Medina College The Island VI Form

Medina College and The Island VI Form

CCTV Policy

Author	Josh Collins, Anna Mursell
Approved by	IEB
Approval date	19 March 2026
Review frequency	Every Three Years
Next review	March 2029

Revision History

Revision	Change	Date
2.0	Initial CCTV Policy version 2.0	03/01/2023
2.1	Amendments following Trust onboard	06/05/2025
2.2	Minor amendments	09/03/2026

1. Introduction

The purpose of this policy is to regulate the management, operation, and use of the closed-circuit television (CCTV) system at both Medina College and The Island VI Form. The system comprises almost 200 cameras located across both college sites. All cameras are centrally monitored, and the footage is available to SLT staff, Head of Years (and Assistants) as well the Facilities and ICT Support team.

This policy is aligned with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025, and the Information Commissioner's Office (ICO) Guidance on Video Surveillance. The CCTV system is owned by Medina College.

2. Objectives of the CCTV scheme

- Increase personal safety of staff, children and visitors and reduce the fear of crime
- Protect the school buildings and their assets
- Provide footage for review in the event of a reported crime, security incident, or health and safety investigation and to assist police in enquiries should they arise
- Assist in identifying, apprehending and prosecuting offenders
- Protect members of the public and private property

3. Statement of Intent

The CCTV system is registered with the Information Commissioner's Office, and the Trust complies fully with UK data protection legislation. All footage and associated data are treated as personal data under the UK GDPR and the Data Protection Act 2018.

Cameras are positioned strategically and will not be used for the routine monitoring of student behaviour, unless such behaviour is linked to crime, violence, safeguarding investigations, security incidents, or direct health and safety risks. Cameras do not monitor private homes, gardens, toilets, changing rooms, staff rooms, or any other areas where individuals have a heightened expectation of privacy.

Clear CCTV warning signs, compliant with ICO guidance, are displayed at all access points and within monitored areas. Footage will only be used for the purposes outlined in this policy and will never be used for commercial or entertainment purposes. While every effort is made to ensure coverage, the system cannot guarantee that every incident will be captured

4. Operation of the system

The CCTV system will be administered and managed by school staff of Medina College. Day-to-day operational responsibility lies with the Estates and ICT Support Teams to handle requests and provide technical assistance relating to the network infrastructure, connectivity, and system performance.

All requests to view or export footage must be submitted through the school's ticketing system, ad-hoc monitoring is not permitted. Viewing will take place in designated secure areas, and only authorised staff may access footage. The system operates 24 hours per day, 365 days a year, recording video only — no audio is captured.

5. Control and Liaison

The ICT Support Team will check and confirm the efficiency of the system regularly, in particular that the equipment is properly recording and that cameras are functional. This includes the digital video recorder (DVR) units across the sites and their storage capacity, and physical condition. The ICT Support Team's involvement is limited to technical support related to the networking infrastructure that the CCTV cameras rely on. For example, providing network connectivity for new cameras and general IT maintenance.

6. Monitoring procedures

Camera surveillance may be maintained at all times and footage continuously recorded and held on system memory for a retention period of 14 days. Beyond the retention period the footage is automatically overwritten by the DVR unit.

7. Recording and retention of images

CCTV footage is recorded continuously and stored on secure DVR/NVR units. To comply with data minimisation principles, recorded images are retained for up to 30 days, after which they are automatically overwritten. Any footage extracted and shared internally for ticketing purpose will be stored on the College's cloud storage platforms for up to 90 days before being automatically deleted.

Where footage is retained beyond the standard retention period (e.g., for police or legal proceedings), it will be securely preserved and access restricted. Storage media reaching end-of-life will be securely wiped and destroyed to ISO 27001 standards.

8. Access to and disclosure of images

Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected and as outlined in Section 2. Requests related to general behavioural monitoring will be denied unless the incident involves crime, safeguarding, or ongoing health and safety investigations.

The images that are filmed are recorded centrally on a DVR at each site and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system and to those line managers who are authorised to view them in accordance with the purposes of the system. Viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing is occurring. If media on which images are recorded are removed for viewing purposes, this will be documented.

