



## CCTV Policy

Last reviewed:	September 2025
Next review date:	September 2027
Approved by:	Trust Board 04.11.25
Trustee Minute No:	0485

## **Contents**

1.0 Context.....	3
2.0 Introduction .....	3
3.0 Statement of Intent .....	3
4.0 Persons Responsible .....	4
5.0 Objectives of the CCTV System.....	4
6.0 Location .....	5
7.0 Identification.....	5
8.0 Image Storage and Retention .....	5
9.0 Disclosure.....	6
10.0 Access by the Data Subject.....	6
11.0 System Maintenance and Monitoring .....	7
12.0 Breaches of the policy (including breaches of security).....	8
13.0 Complaints .....	8
Appendix 1: Code of Practice Check List .....	9
Appendix 2: Disclosure Request .....	11
Appendix 3: Internal Recording Request Form .....	14

## **1.0 Context**

The UK is recognised as a leading user of closed circuit television (CCTV) and the public are used to seeing CCTV cameras on virtually every high street. Such systems continue to enjoy general public support, but they do involve intrusion into the lives of ordinary people as they go about their day-to-day business and can raise wider privacy concerns.

QEGSMAT (the Trust) know the public expect CCTV to be used responsibly with proper safeguards in place and has developed this CCTV Policy to comply with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) to inspire confidence that it is using CCTV responsibly.

Images of people are covered by the Data Protection Act and General Data Protection Regulation (GDPR) and so is information about people, which is derived from images, for example, vehicle registration numbers.

### **Further Reading**

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/>

## **2.0 Introduction**

The Trust is fully committed to the safety of its staff, students/pupils and visitors and to this extent has invested in the security of its buildings and facilities. The purpose of this policy is to regulate the management, operation and use of CCTV within the Trust.

Under the Protection of Freedoms Act 2012 the processing of personal data captured by CCTV systems (including images identifying individuals) is governed by the Data Protection Act, General Data Protection Regulation (GDPR) and the Information Commissioner's Office (ICO) has issued a code of practice on compliance with legal obligations under that Act. The use of CCTV by schools is covered by the Act, regardless of the number of cameras or how sophisticated the equipment is.

All cameras may be monitored and are only available for use by approved members of staff. The CCTV system is owned by the Trust and will be subject to a review annually.

## **3.0 Statement of Intent**

The Trust will seek to comply with the requirements of the Data Protection Act ("the Act"), the Information Commissioner's Guidance on Video Surveillance and the Surveillance Camera Commissioner's Code of Practice.

The school will treat the system and all information, documents and recordings obtained and used as personal data which are protected by the Act.

Materials or knowledge obtained as a result of CCTV will not be used for any commercial purpose. Recordings will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Recordings will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the scheme will give 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.

Cameras will not record any private premises.

A log is kept of authorised staff access to recorded images (template below)

## **4.0 Persons Responsible**

**System Controller** Each Headteacher is herein named the System Controller at each academy and is responsible for the implementation and enforcement of this policy within their respective academies.

**System Manager** The System Controller may name an individual System Manager for the day-to-day management of the CCTV systems.

**System User** The System Controller has the authority to grant access to specific individuals (System User) to view and access media. Each individual will be given a separate account for accessing the system when that feature is available.

### **User Responsibilities**

All users of the CCTV system have the following responsibilities:

- To uphold the arrangements of this policy.
- To handle images/data securely and responsibly, within the aims of the policy. Staff need to be aware that they could be committing a criminal offence if they misuse CCTV images.
- To uphold the recorded procedure for subject access requests.
- To attend training/refresher sessions as required.
- To report any breach of this policy or procedure to the System Controller.

## **5.0 Objectives of the CCTV System**

The Trust uses CCTV equipment to provide a safer, more secure environment for students/pupils, staff and visitors, to prevent bullying, vandalism and theft. Essentially the system is used to:

- Protect the Trust's buildings and its assets to ensure they are kept free from intrusion, vandalism, damage or disruption.
- Support the police in a bid to deter and detect crime.

