CLOSED CIRCUIT TELEVISION (CCTV) MONITORING POLICY & IMPACT ASSESSMENT.

Queen Mary's College

This document is owned, reviewed and maintained by the Senior leadership team. The current version of this document is also available electronically on the QMC Intranet.

Version History

REVISION #	DESCRIPTION OF CHANGE	DATE
1	Replacement of 2019 policy, to include updates to legislation, increased assets and to incorporate the impact assessment.	22/11/2021
2	Initial issue	21/12/2021
3	Update to include internal request for access detail	12/06/2023
4	Reviewed – no updates	05/01/2025
5	Formatted – Font changed - responsibilities updated	08/11/2025

1 Introduction

1.1 Queen Mary's College QMC is an open 25-acre site, comprising of a large number of buildings; significant grounds made up of sports pitches; wooded areas; grass and planted areas, car parks and a Sports Centre open to the public. It is a sixth form College with over 2000 students and staff and is also a community space where members of the public can hire and use spaces within the estate.

1.2 Maintaining security and safeguarding is, not surprisingly, challenging and to support this need, QMC has a Closed-Circuit Television (CCTV) system in place which records live images in key locations around the college. At the time of publication (November 2021) QMC has an existing CCTV system which is aging, deteriorating and no longer fit for purpose. To ensure we can satisfactorily safeguard our students, staff, visitors and assets, the existing system will be upgraded and expanded in January 2022 to cover

vulnerable, high risk or exposed areas.

1.3 This document details the purpose, use and management of the CCTV system at the College and details the procedures to be followed in order to ensure that the College complies with relevant legislation. The College will therefore have due regard to the Data Protection Act 2018, the UK Data Protection Regulations (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998.

1.4 This document is based upon guidance issued by the Information Commissioner's Office, 'In the picture: A data protection code of practice for surveillance cameras.'

2 CCTV System overview

2.1 The CCTV system is owned by QMC and is managed by the Site Services Department under the management of the Senior leadership team, Organisational Support and maintained by appointed contractors. QMC is the data controller for the images produced by the CCTV.

2.2 The College is registered with the Information Commissioner's Office and the registration number is Z6760455. The CCTV system operates to meet the requirements of the Data Protection Act and the Information Commissioner's guidance.

2.3 The Senior leadership team, Organisational Support is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

2.4 The CCTV system operates across QMC's only site at Cliddesden Road, Basingstoke RG21 3HF and details of the number and location of cameras is held at N:\Premises\11. Security\11.02 CCTV. Signs informing members of the public that CCTV is in operation, and who they should contact in relation to this, are displayed site wide. The signage indicates that the system is managed by Queen Mary's College. The Site Services Manager is responsible for ensuring that adequate and compliant signage is erected.

2.5 Cameras are sited to ensure that they cover QMC premises as far as is possible. Cameras are installed throughout the site including roadways, car parks, common areas, hired and licensed premises, within buildings and externally in vulnerable public facing areas. Cameras are not sited to focus on private residential areas located on the Campus boundary.

2.6 The CCTV system is operational and is capable of being monitored for 24 hours a day,

every day of the year. The CCTV system and any proposed new installation is subject to a Data Protection Impact Assessment.

3 Purposes of the CCTV system

3.1 The principal purposes of the CCTV system are as follows:

- for the prevention, reduction, detection and investigation of crime and other incidents.
- to ensure the safety and well-being of staff, students and visitors.
- to assist in the investigation of suspected breaches of QMC rules or UK Law by staff, visitors or students; and
- the monitoring and enforcement of traffic related matters.

3.2 The CCTV system can be used to observe the College campus areas under surveillance in order to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

3.3 The College seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.

4 Monitoring and Recording

4.1 The College complies with the Employment Practices Code which can be found online at https://ico.org.uk/media/fororganisations/documents/1064/the_employment_practicescode.pdf

4.2 Cameras are not typically monitored on a day to day basis, but if that should be required, it will be done, by authorised staff only, from the Site Services Area which is a secure standalone building located at the front of the Campus.

