised disclosure, sharing or misuse of footage
- immediately report suspected misuse, attempted unauthorised access or system anomalies to their Headteacher/Principal or the DPO
- uphold the privacy rights of all individuals whose data is captured by CCTV

h) External Agencies (Law Enforcement & Legal Representatives)
While not internal roles, third-party agencies interacting with RLT CCTV systems shall be subject to strict controls.

- disclosures shall only be made to law-enforcement or authorised legal representatives where a lawful basis, necessity and proportionality are established, in line with ICO surveillance disclosure guidance
- all disclosures must be recorded in the Disclosure Log maintained by the DPO

6. CCTV KPIs and Assurance Metrics

To demonstrate accountability and maintain consistent standards across the Trust, the following Key Performance Indicators (KPIs) apply. Site leaders shall report termly to the DPO; the DPO shall provide an annual consolidated assurance report to the Audit & Risk Committee.

- DPIA Coverage - 100% of active cameras must be covered by a DPIA completed or reviewed within the previous 12 months
- signage compliance - 100% of monitored entrances and internal coverage areas must display ICO-compliant signage at all times
- access control integrity - 0% shared credentials; 100% of authorised viewers reviewed termly; 100% of access, viewing and export events recorded with purpose and legal basis
- security baseline compliance -100% of systems must comply with required

- security measures (unique credentials, multi-factor authentication where supported, encryption in transit and at rest, patching, NTP-accurate timestamps)
- disclosure Timeliness - Lawful police requests fulfilled within ≤5 working days, unless an alternative statutory route requires a faster response.
- SAR / FOI Compliance - 100% of Subject Access Requests and FOI requests handled within statutory timeframes; all redactions and supervised viewings fully documented
- annual self-assessments completed - 100% completion of the ICO CCTV self-assessment and the Home Office 12-principles assessment at each site
- failure to meet KPIs shall trigger corrective actions with defined owners, timescales and escalation via the Director of Risk & Compliance where necessary.

7. System Description – Fixed Cameras

RLT deploys fixed, overt surveillance cameras as part of a structured and formally governed CCTV estate. All cameras must be installed, positioned, configured, operated and maintained in strict accordance with legal, technical and privacy requirements. The system is designed to ensure that surveillance is effective, justified, proportionate and minimally intrusive, in line with the ICO's expectations for video surveillance systems.

a) Standard Camera Coverage

Fixed CCTV cameras are installed only where they serve a clearly evidenced and legitimate purpose. Standard coverage includes:

- entrances and exits (including delivery/visitor access points)
- car parks and on-site roadways
- perimeter lines and boundary fences
- external circulation and recreation areas
- internal circulation routes, including corridors and stairwells
- reception and lobby areas
- communal spaces, such as dining halls, social areas and waiting zones
- high-value rooms, including ICT suites, server rooms and secure storage areas

Camera placement must always reflect necessity, proportionality and data-minimisation principles, ensuring only areas required for the stated security and safeguarding purposes are captured.

b) Risk-Assessed Classroom Coverage

Classroom coverage is not standard practice and may only be approved where a documented and high-risk justification exists—such as significant safeguarding threats, repeated serious incidents, or specialist provision environments.

Any classroom camera deployment must:

- undergo a full DPIA with DPO approval
- demonstrate that no less intrusive measures are adequate
- be reviewed at least termly to confirm ongoing necessity

This reflects the higher privacy expectations in learning spaces and the Article 8 requirement to avoid unjustified intrusion into private life.

c) Prohibited Locations

No cameras may be installed in areas where individuals have a reasonable expectation of privacy, including but not limited to:

- toilets
- changing rooms

The prohibition aligns with both the ICO's guidance on intrusive surveillance and the Human Rights Act 1998's requirement that interference with privacy be lawful, necessary and proportionate.

d) Signage and Transparency Requirements

All CCTV coverage areas must display ICO-compliant signage, which:

- is clearly visible and readable at entry points
- identifies RLT as the data controller
- states the purpose(s) of surveillance
- provides contact details for further information or rights requests

This satisfies the UK GDPR transparency obligation and ICO guidance for overt surveillance.

e) Exceptional Deployments (Sensitive Areas)

In rare and exceptional circumstances—such as cases involving serious safeguarding risks deployment of cameras in sensitive but not private areas may be authorised.