Disclosure to third parties will only occur when permitted by law and consistent with the purposes of this policy:

- The police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness

- Prosecution agencies, such as the Crown Prosecution Service
- Relevant legal representatives
- Line managers involved with disciplinary processes
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders)
- The Executive Headteacher (or another authorised person acting in their absence) is the only person who is permitted to authorise disclosure of information to external third parties such as law enforcement agencies

All requests for disclosure and access to images must be documented on the ICT and Facilities ticketing system in advance of accessing the system, including the date/time of the disclosure, location of the incident, to whom the images have been provided and the reasons why they are required. The ticketing triage process undertaken by the Facilities and ICT Support teams will review the request to ensure it aligns with the stated objectives of the CCTV system. Requests for footage to monitor general behavioural or interactional matters that do not involve a crime, security incident or health and safety concerns will be denied. If disclosure is denied, the reason will be recorded. Access to the CCTV system outside of routine maintenance is only permitted following an appropriately logged ticket by an authorised member of staff, ad-hoc monitoring is not acceptable by any members of staff.

Requests by the Police can only be authorised under section 29 of the Data Protection Act 1998. Should a USB export of footage be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.4 of this policy. USBs will only be released to the Police on the clear understanding that the USB remains the property of the local school, and both the USB and information contained on it are to be treated in accordance with this policy. The Trust also retains the right to refuse permission for the Police to pass to any other person the USB or any part of the information contained thereon. On occasions when a Court requires the release of an original USB this will be produced from the safe, complete in its sealed bag. The Police may require the school to retain the stored USBs for possible use as evidence in the future. Such USBs will be properly indexed and properly and securely stored in a safe until they are needed by the Police.

Applications received from outside bodies (e.g. solicitors) to view or release footage will be referred to the Headteacher. In these circumstances footage will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. This must be provided within 30 calendar days of receiving the required fee and the request. If the decision is taken not to release the images, then the image in question should be held and not destroyed until all legal avenues have been exhausted.

9. Individuals' access rights

Under the GDPR individuals have the right on request to receive a copy of the personal data that the school holds about them, including CCTV images if they are recognisable from the image.

If you wish to access any of your CCTV images, you must make a written request to the Headteacher. Your request must include the date and time when the images were recorded and the location of the CCTV camera, so that the images can be located and your identity can be established as the person in the images. The school will always check the identity of the person making the request before processing it. Requests must be submitted within the 30-day retention window. The College will respond to valid requests within one calendar month. The footage itself is only available for up to 30 days, therefore footage requests outside of this timeframe from the specified date is not possible.

The Headteacher will first determine whether disclosure of your images will reveal third party information as you have no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.

If the Trust is unable to comply with your request because access could prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders, you will be advised accordingly.

10. Training

Medina College will ensure that any staff accessing CCTV systems receive appropriate training on system operation, UK GDPR data protection requirements, and the secure handling of personal data.

11.Breaches of the policy (including breaches of security)

Any breach of this policy by College staff will be investigated by the Headteacher in accordance with College disciplinary procedures. Serious data breaches will be reported to the ICO within 72 hours.

12. Assessment of the policy

Performance monitoring, including random operating checks, may be carried out by the Estates Manager with direction from the Head of Estates, Health and Safety.

13. Complaints

Any complaints about the school's CCTV system should be addressed to the Headteacher. Complaints will be dealt with in accordance with the complaints policy.

14. Public information

Copies of this policy will be available to the public on request and can be found on the school's websites.

15. Summary of Key Points

- This policy will be reviewed every two years.
- The CCTV system is owned and operated by Medin College.
- Liaison meetings may be held with the Police and other bodies.
- All CCTV requests must be ticketed/logged in advance of any footage being viewed and/or exported.
- Recording USBs used will be properly indexed, stored and destroyed after appropriate use.
- Footage may only be viewed by authorised staff and the Police.
- Exported footage required as evidence will be properly recorded, witnessed and packaged before copies are released to the police.
- Footage will not be made available to the media for commercial or entertainment.
- Exported footage will be disposed of securely to ISO 27001 standards.
- Any breaches of this policy will be investigated by the Headteacher. An independent investigation will be carried out for serious breaches.
- Breaches of this policy and remedies will be reported to the Headteacher.