4.3 Site Services, which includes a non-licenced Security person, is equipped with a Home Office licensed radio system linking it with key Support teams throughout the college. The Student Support and Security Officer will respond to incidents alerted either via personal notification or as a result of CCTV monitoring. A separate, key holding and licensed team of Security Officers is available to QMC, subject to availability and by an external contractor.

4.4 The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are periodically maintained to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate. Images are stored on recorders located in E Block and

Spectrum IT Hubs. The CCTV expansion/upgrade will increase the number of NVR's and they will be located in each building site wide dependant on camera location.

4.5 All images recorded by the CCTV System remain the property of QMC.

4.6 The use of covert cameras will be restricted to rare occasions, when a series of criminal acts or acts which could cause personal harm to an individual or College assets, have taken place within a particular area that is not otherwise fitted with CCTV. A request for the use of covert cameras will clearly state the purpose and reasons for use and the authority of the Principal will be sought before the installation of any covert cameras. The Senior leadership team, should be satisfied that all other physical methods of prevention have been exhausted prior to the use of covert recording. Covert recording will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there are reasonable grounds to suspect that illegal or unauthorised activity is taking place. All such monitoring will be fully documented and will only take place for a limited and reasonable period. Body worn cameras should be used at all times, but specifically during security patrol or lock/unlock duties. The downloading of images from such cameras will only be conducted by Site Services Personnel and cameras will be cleansed following each shift. Security staff wearing body worn cameras will disclose, when approaching persons, that they are being video and audio recorded.

5 Compliance with Data Protection Legislation

5.1 In its administration of its CCTV system, QMC complies with the UK Data Protection Act (2018) 'DPA 2018' and UK GDPR which together supersede the Data Protection Act of 1998.

5.2 This policy has been created as a risk-based approach to compliance, and is based on the following fundamental rights of a 'data subject':

- **The right to be informed** of how and why a subject's data is being used. Generally achieved through privacy notices, fair processing notices, terms and conditions or contracts.

- **The right of access to** the personal information a data controller holds, generally done via a 'subject access request' or SAR. An individual **can make a SAR verbally or in writing**, including on social media. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact. The SAR form is found at Appendix A.

- **The right to rectification** of personal data.

- **The right of erasure** (to be forgotten) either by deleting or anonymising personal information when requested (however, this right is not always applicable).

- **The right to restrict** processing of personal data, such as restricting the sharing with another organisation or to restrict sending emails.

- **The right to data** portability of personal data, provided by them, to another data controller or processor.

- **The right to object** to the processing of personal data (however, this right is not always applicable).

- **Rights in relation to automated decision making** and profiling the right of a data subject to be notified when software is making important decisions or profiling them via an automated process. *Applications for disclosure of images*

5.3 Requests by individual data subjects for images relating to themselves "Subject

5.4 Access Request" should be submitted in writing to the Senior leadership team together with proof of identification. A form at Appendix A is available for this purpose

5.5 In order to locate the images on the College's system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

5.6 Where QMC is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

5.7 A request for images made by a third party should be made in writing to the Senior leadership team- Organisational Support.

5.8 In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation. Such disclosures will be made at the discretion of the Senior leadership team with reference to relevant legislation and where necessary, following instruction from the Principal.

5.9 Where a suspicion of misconduct arises and at the formal request of the Director of HR & Commercial Ops, the senior leadership team may provide access to CCTV images for use in staff disciplinary cases. A form is available at Appendix B for this purpose.

5.10 Access to CCTV images will be sought as evidence in relation to student discipline cases.

A form is available at Appendix B for this purpose.

5.11 A record of any disclosure made under this policy will be retained on file in the Site Services Office by the Security team.

6 Retention of images

6.1 Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.

6.2 Where an image is required to be held in excess of the retention period referred to in 7.1, the Principal or their nominated deputy, will be responsible for authorising such a request, see form at Appendix B

6.3 Images held in excess of their retention period will be reviewed on a three-monthly basis and any not required for evidential purposes will be deleted.

