Lowton
Church of England High School

CCTV POLICY

Original Policy Date:	**September 2018**
Date Adopted:	**December 2023**
Date of next review:	**December 2026**
Name of Responsible Person:	**Mr D Rostron**

The Governors and staff of Lowton Church of England High School are committed to the provision of a high quality education in a Christian context. We aim to provide a school where we can live out our ethos of Caring, Learning and Succeeding on a daily basis. At the heart of the commitment is the notion of the uniqueness and infinite worth of the individual, that every person is valuable in the eyes of God

This policy has been produced in accordance with the Equality Act 2010 and the Special Education Needs Disability Act 2001, the SEND Code of Practice 2014 and the Children and Families Act 2014. It has been reviewed in accordance with all other school policies and related Acts.

Signed:
Date:

Introduction

The school recognises that CCTV systems can be privacy intrusive.

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.

Objectives

The purpose of the CCTV system is to assist the school in reaching these 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;

(c) To protect the school 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 school.

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 school. The CCTV system used by the school comprises of:

Camera No.	Type	Location	Sound	Recording Capacity	Swivel/ Fixed
1	Internal	Staffroom Entrance	No	Yes	Fixed
2	Internal	Reception Entrance	No	Yes	Fixed
3	Internal	Reception Corridor	No	Yes	Fixed
4	Internal	C Block Small Canteen Servery	No	Yes	Fixed
5	Internal	Head Teacher Corridor	No	Yes	Fixed
6	External	Main Gate	No	Yes	Fixed
7	External	B Block Facing F	No	Yes	Fixed
8	External	C Block Side/B Gate	No	Yes	Fixed
9	External	B Block Facing Main Entrance	No	Yes	Fixed
10	External	G Facing B	No	Yes	Fixed
11	External	A Block Student Entrance	No	Yes	Fixed
12	External	J Block Compound	No	Yes	Fixed
13	External	J Block Back Side	No	Yes	Fixed
14	External	J Block Gate	No	Yes	Fixed
15	External	A Block Looking at B	No	Yes	Fixed
16	External	A Block Looking at H	No	Yes	Fixed
17	External	A Block Looking at J	No	Yes	Fixed
18	External	J Block Adult Ed	No	Yes	Fixed
19	External	Adult Ed Main Gate	No	Yes	Fixed

20	External	H Car Park Entrance	No	Yes	Fixed
21	External	H Block Looking At Bus	No	Yes	Fixed
22	External	B Block Delivery Store	No	Yes	Fixed
23	External	H Car Park PTZ	No	Yes	Swivel
24	External	C Block Car Park/Deliveries	No	Yes	Fixed
25	External	D Block Looking At Car Park	No	Yes	Fixed
26	External	D Looking At Gates	No	Yes	Fixed
27	External	L Block Yard	No	Yes	Fixed
28	External	Sports Pitch PTZ	No	Yes	Swivel
29	External	Sports Hall/Tennis PTZ	No	Yes	Swivel
30	External	M Block Tennis Court	No	Yes	Fixed
31	External	M Block Dance to K	No	Yes	Fixed
32	External	K Block Side to L Gate	No	Yes	Fixed
33	External	K Block SEN Main Entrance	No	Yes	Fixed
34	External	E Block to D Gate	No	Yes	Fixed
35	External	C Block Courtyard	No	Yes	Fixed
36	External	E Block to B Courtyard	No	Yes	Fixed
37	External	F Block Looking At K	No	Yes	Fixed
38	External	K Block Sports to G Gate	No	Yes	Fixed
39	External	G Block Side	No	Yes	Fixed
40	Internal	J Block Corridor	No	Yes	Fixed
41	Internal	J1 Classroom	No	Yes	Fixed
42	Internal	J Block Canteen	No	Yes	Fixed
43	Internal	H Block Toilet	No	Yes	Fixed
44	Internal	A Block Reception	No	Yes	Fixed
45	Internal	C Block Entrance 1	No	Yes	Fixed
46	Internal	C Block Dining 1	No	Yes	Fixed
47	Internal	C Block Dining 2	No	Yes	Fixed
48	Internal	C Block Entrance 2	No	Yes	Fixed
49	Internal	F Block Entrance	No	Yes	Fixed
50	Internal	F Block LRC	No	Yes	Fixed
51	Internal	E5 Classroom	No	Yes	Fixed
52	Internal	E6 Classroom	No	Yes	Fixed
53	Internal	E4 Classroom	No	Yes	Fixed
54	Internal	D4 Classroom	No	Yes	Fixed
55	Internal	D Block Entrance	No	Yes	Fixed
56	Internal	L Block Main Corridor	No	Yes	Fixed
57	Internal	L Block Fire Exit	No	Yes	Fixed
58	Internal	L Block - Girls Toilet	No	Yes	Fixed
59	Internal	L Block - Boys Toilet	No	Yes	Fixed
60	Internal	K5 Classroom	No	Yes	Fixed
61	Internal	K Block Inclusion	No	Yes	Fixed
62	Internal	K Block Entrance	No	Yes	Fixed
63	Internal	K Block Gym Corridor	No	Yes	Fixed
64	Internal	B Block Down Stairs	No	Yes	Fixed