- Assist in identifying, apprehending and prosecuting offenders.
- Safeguard students/pupils, staff and the public.
- Monitor behaviour where there is cause for concern.
- Assist in the usage and management of Trust buildings on a day-to-day basis.

The Trust does not have hidden cameras.

## **6.0 Location**

Cameras are located in those areas where each academy has identified a need. The academies' CCTV systems are solely used for the purposes identified above.

## **7.0 Identification**

In areas where CCTV is used the Trust will ensure that there are prominent signs placed at the entrance of the CCTV zone.

The signs will be:

- Clearly visible.
- Contain details of the organisation operating the scheme and who to contact about the scheme.

## **8.0 Image Storage and Retention**

Recorded images will be stored in a way that ensures their integrity and in a way that allows specific times and dates to be identified. Access to live images is restricted to a list of approved users unless the monitor displays a scene which is in plain sight from the location of the monitors. Recorded images can only be viewed in a restricted area by those staff authorised by the System Manager. The recorded images are viewed only when there is a clear reason for this to happen.

The Trust reserves the right to use images captured on CCTV where there is activity that the Trust cannot be expected to ignore such as potential criminal activity, safeguarding, gross misconduct or behaviour which puts others at risk. Images retained for evidential purposes will be retained in a locked area accessible by the System Controller or System Manager only. Where images are retained, the System Controller will ensure the reason for its retention is recorded, along with where it is kept, any use made of the images and finally when it is destroyed.

Neither the Data Protection Act nor the Information and Records Management Society prescribe any specific minimum or maximum periods which apply to CCTV recorded images. CCTV images are usually retained for a period of between 7-31 days depending on the resolution of the footage and the capacity of the storage device.

Where CCTV is copied to be retained for longer periods this will be documented and justified in the Access Log.

## **9.0 Disclosure**

Disclosure may be authorised to law enforcement agencies, even if a system was not established to prevent or detect crime, if withholding it would prejudice the prevention or detection of crime.

### **Academy Staff**

Viewing of recorded images by members of staff can only be authorised by the System Controller or those with delegated access. Disclosure will only be granted if it is consistent with the objectives of the CCTV system.

### **Third Parties**

Disclosure of the recorded images to third parties can only be authorised by the System Controller. Disclosure will only be granted if either:

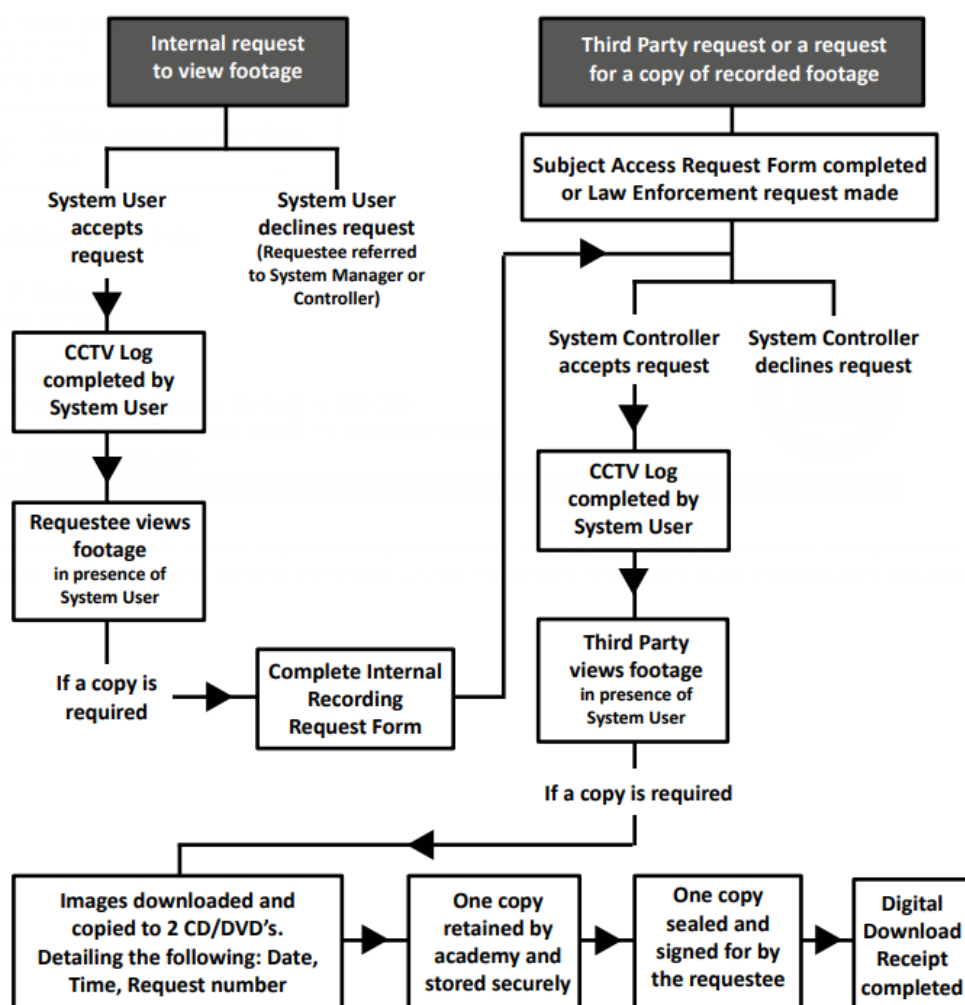
- Its release is fair to the individuals concerned; or
- There is an overriding legal obligation (e.g. information access rights); or
- It is consistent with the purpose for which the system was established.

## **10.0 Access by the Data Subject**

The Data Protection Act provides Data Subjects (individuals to whom “personal data” relate) with a right to data held about themselves, including those obtained by CCTV. Requests for Data Subject Access should be made in writing to the academy’s Data Protection Co-ordinator (see Subject Access Request form, Appendix 2) and will be dealt with in accordance with the Trust’s Data Protection Policy.

## The Request Procedure

Initial request for disclosure:



## 11.0 System Maintenance and Monitoring

The Trust undertakes regular audits to ensure that the use of CCTV continues to be justified. The audit includes a review of:

- Completed Code of Practice checklist
- Its stated purpose
- The location of cameras
- The images recorded and the length of time they may be stored for
- CCTV Policy and procedure

The CCTV systems are owned by the Trust.

The school will carry out a Data Protection Impact Assessment to review the use of CCTV whenever there is any significant change to the use of the system or the purpose for which it is used.

## **12.0 Breaches of the policy (including breaches of security)**

Any breach of this policy by school staff will be initially investigated by the Headteacher, in order for him/her to take the appropriate disciplinary action.

Any serious breach of this policy will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

## **13.0 Complaints**

Any complaints about an academy's CCTV system should follow the QEGSMAT Complaints Policy. A copy of which is available from [on the QEGSMAT website](#).



### Appendix 1: Code of Practice Check List

This CCTV system and the images produced by it are controlled by the academy which is responsible for how the system is used.

The Trust has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of our community. It will not be used for other purposes.

	<b>Checked (Date)</b>	<b>By</b>	<b>Date of next review (12 Months)</b>
<b>There is a named individual who is responsible for the operation of the system.</b>			
<b>The problem we are trying to address has been defined and recorded, and installing cameras is the best solution. This decision should be reviewed on a regular basis.</b>			
<b>A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.</b>			
<b>Cameras have been sited so that they provide clear images.</b>			
<b>Cameras have been positioned to avoid capturing the images of persons not visiting the premises.</b>			
<b>There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system, contact details are displayed on the sign(s).</b>			
<b>Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.</b>			

<b>The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.</b>			
<b>Except for law enforcement bodies, images will not be provided to third parties unless deemed appropriate by the system controller, in line with the CCTV policy.</b>			
<b>The potential impact on individuals' privacy has been identified and taken into account in the use of the system.</b>			
<b>The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.</b>			
<b>Regular checks are carried out to ensure that the system is working properly.</b>			
<b>Academy Authorised User list has been updated.</b>			

## Appendix 2: Disclosure Request

### QEGSMAT CCTV SUBJECT ACCESS REQUEST FORM

Under the terms of the Data Protection Act 1998, an individual has the right to request a copy of any personal information held about him/her by QEGSMAT, whether it is in hard copy, electronic or CCTV.