6.4 Access to retained CCTV images is restricted to The Student Support & Security Officer and the Site Services Manager and other persons as required and as authorised by the senior leadership team

7 Monitoring Compliance

7.1 All staff involved in the operation of the College's CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.

7.2 All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training.

8 Policy review

8.1 The College's usage of CCTV and the content of this policy shall be reviewed annually by the senior leadership team with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.

8.2 Next review due: January 2027

CCTV SUBJECT ACCESS REQUEST FORM DATA SUBJECT ACCESS CCTV APPLICATION FORM – APPENDIX A

Under the terms of the Data Protection Act 2018, the UK Data Protection Regulations (GDPR), an individual is entitled to ask the authority for a copy of all personal information which it holds about him/her for the purposes of providing services to the individual. The information, which the individual is entitled to receive from the authority, includes a description of these purposes and the recipients to whom the data can be disclosed. The entitlement is known as the “Right of Access to Personal Data”.

Please complete this form, providing as much information as possible, should you wish to exercise your right in requesting disclosure of your data. Information on this document will be used only for the purposes described above. We may, however, store the data in manual or electronic form, but only for as long as we are required to do so by law

PERSONAL DETAILS

Name	
Address	
Telephone Number	
E-Mail Address	
Gender /Pronoun	

INFORMATION REQUIRED

To help us find the CCTV data you require, please complete the following section: please be as accurate as possible with times, location and identification.

Date	
Time	
Location	
Description of incident	

DECLARATION

I confirm that this is all of the personal data to which I am requesting access and which is held by the authority for its purposes. I also confirm that I am the Data Subject and not someone acting on his/her behalf.		
Signed	Mr/Mrs/Miss/Title	Date
For completion only if you are acting on behalf of another person(s): I confirm that I am acting on behalf of the data subject and have submitted proof of my authority to do so.		
Name		
Address		
Telephone No		
Signed	Date	

FEE & PROOF OF IDENTITY

Under the Data Protection Act 2018, we are entitled to charge a small administration fee of £10 for processing your application. You will be contacted to effect payment.

We also require evidence that this enquiry is genuine. Therefore, please be prepared to provide, on request, originals of two proofs of identify such as a driving licence, passport, recent utility bill etc. If you are applying on someone else's behalf, you will be asked to provide proof of identity for both the data subject and yourself as well as documented authority to act on the Data Subjects behalf. Failure to provide these documents with your application will mean that your request is refused.

5. POSTAL ADDRESS

After completing the application form, please check to ensure that all the information you have provided is accurate and return the application by post to Queen Mary's College, Cliddesden Road, Basingstoke RG21 3HF, or by e mail to Security@qmc.ac.uk.**INTERNAL ACCESS TO CCTV FOOTAGE – Appendix B**

Where a suspicion of misconduct arises and at the formal request of the Director of HR & Commercial Ops, the Senior leadership team- Organisational Support may provide access to CCTV images for use in staff disciplinary cases.

The Senior leadership team- Organisational Support may provide access to CCTV images to the Senior Leadership Team (SLT) when sought as evidence in relation to student discipline cases.

A record of any disclosure made under this policy will be retained on file in the Site Services Office by the Security team.

REQUESTOR

Name	
Staff I. D.	
E-Mail Address	
Department	

INFORMATION REQUIRED

To help us find the CCTV data you require, please complete the following section: please be as accurate as possible with times, location and identification.

Date	
Time	
Location – include building and room numbers wherever possible	
Description of incident	
Reason (Brief description of why this footage is required)	

APPROVALS

Approval is given for the requestor to be shown the CCTV footage requested**. Note:** CCTV is only retained for 30 days – should retention be required for longer, please ask the CCTV operator to download the footage to the secure folder held for that purpose. Images are not to be shared with a third party without the permission of the Principal.

Signed……

Senior leadership team- Organisational Support

Office use only

Only the Student Support & Security Officer and the Site Services Manager are permitted to access the CCTV system for the purpose of recovering footage.

Footage shown to requestor (date/initials of operator)

Extended retention only – file name/location