

CCTV Policy

Introduction

OMG Education (OMG) has a closed-circuit television (CCTV) system in place to help provide a safe and secure environment for students, staff, and visitors and protect organisational property.

CCTV systems are based on digital technology and, therefore, need to be treated as information that will be processed under the Data Protection Act 2018. The person ultimately responsible for data protection within the OMG is the Data Protection Officer (DPO).

The purpose of this policy is to regulate the management, operation and use of the CCTV system at the OMG. This document sets out the accepted use and management of the CCTV system and images to ensure the OMG complies with the Data Protection Act 2018, Human Rights Act 1998 and other legislation.

OMG has produced this policy in line with the ICO's code of practice: <https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>

The system will be provided and operated in a way that is consistent with an individual's right to privacy and in accordance with the OMG Data Protection policy and privacy notices, which are available at <https://www.omg.school/policies/>.

Purpose of CCTV

OMG has installed CCTV systems to:

- Protect organisational buildings and assets and ensure they are free from intrusion, vandalism, damage, or disruption.
- Increase the personal safety of staff and students and reduce the fear of physical abuse, intimidation, and crime.
- Support the police in a bid to prevent and detect crime.
- Assist with the identification, apprehension, and prosecution of offenders.
- Assist with identifying actions or activities that might result in disciplinary proceedings against staff and students.
- Assist in the usage and management of the organisation building on a day-to-day basis.
- Provide management information relating to contract compliance of third-party service providers.
- Monitor the security of organisation building.

Overview of system

The system comprises several fixed and dome cameras located both internally and externally around the OMG building. All cameras may be monitored and are only available for use by approved staff members.

The CCTV runs continuously seven days a week all year round.

The CCTV system comprises fixed-position cameras, digital recorders and public information signs.

CCTV cameras are located at strategic points on site, principally at the entrance and exit points for the site and areas where young people may congregate.

CCTV signs will be prominently placed at strategic points and at entrance and exit points of the building to inform staff, students, visitors and members of the public that a CCTV installation is in use.

Although every effort has been made to ensure maximum effectiveness of the CCTV system, it does not cover all areas, and it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Operation

The CCTV surveillance system is owned by OMG.

The IT department (ITD) is responsible for the day-to-day operation of the system and ensuring compliance with this policy.

Cameras will be used to monitor activities within the OMG building, the car parks, and other areas to identify criminal activity as it occurs, anticipates, or is perceived and to secure the safety and well-being of the organisation's grounds occupants and visitors.

Static cameras will not focus on private homes, gardens, or other areas of private property.

Operators of cameras with tilt, pan, and zoom capability will not direct cameras at an individual, their property, or a specific group of individuals without verbal authorisation from the Director unless an emergency response to events is required.

Materials or knowledge secured from the CCTV system will not be used for any commercial purpose.

Downloads will only be released to the media for use in investigating a specific crime and with the written authority of the police. Footage from the CCTV must not be viewed or released for entertainment purposes under any circumstances.

The planning and design of the existing CCTV system have endeavoured to ensure maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the information commissioner's code of practice, have been placed at access routes and areas covered by the OMG CCTV system.

Viewing of live CCTV

The system allows for the viewing of live CCTV images. The staff members named may monitor these images live for the purposes listed above.

Image searching and download procedure

Recorded CCTV may be searched or downloaded by authorised staff members and the police only. Permission to search or download must be requested using the CCTV release form, which must be submitted and approved by the person listed below before the CCTV is searched or downloaded. All requests, whether approved or denied, will be logged.

Student, visitors or public incidents – requests approved by the Director
Staff incidents – requests approved by the Director

For administrative purposes, such as looking for lost property, the IT Operations manager may only view the recorded footage without completing a release form. The details of the viewing must be recorded in the log as usual.

The form is available in Appendix B of this policy.

