SOUTH WESTMORLAND MULTI ACADEMY TRUST

CCTV Policy

Committee:	Risk, Audit & Finance Committee
Date of adoption:	01/09/2022
Date of next review:	Autumn Term 2024

Review Sheet

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	Version Description	Date of Revision
1	Original – based on Information Commissioner's Office, Department for Education and Judicium Education guidance	27/09/2022
2		
3		
4		
5		

Contents

1. Introduction

The purpose of this of this policy is to regulate the use of Close Circuit Television and its associated technology in the monitoring of both the internal and external environs of Dallam School (hereafter referred to as 'the school).

CCTVs are installed internally and externally in the premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day.

This policy applies to all personnel, and relates directly to the location and use of CCTV, the monitoring, recording and subsequent use of recorded materials:

- The system comprises a number of fixed and dome cameras located around the school site. All cameras are monitored from a Central Control Room and are only available to selected senior staff on the Administrative Network
- This Policy follows Data Protection Act guidelines (Appendix 2,) Surveillance Cameras Code of Practice 2022
- This Policy will be reviewed bi-annually
- The Code of Practice will be subject to review to include consultation as appropriate with interested parties (This will be performed by Government bodies)
- The CCTV system is owned by the school

2. Objectives of the CCTV Scheme

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 school in reaching these objectives:

- To increase personal safety and reduce the fear of crime
- To protect pupils, staff, visitors and members of the public against harm to their person and/or property
- To protect the school buildings and their assets
- To assist in managing the school
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence

3. Statement of Intent

The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

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

Cameras will be used to monitor activities within the school and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the school, together with its visitors.

Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.

CCTV systems are not normally within the scope of the Investigatory Powers Act 2016 (IPA 2016) since they are overt and not being used for "a specific operation or investigation". In other words, it is not

directed surveillance. The school recognises that on some occasions CCTV may be used for enforcement activities. In such cases directed surveillance authorisations should be obtained, setting out what is authorised, how it will be carried out (e.g. which cameras are to be used), and what activity is to be recorded. The school will ensure that staff authorised to use the CCTV system a) understands when IPA applies and b) comply with the provisions of IPA and the terms of. The school will also ensure that authorisations are properly implemented even when acting on behalf of others, such as the police. (Appendix 1 School authorisation form).

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Data 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.

Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at strategic access routes to areas covered by the school CCTV.

Monitoring for security purposes will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies and personnel for other purposes is prohibited e.g. monitoring of political or religious activities, or employee and/or pupil evaluations that would undermine the acceptability of the resources for use regarding critical safety and security objectives.

CCTV monitoring of public areas, for security purposes, will be conducted in a manner consistent with all existing policies adopted by the school including Discrimination, Bullying and Harassment, Sexual Harassment etc.

The code of practice for video monitoring prohibits monitoring based on the characteristic and classification contained in Equality and other related legislation, for example race, gender, sexual orientation, national origin, disability etc.

The system is in place to monitor suspicious behaviour and not individual characteristics

Video monitoring of public areas, for security purposes is limited to uses that do not violate the reasonable expectation of privacy as defined by Law

Consideration will be given to both staff and pupils regarding possible invasions of privacy and confidentiality due to the location of a particular CCTV camera or associated equipment

The Headteacher will ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place.

The camera control will be monitored to ensure it is not in breach of the intrusion on intimate behaviour by persons in public changing and toilet areas.

When a zoom facility on a camera is being used, a second person will be present with the camera operator to guarantee that there is no unwarranted invasion of privacy.

4. Operation of the System

The Scheme will be administered by the ICT Manager and managed by the Headteacher, in accordance with the principles and objectives expressed in the code. The day-to-day management will be the responsibility of the ICT Manager, School Business Manager and the Premises, Health & Safety Manager.

Access to the CCTV management system will be restricted to those authorised by the Headteacher.

The CCTV system will be operated 24 hours each day, every day of the year.

The CCTV system will be password protected and only users authorised by the Headteacher will receive passwords to access the system.

Authorised CCTV user's passwords, must remain confidential to the user.