65	Internal	B Block Up Stairs	No	Yes	Fixed
66	Internal	J Block Science Corridor	No	Yes	Fixed
67	Internal	J Block Upstairs Corridor	No	Yes	Fixed
68	Internal	J Block Upstairs	No	Yes	Fixed
69	Internal	J Block Downstairs	No	Yes	Fixed
70	External	B Block to F Side	No	Yes	Fixed
71	External	F Block Side to G Side	No	Yes	Fixed
72	External	J Block Doors	No	Yes	Fixed
73	Internal	M Block Entrance	No	Yes	Fixed
74	Internal	B1	No	Yes	Fixed
75	Internal	M Block Dance	No	Yes	Fixed
76	Internal	Canteen Counter 1	No	Yes	Fixed
77	Internal	Canteen Counter 2	No	Yes	Fixed
78	Internal	J Block Adult Ed	No	Yes	Fixed
79	Internal	J Block Reval	No	Yes	Fixed
80	Internal	J9	No	Yes	Fixed
81	Internal	Meeting Room	Yes	Yes	Fixed
82	Internal	G Block Upper Toilets	No	Yes	Fixed
83	Internal	Paper Store	No	Yes	Fixed
84	Internal	Pastoral Reception	No	Yes	Fixed
85	Internal	E Block Landing	No	Yes	Fixed
86	Internal	G Block Lower Toilet	No	Yes	Fixed
87	Internal	J Block Toilet	No	Yes	Fixed
88	Internal	A Block Upper Toilet	No	Yes	Fixed
89	Internal	H Block Stairwell	No	Yes	Fixed
90	Internal	J Block Toilet	No	Yes	Fixed
91	Internal	Fitness Foyer	No	Yes	Fixed
92	Internal	K1 Music Room	No	Yes	Fixed
93	Internal	F Block Toilet	No	Yes	Fixed
94	External	E Facing C Doors	No	Yes	Fixed
95	Internal	E Bottom Stairs	No	Yes	Fixed
96	Internal	L8 Corridor	No	Yes	Fixed
97	Internal	G Top Stairs	No	Yes	Fixed
98	Internal	G Bottom Stairs	No	Yes	Fixed

CCTV cameras are in areas where individuals would have an expectation of privacy. These are located in our wash areas. The cameras do not show inside the cubicles. We have carried out a Data Protection Impact Assessment (DPIA) to assess the risks which has been approved by our Data Protection Officer.

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.

The school 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 has endeavoured 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 approx. 1 month or when the storage disc is full.

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

1. 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 Network Manager who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager the system will be managed by the IT Technician.

The system and the data collected will only be available to the Systems Manager, 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 between the hours of or 24 hours each day, every day of the year, though the school does not guarantee that it will be working during these hours.

The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that the 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 System Manager 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.

2. 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 System Manager 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 System Manager, 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 System Manager, 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 Systems Manager, 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 school and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school 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 school 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 school's Data Protection Officer and a decision made by a senior leader of the school in consultation with the school's data protection officer.

3. Complaints About the Use Of CCTV

Any complaints in relation to the school's CCTV system should be addressed to the Headteacher.

4. Request 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 Headteacher.

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.

5. Public Information

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

Date	Description of Change
November 2022	Changes made in regard to CCTV sharing with third parties, retention and security practices around portable media devices. Formatting amendments
December 2024	Updated the CCTV camera list and included that CCTV is used in sensitive areas.
September 2025	Included additional guidance around image quality, access to and disclosure of images to data subjects and the complaints process.