Such deployments must:

- be justified by an exceptional and evidenced need
- be strictly time-limited
- apply privacy masking or restricted fields of view wherever possible
- undergo a full DPIA detailing necessity, proportionality, risks and mitigations
- receive written approval from the DPO
- be logged in the CCTV Asset Register

This ensures exceptional surveillance is never normalised and always rigorously governed.

f) Prohibition of Covert Surveillance

- RLT does not operate covert CCTV.
- covert surveillance is prohibited under this policy and may only be used by law-enforcement agencies under separate statutory frameworks. The Trust operates overt surveillance exclusively, which does not fall within the scope of RIPA (Regulation of Investigatory Powers Act)

This complies with the principle that covert surveillance in educational settings is inherently intrusive and incompatible with Article 8 unless authorised by appropriate legal authorities.

g) Technical Configuration

All fixed cameras shall be configured to:

- capture the minimum area necessary
- avoid private areas through privacy masking
- maintain accurate date/time metadata
- use fixed fields of view, preventing manual manipulation that could result in unnecessary intrusion
- record at a quality suitable for evidential use while upholding data-minimisation principles

Technical configuration standards directly follow ICO guidance on ensuring data quality and minimisation.

8. System Description – Fixed Cameras (Enhanced, Compliance-Led)

Control objective. RLT operates fixed, overt CCTV to provide reliable, proportionate and minimally intrusive surveillance that demonstrably meets legitimate safeguarding and security aims while upholding UK GDPR principles, the Surveillance Camera Code of Practice and Article 8 ECHR (HRA 1998).

a) Coverage principles & siting controls

All fixed cameras shall be sited and configured according to the following principles:

- necessity & proportionality. Placement must be purpose-driven (e.g., crime prevention, safeguarding, asset protection) and record only what is necessary to achieve that purpose. Alternative, less intrusive measures must be considered and discounted within the DPIA.
- data minimisation by design. Fields of view (FoV) must be limited to relevant areas; privacy masking shall be used where adjacent areas are not necessary (e.g., private windows, neighbouring property, or staff-only rooms not relevant to the risk).
- standard coverage categories & purpose mapping:
  - External perimeters & car parks – deter/detect trespass, theft, criminal damage, anti-social behaviour; support safe arrivals/departures
  - Entrances, exits & receptions – control of access/egress; verification

of visitor flows; incident investigation

- internal circulation (corridors/stairwells) – incident reconstruction, safeguarding of pupils/staff, route-based risks (e.g., crowding/flight)
- communal spaces (dining/social areas) – safety/welfare monitoring and asset protection (e.g., catering/AV)
- high-value rooms (ICT/server/secure stores) – deter/detect theft or damage to critical systems and assets

Justification: The Surveillance Camera Code requires clear purpose definition, proportionality and transparency for each deployment; the ICO guidance requires video surveillance to be necessary, targeted and configured to minimise intrusion.

b) Prohibited & sensitive locations

- prohibited: No cameras may be installed where there is a reasonable expectation of privacy, including toilets, changing rooms, staff rest areas and medical/first-aid rooms
- sensitive (non-private) areas: If a compelling and evidenced risk exists (e.g., repeated serious incidents in a specific corridor niche), deployments must be strictly justified and tightly configured (privacy masking, narrow FoV, shortest feasible retention) and subject to DPO-approved DPIA and time-limited authorisation

c) Classroom deployments (exceptional, risk-assessed only)

Cameras in classrooms are not standard and shall be considered only where a documented, high-risk safeguarding or security need exists and lesser measures cannot achieve the objective.

Any such deployment must:

- complete a full DPIA evidencing necessity, proportionality, alternatives considered, and safeguards;
- be approved in writing by the DPO and Headteacher;
- involve the DSL in design and review;
- be termly-reviewed to confirm ongoing necessity and to minimise intrusion (e.g., masking, restricted hours)

These controls reflect heightened privacy expectations in learning spaces and the requirement to avoid unjustified interference with Article 8 rights.

d) Transparency & signage

RLT operates overt surveillance only. Prominent signage shall be placed at site entry points and in monitored areas, stating RLT as the controller, the purpose(s) of surveillance, and contact details for information/rights requests. Signage must be clear, visible and intelligible to meet transparency duties.

e) Exceptional deployments & time-limited authorisations
Where exceptional risk necessitates cameras in sensitive (but not private) areas:

- a DPIA must demonstrate exceptional need and explain why less intrusive measures fail
- deployments must be time-limited with a specified review/expiry
- privacy masking and FoV restriction must be applied wherever feasible
- DPO written approval is mandatory
- the CCTV Asset Register shall be updated (location, purpose, DPIA reference, expiry date)
- a decommissioning/rollback plan must be agreed before activation.
  These measures operationalise the Surveillance Camera Code's principles on necessity, proportionality and governance

9. Technical configuration & quality standards

All fixed cameras and recording platforms shall be configured to ensure data quality, security and minimisation:

- FoV & masking: capture is limited to areas necessary for the purpose; masking applied to any surplus areas; digital zoom or angle changes that increase intrusiveness are prohibited unless re-approved via change control/DPIA
- image quality fit for purpose: resolution and frame rate set only as high as necessary to identify events/individuals for the stated aim (e.g., entrance identification vs. general movement monitoring)
- accurate metadata: date/time, camera ID and location must be accurate and synchronised (e.g., NTP) to enable reliable evidential use and accountability
- audio disabled by default: audio capture is not permitted on fixed cameras unless separately justified and approved via DPIA due to its higher intrusiveness
- security controls: unique admin credentials (no defaults), role-based access, strong authentication/MFA (where supported), encryption in transit and at rest, patching and audit logging to meet Article 32 requirements
- maintenance & hardening: physical anti-tamper measures, protected cabling/racks, and documented maintenance with post-maintenance verification of FoV/masking/time sync