5. Control Room (IT Office – Room 143)

The ICT Manager will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

Access to the CCTV management system will be restricted to those authorised by the Headteacher – these include the ICT Manager, School Business Manager and the Premises, Health & Safety Manager.

Unless an immediate response to events is required, staff with access authorisation must not direct cameras at an individual or a specific group of individuals.

Control Room Operators must satisfy themselves over the identity of any other visitors to the Control Room and the purpose of the visit. Where any doubt exists access will be refused.

Details of all maintenance access to the CCTV system will be endorsed in the Control Room log book. The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual access to the CCTV system will not be permitted.

The CCTV system access log book will be maintained in the Control Room. Full details of visitors including time/data of entry and exit will be recorded.

During the working day and out of hours when the control room is not occupied access to the CCTV system must be kept secured.

Other administrative functions will include maintaining image and data recording and hard disc space, filing and maintaining occurrence and system maintenance logs.

Emergency procedures will be used in appropriate cases to call the Emergency Services.

6. Liaison

Liaison meetings may be held with all bodies involved in the support of the system.

7. Monitoring Procedures

Camera surveillance may be maintained at all times.

An ICT system data storage device is installed in the Control Room to which pictures will be continuously recorded.

Strict ICT system controls exist, within the control room, to restrict access to the monitoring equipment.

8. Recording Procedures

In order to maintain and preserve the integrity of the data used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- Data is recorded to NAS and stored for 21 days

- When an event needs recorded for evidential purpose it will be archived on DVD
- DVD required for evidential purposes must be sealed, witnessed, signed by the controller, dated and authorized by the Headteacher before the DVD is released
- If the DVD is archived the reference must be noted

Data may be viewed by the Police for the prevention and detection of crime, authorised officers of Cumbria County Council for supervisory purposes, authorised demonstration and training.

A record will be maintained of the release of data to the Police or other authorised applicants. A register will be available for this purpose. Viewing of data by the Police must be recorded in writing and in the log book. Requests by the police can only be actioned under section 29 of the Data Protection Act 1998.

Should a DVD be required as evidence, a copy may be released to the Police under the procedures described previously in this policy. Data will only be released to the Police on the clear understanding that the tape remains the property of the school, and both the DVD and information contained on it are to be treated in accordance with this policy. The school also retains the right to refuse permission for the Police to pass to any other person the DVD or any part of the information contained thereon.

The Police may require the school to retain the stored data for possible use as evidence in the future. Such data will be properly indexed and properly and securely stored until they are needed by the Police.

Applications received from outside bodies (e.g. solicitors) to view or release data will be referred to the Headteacher. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

9. Breaches of the Policy (including breaches of security)

Any breach of the 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 the policy will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach. Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the school, or a student.

10. Assessment of the CCTV System and the Code of Practice

Performance monitoring, including random operating checks, may be carried out by the ICT Manager, School Business Manager or Premises, Health & Safety Manager.

11. Complaints

Any complaints about the school's CCTV system should be addressed to the Headteacher. Complaints will be investigated in accordance with Section 9 of this Code.

12. 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 Headteacher.

13. Public Information

Copies of this Policy will be available to the public to read from the School office. Staff access will be available on the school's intranet (R Drive).

14. Summary of Key Points

(i) This Policy will be reviewed bi-annually
(ii) The CCTV system is owned and operated by the school
(iii) The Control room will not be manned out of school hours
(iv) The Control Room is not open to visitors except by prior arrangement and good reason
(v) Liaison meetings may be held with the Police and other bodies
(vi) Recording data will be used properly indexed, stored and destroyed after appropriate use
(vii) Data may only be viewed by Authorised School Officers, Control Room staff and the Police
(viii) Data required as evidence will be properly recorded witnessed and packaged before copies are released to the police
(ix) Data will not be made available to the media for commercial or entertainment
(x) Data will be disposed of securely by the ICT Manager
(xi) Breaches of the code and remedies will be reported to the Headteacher
(xii) Any breaches of this policy will be investigated by the Headteacher. An independent investigation will be carried out for serious breaches