



CCTV Policy

Policy responsibility	Data Protection Officer Liaison
Last reviewed	June 2026
Next review due	Sept 2026
Summary of key changes	Information added regarding SARs and complaints
Approved by LGB	8 July 2026

CCTV Policy

The Trust recognises that CCTV systems can be privacy intrusive.

For this reason, the school has carried out a data protection impact assessment with a view to evaluating whether the CCTV system in place is a necessary and proportionate means of achieving the legitimate objectives set out below.

The result of the data protection impact assessment has informed the school's use of CCTV and the contents of this policy.

Objectives

Review of this policy shall be repeated regularly and whenever new equipment is introduced, a review will be conducted and a risk assessment put in place. We aim to conduct reviews no later than every two years.

The purpose of the CCTV system is to assist the Trust in reaching the following objectives:

- (a) To protect pupils, staff and visitors against harm to their person and/or property;
- (b) To increase a sense of personal safety and reduce the fear of crime and safeguarding issues;
- (c) To protect the Trust buildings and assets;
- (d) To support the police in preventing and detecting crime;
- (e) To assist in identifying, apprehending and prosecuting offenders;
- (f) To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence; and
- (g) To assist in managing the Trust and our Academies.

Purpose of This Policy

The purpose of this policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at the Trust. The CCTV system used by the Trust comprises of:

Camera Type & Number	Location	Sound	Recording Capacity	Swivel/Fixed
1. CCTV	Staff Car Park/Reception	N	Yes on a 30 day loop	Swivel
2. CCTV	Stairwell 2 in Main Building	N	Yes on a 30 day loop	Fixed
3. CCTV	Basketball Court	N	Yes on a 30 day loop	Fixed
4.	Staff Car Park at front of school	N	Yes on a 30 day loop	Fixed
5.	Girls toilets in Maths	N	Yes on a 30 day loop	Fixed
6.	Bicycle storage area	N	Yes on a 30 day loop	Fixed
7.	Neutral Toilets in main building x 2	N	Yes on a 30 day loop	Fixed
8.	Reception	N	Yes on a 30 day loop	Fixed
9.	School Hall x 2	N	Yes on a 30 day loop	Fixed
10.	Library	N	Yes on a 30 day loop	Fixed
11.	Science double doors	N	Yes on a 30 day loop	Fixed
12.	Blue Canopy – main building	N	Yes on a 30 day loop	Fixed
13.	Maths corridor double doors	N	Yes on a 30 day loop	Fixed
14.	Stairwell 1 - main building	N	Yes on a 30 day loop	Fixed
15.	Reception/Maths Entrance	N	Yes on a 30 day loop	Fixed
16.	Reception door outside camera	N	Yes on a 30 day loop	Fixed
17.	PE Corridor	N	Yes on a 30 day loop	Fixed
18.	Roundabout entrance	N	Yes on a 30 day loop	Fixed

19.	Rear of Art - outside	N	Yes on a 30 day loop	Fixed
20.	Rear of DT – outside	N	Yes on a 30 day loop	Fixed
21.	Front of School	N	Yes on a 30 day loop	Fixed
22.	Garage/Rear of School Hall	N	Yes on a 30 day loop	Fixed
23.	Maths Ground Floor	N	Yes on a 30 day loop	Fixed
24.	Maths 1 st Floor	N	Yes on a 30 day loop	Fixed
25.	Inclusion	N	Yes on a 30 day loop	Fixed
26.	Side of MFL Block	N	Yes on a 30 day loop	Fixed
27.	Roundabout/Memorial Garden/Rear of Kitchen	N	Yes on a 30 day loop	Fixed
28.	MFL Entrance	N	Yes on a 30 day loop	Fixed
29.	Pride Centre	N	Yes on a 30 day loop	Fixed
30.	Corridor 2 ADT	N	Yes on a 30 day loop	Fixed
31.	Girls Toilets in ADT	N	Yes on a 30 day loop	Fixed
32.	Boys Toilets in ADT	N	Yes on a 30 day loop	Fixed
33.	Corridor 1 in ADT	N	Yes on a 30 day loop	Fixed

CCTV cameras are in areas where individuals would have an expectation of privacy.

These are in near open space bathrooms. We have carried out a Data Protection Impact Assessment (DPIA) to assess the risks and have consulted parents prior to installing them in these areas.

