Change log:	
Date	**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.
June 2025	**Change log added; expansion of objectives and definitions of appropriate use for the system; legislation, guidance, and definitions added; clarification of covert surveillance added; camera list removed; headteacher approval for access and release of footage added; note of live feed monitors added; access control limitations of workstations added; data access logging process added**

CCTV POLICY

Original Policy Date:	**September 2018**
Date Adopted:	**December 2023**
Date of next review:	**June 2027**
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.

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.

This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

Objectives

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

- To protect pupils, staff, and visitors against harm to their person and/or property;
- To increase a sense of personal safety and reduce the fear of crime;
- To protect the school buildings and assets;
- To deter criminality in school
- To support the police in preventing and detecting crime;
- To assist in identifying, apprehending, and prosecuting offenders;
- To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence; and
- To assist in managing the school.
- To assist in the resolution of any disputes that may arise in the course of disciplinary and/or grievance proceedings.
- To assist in the investigation of incidents that breach school policies, where witness statements may be supported by captured images.
- To assist in defence of any litigation proceedings.

The CCTV system will not be used to:

- Encroach upon an individual's right to privacy
- Follow individuals on live images, unless there is an on-going emergency and/or safeguarding situation.

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and the UK GDPR.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

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.

Legislation

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

Guidance

- Surveillance Camera Code of Practice (2021)

Definitions

Surveillance: the act of watching a person or a place

CCTV: closed circuit television; video cameras used for surveillance

Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

Covert surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.

Additionally, the proper authorisation forms from the Home Office will be completed and retained where necessary.

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. This period may reduce if system capacity requires the overwriting of non-archived footage.

System Management & Operation

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.

Only individuals authorised to access the system by the Headteacher will have access.

Access to the CCTV shall be limited to designated workstations. Only approved users will be able to log on to these workstations.

Upon accessing the CCTV system, an electronic record shall be completed to document the reason and focus of any use.

The only live feed monitors in use shall be those that enhance the security of the school site during day-to-day operations. These external and entry point systems are utilised only for the safeguarding of all occupants and not for monitoring of individual students and/or colleagues on a live feed. Live feed monitors are to be located only where they are non-viewable by pupils and the general public.

The headteacher shall, in liaison with the DPO, either authorise or decline disclosure of footage in response to requests from third parties.

The CCTV system is designed to be in operation for 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 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.

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 viewers of the system data 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 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.

Complaints About the Use Of CCTV

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

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 the Headteacher in the first instance.

Public Information

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