- Members of staff authorised to make requests and search CCTV if approved
 - Directors
 - Data Protection Officer
 - Designated safeguarding lead
 - Operations Manager
- In a police emergency the operations manager may facilitate the police to view footage on the sight of a warrant card. They will record the details, including the warrant card information, on the viewing log.
- Should a download be required as evidence, an electronic copy may only be made with written authorisation from the Director:
 - Where this is to be released to the police, it will only be completed upon receipt of the CCTV release form and upon sight of their warrant card.
 - Where this is to be released to a staff member it must only be the people on the authorised list above.
 - Where this is to a third party, this must be in accordance with the procedures laid out elsewhere in this policy.
 - Where a download is approved, it must be provided on a password-protected storage device which is to be returned to the Data and IT Officer for the files to be destroyed on completion of the investigation.
 - Downloads should not be emailed or shared via any other means under any circumstances.
 - All requests will be logged whether they were approved or denied.

Data Protection Act of 2018

For the purpose of the Data Protection Act 2018, OMG is the data controller.

If CCTV digital images show a recognisable person, they are considered personal data and are covered by the Data Protection Act 2018. This policy is to be considered with the organisation's Data Protection and Privacy policy, the provisions of which should always be adhered to.

Where new cameras are to be installed on OMG premises, part 4 of the ICO's CCTV code of practice will be followed before installation:

- The appropriateness of and reasons for using CCTV will be assessed and documented;
- The purpose of the proposed CCTV system will be established and documented;

- Responsibility for day-to-day compliance with this policy will be established and documented.

Access to images – individual access rights

The Data Protection Act of 2018 gives individuals the right to access personal information about themselves, including CCTV images.

Individuals who believe they have been captured on CCTV may request those images. All requests for access to view or copy CCTV footage by individuals should be made in writing to the Director in line with the advice at this link <https://www.gov.uk/request-cctv-footage-of-yourself>

Access to images – third parties

Unlike data subjects, third parties who wish to have a copy of CCTV images (i.e. images not of the person making the request) do not have a right of access to images under the Data Protection Law. Care must be taken when complying with such requests to ensure that neither the Data Protection Law nor the CCTV Policy are breached. Requests from third parties will only be granted if the requestor satisfies the following criteria:

- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
- Prosecution agencies and their legal representatives
- Insurance companies and their legal representatives

Access to images – procedure for third parties

Requests for access to CCTV images must include:

- Payment of appropriate fee per application
- Completed CCTV release form, which is available in Appendix A.
- The reason for the request
- The date and time the images were recorded.
- Information to identify the individual, if necessary
- The location of the CCTV camera
- Name and address of the requester
- Proof of identity of the requester (passport or driving licence)

OMG will respond promptly and, at the latest, within 30 calendar days of receiving the payment and request, assuming sufficient information exists to identify the requested images.

All third-party requests for access to a copy of CCTV footage should be made in writing to the Director.

All requests and whether they were approved or denied will be logged.

If OMG cannot comply with the request, the reasons will be documented. Where possible, the requester will be advised of these in writing.

Retention and disposal

Recorded images will be retained for no longer than 1 month from the recording date unless required for evidential purposes or the investigation of crime or otherwise required and retained as a download with the requisite approval form.

All images on electronic storage will be erased by automated system overwriting. All downloads, still photographs and hard copy prints will be securely disposed of as confidential waste.

Central responsibilities

The Data Protection Officer is responsible for producing and reviewing this policy.

The Director is responsible for the day-to-day implementation of procedures to comply with this policy.

Complaints regarding the operation of the system

Complaints regarding the CCTV system and its operation should be made under the OMG complaints procedure.

Breaches of this policy

Staff must not interfere with or disrupt the system's operation in any way, such as by unplugging, moving, or covering cameras. Any suspected breach of this policy will be considered under OMG's disciplinary policy and procedure.

APPENDIX A: CCTV Playback and Release Request Form

Staff Name:	
Date of Incident:	
Location/Area to be viewed:	

Description of Incident:	
Starting Time:	Ending Time:
Staff Member Signature:	
Date of Request:	

Data Protection Officer consent:	
I hereby authorise/deny the reviewing & release of the above CCTV request	
Approved:	Denied:
DPO Name:	
DPO Signature:	Date:

Police Authorisation (if required)	
Crime Ref. Number:	CAD Number:
Police Officer Name:	Rank:
Police Station Attached to:	Station Contact Number:

