The Rowan Learning Trust

POLICY NAME: **CCTV Policy**

ADOPTED: Autumn term 2024

REVIEW PERIOD: Annually

REVIEWER: Director of Risk and Compliance

MAXIMISING POTENTIAL

Policy Document Version Control

Version 1

Responsibility for Policy:	Director of Risk and Compliance
Policy approval/date:	June 2023
Frequency of Review:	Annual
Next Review date:	June 2024
Related Policies:	If this policy relates to / links with any other policies, these can be listed here for context. Data protection policy
Minor Revisions:	An Addendum was added on the 29th June 2023. The addendum highlights the specific nuances that the policy doesn't cover when in relation to Three Towers Alternative Provision Academy. A second minor revision was made on 19th July 2023 as the DPA Act 2016 was changed to the correct year of 2018.

Version 2

Responsibility for Policy:	Director of Risk and Compliance
Policy approval/date:	June 2023
Frequency of Review:	Annual
Next Review date:	October 2024
Related Policies:	If this policy relates to / links with any other policies, these can be listed here for context. Data protection policy
Minor Revisions:	A change was made to 7.1 in **Retention and Disposal** on 11th Sept 2024 to highlight the fact that, dependent on requirement, phase and condition of the system a maximum of 50 days storage can be applied to the system.

Contents

POLICY AIM

This document will enable staff of the **Rowan Learning Trust** to comply with legislation relating to CCTV in all circumstances.

1. Executive Summary

1.1 The purpose of CCTV is to protect staff, students and the public, discourage aggressive and abusive behaviour protect the **Rowan Learning Trust** infrastructure, and provide evidence where required to investigate complaints.

1.2 The policy will set out the purpose of using CCTV, what information will be recorded, who will have access to this information and how this information will be stored and disposed of.

2. Policy Statement

2.1. This Policy seeks to ensure that the Close Circuit Television (CCTV) system used at **all RLT academies** is operated in compliance with the law relating to data protection (currently the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018") and as amended from time to time) and includes the principles governing the processing of personal data as set out in Appendix 1. It also seeks to ensure compliance with privacy law. It considers best practice as set out in codes of practice issued by the Information Commissioner and by the Home Office. **The Rowan Learning Trust** therefore uses CCTV only where it is necessary in pursuit of a legitimate aim, as set out in clause 2.2, and only if it is proportionate to that aim.

2.2. **Rowan Learning Trust** seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors, contractors, its property, and premises.

Rowan Learning Trust therefore deploys CCTV to:

- promote a safe **Rowan Learning Trust** community and to monitor the safety and security of its premises, staff, students and visitors.
- increase personal safety and wellbeing
- to prevent the loss of, or damage to the school buildings and/or assets;
- assist in the prevention, investigation, and detection of crime.
- assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings; and
- assist in the investigation of breaches of its codes of conduct and policies by staff, students, visitors and contractors and where relevant and appropriate investigating complaints.

2.3 This policy will be reviewed annually by **Chris Bolton – Data Protection Officer** to assess compliance with clauses 2.1 and 2.2 and to determine whether the use of the CCTV system remains justified.

3. Scope

3.1 This policy applies to CCTV systems in all parts of **Rowan Learning Trust** and other related facilities.

3.2 This policy does not apply to any Webcam systems located in meeting rooms, classrooms or lecture theatres operated by Faculties or ICT, which are used for the purposes of monitoring room usage and to assist with the use of the audio-visual equipment.

3.3 This policy applies to all **Rowan Learning Trust** staff, contractors and agents who operate, or supervise the operation of, the CCTV system including Security Management and Staff, and the Data Protection Officer.

4. Roles and Responsibilities

4.1 **Rowan Learning Trust** has the overall responsibility for this policy but has delegated day-to-day responsibility for overseeing its implementation to the staff identified in this policy. All relevant members of staff have been made aware of the policy and have received appropriate training.

4.2 The **Rowan Learning Trust** is responsible for ensuring that the CCTV system including camera specifications for new installations complies with the law and best practice referred to in clause 2.1 of this policy. Where new surveillance systems are proposed, the **Rowan Learning Trust** will consult with the Data Protection Officer to ensure an updated data protection impact assessment is completed if required.

4.3 Only the staff of **the IT and site departments** or a properly appointed maintenance contractor for **Rowan Learning Trust** CCTV system is authorised to install and/or maintain it.

4.4 The **Data Protection Officer** is responsible for the evaluation of locations where live and historical CCTV images are available for viewing. The list of such locations and the list of persons authorised to view CCTV images is maintained by the **Data Protection Officer**

4.5 Changes in the use of CCTV system can be implemented only in consultation with **Rowan Learning Trust** Data Protection Officer or the **Rowan Learning Trust** Legal Advisors. Proposed changes must include an updated DPIA.

5. System Description – Fixed cameras

5.1 The CCTV systems installed in and around the **Rowan Learning Trust** estate cover building entrances, car parks, perimeters, classrooms (in some circumstances) external areas such as courtyards, internal areas such as social/communal spaces eg staffrooms and dining rooms, computer rooms, rooms with high value equipment, corridors and reception areas. They continuously record activities in these areas *[and some of the cameras are set to motion detection].*

5.2 CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities etc.

5.3 CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant, so that staff, students, visitors, and members of the public are made aware that they are entering an area covered by CCTV. *(The signs also contain contact details as well as a statement of purposes for which CCTV is used*).

5.4 Contact with a specific school about CCTV should be made during normal business hours through the main school number. Queries will then be directed to the appropriate member of staff.

6. Operating Standard

6.1 The operation of the CCTV system will be conducted in accordance with this policy.

6.2 Software viewing area

6.2.1 No unauthorised access to the software viewing area ("the Control Room") will be permitted at any time.

6.2.2 Other than specified members of staff, access to the viewing software will be limited to:

- persons specifically authorised by the **headteacher**
- maintenance engineers.
- police officers where appropriate; and
- any other person with statutory powers of entry.

6.2.3 Monitors are not visible from outside the Control Room.

6.2.4 Before permitting access to the Control Room, designated staff will satisfy themselves of the identity of any visitor and existence of the appropriate authorisation. All visitors are required to complete and sign the visitors' log, which includes details of their name, department and/or the organisation that they represent, the person who granted authorisation and the times of entry to and exit from the Control Room.

6.2.5 A log of shall be retained setting out the following:

- person reviewing recorded footage.
- time, date, and location of footage being reviewed; and
- purpose of reviewing the recordings.

6.3 Processing of Recorded Images

6.3.1 CCTV images will be displayed only to persons authorised to view them or to persons who otherwise have a right of access to them. Where authorised persons access or monitor CCTV images on workstations, they must ensure that images are not visible to unauthorised persons for example by minimising screens when not in use or when unauthorised persons are present. Workstation screens must always be locked when unattended.

6.4 Quality of Recorded Images

6.4.1 Images produced by the recording equipment must be as clear as possible, so they are effective for the purpose for which they are intended. The standards to be met in line with the codes of practice referred to clause 1 of these procedures are set out below:

- recording features such as the location of the camera and/or date and time reference must be accurate and maintained.
- cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established.
- consideration must be given to the physical conditions in which the cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas;
- cameras must be properly maintained and serviced to ensure that clear images are recorded, and a log of all maintenance activities kept; and
- as far as practical, cameras must be protected from vandalism to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

7. Retention and Disposal

7.1 CCTV images are not to be retained for longer than necessary, considering the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce a maximum of 50 days rotation in data retention dependent on phase requirements.

7.2 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the retention period.

7.3 All retained CCTV images will be stored securely.

8. Data Subjects Rights

8.1 Recorded images, which directly or in combination with other factors enable a data subject to be identified, are considered to be the personal data of the individuals whose images have been recorded by the CCTV system.

8.2 Data Subjects have a right of access to the personal data under the GDPR and DPA 2018. They also have other rights under the GDPR and DPA 2018 in certain limited circumstances, including the right to have their personal data erased, rectified, to restrict processing and to object to the processing of their personal data.

8.3 Data Subjects can exercise their rights by submitting a request in accordance with the **Rowan Learning Trust** policies.

8.4 On receipt of the request, the Data Protection Officer, or their representative, will liaise with the **GDPR SENTRY** regarding compliance with the request, and subject to clause 8.5, the Data Protection Officer will communicate the decision without undue delay and at the latest within one month of receiving the request from the Data Subject.

8.5 The period for responding to the request may be extended by two further months where necessary, considering the complexity and number of the requests. The Data Protection Officer will notify the Data Subject of any such extension within one month of receipt of the request together with reasons.

9. Third Party Access

9.1 Third party requests for access will usually only be considered in line with the GDPR and DPA 2018 in the following categories:

- legal representative of the Data Subject.
- law enforcement agencies including the Police.
- disclosure required by law or made in connection with legal proceedings; and
- HR staff responsible for employees and university administrative staff responsible for students in disciplinary and complaints investigations and related proceedings.

9.2 Legal representatives of the Data Subjects are required to submit to **Rowan Learning Trust** a letter of authority to act on behalf of the Data Subject along with appropriate proof of the Data Subject's identity.

9.3 The Data Protection Officer will disclose recorded images to law enforcement agencies including the Police once in possession of a form certifying that the images are required for either:

- an investigation concerning national security.

- the prevention or detection of crime; or
- the apprehension or prosecution of offenders

and that the investigation would be prejudiced by failure to disclose the information. Where images are sought by other bodies/agencies with a statutory right to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.

9.4 Every CCTV image disclosed is recorded in the CCTV Operating Logbook and contains:

- the name of the police officer or other relevant person in the case of other agencies/bodies receiving the copy of the recording.
- brief details of the images captured by the CCTV to be used in evidence or for other purposes permitted by this policy.
- the crime reference number where relevant; and
- date and time the images were handed over to the police or other body/agency.

9.5 Requests of CCTV images for staff or student disciplinary purposes shall be submitted in writing to **the headteacher** in consultation with the Data Protection Officer.

9.6 Requests for CCTV information under the Freedom of Information Act 2000 will be considered in accordance with that regime.

10. Misuse of CCTV systems

10.1 The misuse of CCTV system could constitute a criminal offence. Any member of staff who breaches this policy may be subject to disciplinary action.

11. Complaints procedure

11.1 Any complaints relating to the CCTV system should be directed in writing following the Rowan Learning Trust's complaints policy. If a complainant is not satisfied with the response, they may appeal to **the Information Commissioners Office (ICO)**

11.2 Complaints in relation to the release of images should be addressed to the **headteacher** as soon as possible and in any event no later than three months from the event giving rise to the complaint.

12. Useful Links

The Information Commissioner's Code of Practice can be found at:

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Rowan Learning Trust Data Protection Officer

Chris Bolton – RLT DPO
Email: dpo@rlt.education

13. Addendum

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

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.**

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

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.