10. Commissioning, change & decommissioning

- commissioning: No new camera goes live without (i) approved DPIA, (ii) signage installed, (iii) acceptance testing confirming FoV, masking and metadata, and (iv) updates to the Asset Register and Authorised Viewers Register
- change control: Any material change in location, FoV, purpose, resolution, retention or integration requires DPIA review and DPO approval prior to implementation
- decommissioning: Equipment and media must be securely wiped/destroyed; records updated to reflect removal, satisfying UK GDPR security and accountability duties

11. Asset identification & documentation

Each camera shall have a unique identifier physically and logically mapped to its location, purpose, DPIA reference, retention setting and risk rating within the CCTV Asset Register held by the DPO. This supports transparency, auditability and accountability.

12. Overt operation; prohibition of covert surveillance

RLT does not conduct covert surveillance. The Trust operates overt CCTV exclusively; covert activity requires law-enforcement authorisation under separate statutes and is outside RLT's remit. The Surveillance Camera Code defines overt surveillance and requires transparency for public-facing systems.

13. Ongoing assurance & review

Site leaders shall conduct periodic walk-through checks (signage visibility, camera FoV/masking, time/date accuracy), and sample viewer/disclosure log audits. The DPO's annual review will test ongoing necessity/proportionality and control effectiveness and report to the Audit & Risk Committee.

14. Processor & Supplier Governance (Article 28 UK GDPR)

Where CCTV personal data is processed by an external supplier—including installers, maintenance contractors, remote monitoring centres or hosted video management system providers, RLT shall only engage processors who provide sufficient guarantees of UK GDPR compliance.

All such arrangements must be governed by a written Data Processing Agreement (DPA) meeting Article 28 UK GDPR requirements. Each DPA must:

- specify the subject-matter, duration, nature and purpose of processing
- define the categories of personal data and data subjects
- require processing only on RLT's documented instructions
- impose confidentiality obligations on all authorised persons
- require appropriate technical and organisational security measures, including encryption, access control and patching

- restrict sub-processors, requiring prior authorisation and mandatory flow-down of terms
- require the processor to assist with data subject rights, DPIAs, breaches and regulatory enquiries
- require secure deletion or return of all data at contract end
- grant RLT the right to conduct audits or inspections

The DPO and Procurement shall maintain and periodically review the register of all CCTV-related processors to ensure ongoing compliance with ICO expectations.

15. Regulatory Horizon Scanning – DUAA 2025

RLT recognises that the ICO's Video Surveillance Guidance is undergoing updates following the implementation of the Data (Use and Access) Act 2025. The DPO will monitor all ICO surveillance-related updates and recommend revisions to this policy where changes materially affect legal or regulatory expectations for CCTV governance

16. Addendum

Specifics for Three Towers for consideration not covered in the new policy

a) Camera locations:
- cameras are located in all communal areas of the school, and in classrooms. Camera also cover the immediate external grounds of both sites.
- many internal cameras have audio recording capability. This capability is disabled at hardware level in classrooms and private spaces. Audio recording is enabled in communal areas (corridors, stairwells etc.).
- all external cameras are used to cover school grounds only, and privacy masks are used to obscure any areas that are not school property.
- all internal cameras are fixed. There are no PTZ (Pan-tilt-zoom) cameras at the Hindley site. The Whelley site has 3x PTZ cameras covering external areas of the school

b) Management & Access
- the viewing of live CCTV images will be restricted to the Headteacher, Core Leadership Team, Designated Safeguarding Leads, site staff, the school business manager and the IT support staff. These groups of people require access to investigate incidents.
- footage of incidents where physical intervention has been used is download and used by the staff involved and our staff PRICE trainers to debrief the incident, inform practice and change PHP for students. This increases the personal safety of all site users.

- site staff and office staff monitor CCTV live footage of all access and egress points of the school site to manage the safety and security of the site, given the high-risk nature of those who attend. In this way the system operates much like a "Ring" doorbell in that we can see who is trying to access site before granting them entry.
- the CCTV system is checked weekly by the IT support team to ensure that it is operating effectively

c) Storage

Recorded images are stored only for a period of 14 calendar days unless there is a specific purpose for which they are retained for a longer period.

The school will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

- CCTV recording systems being located in restricted access areas
- the CCTV system being encrypted/password protected
- restriction of the ability to make copies to specified members of staff
- the CCTV system not having direct access to / from the internet, with active firewalls in place to prevent such access