Statement of Intent

CCTV cameras are installed in such a way that they are not hidden from view. Signs are predominantly 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.

The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice. It should however be noted that the school has experienced some incidents of anti social behaviour, vandalism and issues around child protection in toilet areas and as such the school feels the necessity for cameras to remain in those areas of school in particular from a Duty of Care and Child Protection perspective, which ultimately, we cannot compromise on. This decision and stance of the school will remain under review.

The Trust will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design have endeavored to ensure that the system 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.

Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 30 days.

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. In the absence of a compelling

need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 6 months.

System Management

Access to the CCTV system and data shall be password protected and will be kept in a secure area.

The CCTV system will be administered and managed by the IT Department under the direction of SLT who take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the IT Department , the system will be managed by SLT.

The system and the data collected will only be available to the IT Department, his/her replacement and appropriate members of the senior leadership team as determined by the Headteacher.

The CCTV system is designed to be in operation 24 hours each day, every day of the year, though the Trust does not guarantee that it will be working during these hours.

The IT Department will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images. Images produced by the equipment must be as clear as possible so that they are effective. To achieve this, we will ensure that:

- a. the equipment is properly installed, serviced, checked and maintained (and maintenance logs maintained) to ensure it works properly;
- b. any recording media, if needed, will be of good quality and will be replaced if the quality of the images has begun to deteriorate;
- c. where time/date of images are recordable, the equipment will be set accurately and this will be regularly checked and documented;
- d. cameras will be correctly positioned;

- e. assessments will be made as to whether constant real-time recording is necessary, or if recording can be limited to those times when suspect activity is likely to occur;
- f. cameras will be protected from vandalism so far as is possible; and
- g. if cameras break down or are damaged, the IT Department is responsible for arranging timely repair.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned above, requests access to the CCTV data or system, the IT Department must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists, access will be refused.

Details of all visits and visitors will be recorded in a system log book including time/data of access and details of images viewed and the purpose for so doing.

Downloading Captured Data on to Other Media

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings), any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures: -

- (a) Each downloaded media must be identified by a unique mark.
- (b) Before use, each downloaded media must be cleaned of any previous recording.
- (c) The IT Department will register the date and time of downloaded media insertion, including its reference.
- (d) Downloaded media required for evidential purposes must be sealed, witnessed and signed by the IT Department, then dated and stored in a separate secure evidence store. If a downloaded media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the IT Department, then dated and returned to the evidence store.
- (e) If downloaded media is archived, the reference must be noted.

- (f) If downloaded media is put onto a device, the device will be encrypted and password protected.

Images may be viewed by the police for the prevention and detection of crime and by the IT Department, his/her replacement and the Headteacher and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the Trust and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The Trust also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media, this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the Trust to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until needed by the police.

Applications received from outside bodies (e.g., solicitors or parents) to view or release images will be referred to the Trust's Data Protection Officer and a decision made by a senior leader of the Trust in consultation with the Trust's Data Protection Officer.

Requests for Access by the Data Subject

The Data Protection Act provides data subjects – those whose image has been captured by the CCTV system and can be identified - with a right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to Mrs Jaclyn Harrison.

Please refer to our Data Protection Policy with Subject Access Request appendix for further details.

If we cannot comply with the request, the reasons for not being able to comply will be documented and the data subject will be advised of these in writing.

The assigned manager responsible for the CCTV system will liaise with the Data Protection Officer, Judicium Consulting, and the school's Designated Safeguarding Lead to determine whether disclosure of the images will reveal third-party information, to assess the risks involved with disclosure and the reasonableness in disclosure.

Particular care should be exercised when images of other people are included in the materials for disclosure. Images of other individuals will, if possible, be redacted unless there would be an expectation that their images would be released in such circumstances. Non-disclosure will be appropriate in most circumstances. If there is any doubt about what information must be provided to enquirers, please contact the school's Data Protection Officer, Judicium Consulting.

Complaints

Complaints and enquiries about the operation of our CCTV systems should be made by staff in line with our Grievance Procedure available on the X Drive or, by customers and visitors, under our Data Protection Policy/Complaints Procedure, available on our website.

If a member of staff believes that there has been a breach of the Data Protection Act, or any other legal obligations, they should contact the Headteacher as a matter of urgency in accordance with the data breach reporting process set out in our Data Breach Policy.

Public Information

Copies of this policy will be available to the public from the school office.