Please complete this form, providing as much information as possible, should you wish to exercise your right in requesting disclosure of your data recorded on CCTV.

**PLEASE NOTE THAT RECORDED DATA IS HELD FOR APPROXIMATELY 28 DAYS BEFORE IT IS DELETED.**

1. PERSONAL DETAILS	
Applicant's full name:	
Applicant's postal address:	
Applicant's email address:	
2. INFORMATION REQUIRED	
<b>To help us find the CCTV data you require, please complete the following section.</b>	
Location/position of CCTV camera:	
Date image taken:	Time image taken:
Brief description of the applicant's appearance and likely activities captured by CCTV:	

A recent photograph will be required to assist identification of the relevant images.	
Any other information that might assist us in finding the information required:	
Do you require a hard copy of the image or would “viewing” the images be sufficient?	Hard copy <input type="checkbox"/> Viewing <input type="checkbox"/>
Please state reason for requesting a hard copy:	
Please give explanation of how hard copy will be kept secure:	
<b>3. DECLARATION</b>	
I confirm that all of the information I have provided is correct and that I am the Data Subject.	
Signed:	Date:
<b>OR</b> I confirm that I am acting on behalf of the Data Subject and have submitted proof of my authority to do so.	
Name:	

Postal address:	
Email address:	
Signed:	Date:
<b>4. PROOF OF IDENTITY</b>	
If you are applying on someone else's behalf, please enclose documented authority to act on the Data Subject's behalf.	
<b>5. POSTAL ADDRESS</b>	
After completing the application form, please check to ensure that all the information you have provided is accurate and all the required documents and the fee are enclosed.	
Please return the application form to:	
<b>Data Controller QEGSMAT The Green Road Ashbourne Derbyshire DE6 1EP</b>	

### Appendix 3: Internal Recording Request Form

1. STAFF DETAILS	
Name:	Signature:
2. INFORMATION REQUIRED	
Location/position of CCTV camera:	
Date image taken:	Time image taken:
Brief description of activities captured by CCTV:	
Reason for storing recorded footage:	
3. COMPLETED BY SYSTEM CONTROLLER	
Recording approved Yes/No:	
Signature:	
Date:	
CCTV Log and Digital Download Receipt must be completed before any recordings are released to staff.	

**Annexe 2 EXAMPLE CCTV Recorded Image Access Log**

CCTV Recorded Image Access Log					
Authorised Staff Name	Camera Number/Location	Date and Time of recording	Reason for Viewing (e.g. Vandalism, Behaviour incident)	Further Action Taken (e.g. any images/recordings saved or shared?)	Notes- e.g. Authorisation for sharing/retention period for retained images

**CCTV OPERATOR AGREEMENT**

People authorised to view the recordings are set out in the CCTV Policy.

I confirm I have read and understood the CCTV Policy and agree to adhere by the rules of the policy as an operator of this system.

In addition, I will update the CCTV Recorded Image Access Log each time I access the system to review a recording. I will:

- record the reason for viewing any images
- detail any retained images, why these were retained and diarise to review saved images for deletion
- I will ensure any retained images are password protected.
- I understand images including retained images must not be shared with third parties, including staff who are not part of the senior leadership team.
- any shared images must have approval for sharing from the Headteacher.

Name of authorised operator:

Signature:

Date:

I confirm that \_\_\_\_\_ is an authorised operator of the CCTV system.

Headteacher:

Date: