



DIOCESE OF SOUTHWELL
& NOTTINGHAM

MULTI ACADEMY TRUST

SNMAT

Security Camera Policy

A reference policy for SNMAT schools

Policy:	Security Camera Policy – A reference policy for SNMAT schools
Approved by:	
Date:	September 2024
Review Cycle:	Annual

Versions:			
VERSION	DATE	AUTHOR	CHANGES
2024	SEPT 2024	MJH – Trust IT Manager	Based upon SCA policy. Thanks to Donna Barnes. Converted to a template and expanded. Added Keeping Children Safe in Education 2024.
2025	APRIL 2025	MJH	Highlighted required changes. Minor formatting changes.

CONTENTS

CONTENTS.....	3
EXECUTIVE SUMMARY	4
RATIONALE	4
SCOPE.....	4
ROLES & RESPONSIBILITIES	5
LOCAL GOVERNING BODIES	5
THE PRINCIPAL/HEADTEACHER.....	5
GDPR	6
LEGISLATION	6
OPERATION	6
ACCESS TO DATA.....	7
ACCESS AUTHORISATIONS	7
DATA RETENTION.....	8
MAINTENANCE.....	8
MANAGEMENT & CONFIGURATION	8
CONSENT AND NOTIFICATION	9
COMPLAINTS.....	9
REVIEW AND MONITORING	10
APPENDIX 1 – STAFF ACCESS RIGHTS.....	11
APPENDIX 2 – CAMERA LOCATIONS & TYPES	12

EXECUTIVE SUMMARY

At Hucknall National C of E Primary School, we take our responsibility towards the safety of staff, visitors and students very seriously. We expect all people to behave responsibly and safely but use security cameras to safeguard school assets and monitor any instances of aggression or physical damage to our site and our community.

RATIONALE

The purpose of this policy is to manage and regulate the use of the security camera systems at the academy. It is to ensure that we comply with relevant legislation and that systems are secure and suitable for purpose.

The rationale behind the installation of a security camera system was an operational decision from SNMAT to fit with the scope outlined in this policy and support safety and security at the Academy.

SCOPE

This policy covers the use of security camera systems on the Academy estate where video and image are recorded and viewed of individuals who could be identified, as well as information relating to individuals for any of the following purposes:

- Protecting the school buildings and school assets, both during and after school hours;
- Reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- Assisting in the investigation of safeguarding incidents, accidents and other incidents;
- Using video, images or audio (audio switched off unless required in line with the policy) that could affect their privacy;
- Supporting the Police or other agencies in a bid to deter and detect crime;
- To provide a safe and secure environment for pupils, students, staff and all visitors.

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.

The surveillance system will not be used:

- To monitor staff or staff performance.
- For covert surveillance, which is any use of surveillance which is intentionally not shared with the subjects it is recording. The school does not condone the use of covert surveillance.
- There will be no recording of biometric data (data which is related to the physiological characteristics of a person, which confirm the unique identification of that person, such as fingerprint recognition, facial recognition (FRT), or iris recognition).
- There will be no automated biometric recognition system (a system which uses technology to measure an individual's physical or behavioural characteristics by using equipment that operates 'automatically').
- There will be no use of facial recognition technology (the process by which a person can be identified or otherwise recognised from a digital facial image.)

Be subject to stringent security measures to safeguard against unauthorised access.

Be regularly reviewed and audited to ensure that policies and standards are maintained.

Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.

- The use of the system is at the headteacher's discretion and will only be used within the remit of the policy and if absolutely necessary.

ROLES & RESPONSIBILITIES

LOCAL GOVERNING BODIES

1. It is the responsibility of the governing body to ensure there is management of security cameras within the school and the school meets the relevant statutory legislation requirements.

THE PRINCIPAL/HEADTEACHER

2. It is the responsibility of the principal/headteacher to ensure that the day-to-day effectiveness of this policy school is maintained.
3. The principal/headteacher must ensure that adequate and effective consultation, notification and training is provided to staff to understand and adhere to the policy and its procedures. The consultation will allow time for feedback and reviews to be recorded and considered before implementation.
4. The principal/headteacher must ensure that the authorisations and locations of access to cameras and locations as detailed in the appendices are enacted and supported in an effective manner.
5. Dealing with freedom of information requests and subject access requests (SARs) in line with legislation, including the Freedom of Information Act 2000.
6. Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
7. Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
8. Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
9. Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
10. Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
11. Presenting reports regarding data processing at the school to senior leaders and the governing board.
12. Processing surveillance and CCTV footage legally and fairly.
13. Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
14. Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.

15. Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
16. Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure.

GDPR

The Diocese of Southwell and Nottingham Multi Academy Trust (SNMAT) is the corporate body registered with the Information Commissioners' Office as a Data Controller.

The security camera system is owned and operated by the school and the deployment of which is determined by the school's headteacher. The security camera is a standalone system and operated by the school.

LEGISLATION

This policy has due regard to legislation including, but not limited to, the following:

- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- The UK General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Education (Student Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998
- Children Act 1989
- Children Act 2004
- Equality Act 2010
- Keeping Children Safe in Education 2025

This policy has been created regarding the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2017) 'In the picture: A data protection'

OPERATION

The use of the security camera system will be conducted in a professional, ethical and legal manner and any diversion of the technologies for other purposes is prohibited by this policy e.g. Cameras will not be used for monitoring employee performance.

Monitoring of restricted access areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the academy, including Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and other educational and related legislations.

- The Academy will only use security cameras for the safety and security of the site and its staff, students and visitors.
- Adequate signage will be placed so all members of the academy community are aware that they are entering an estate which is covered by security camera equipment.
- The Academy will only use security cameras as a deterrent and cameras will not be used in toilets or changing facilities.

ACCESS TO DATA

Access to the camera system, live data and historical data will be restricted to authorised personnel only. The system can only be accessed by username and password encryption with multi-factor authentication where possible on authorised devices. The system software keeps a log of when the authorised user accesses the system or stored media.

ACCESS AUTHORISATIONS

All authorised operators with access to recorded images are aware of the procedures that need to be followed when accessing the images. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

Only the site manager and office manager have access to the recording system and their access is only granted within the scope of this policy. The Chair of Governors will monitor the log of access every month to check appropriate use.

The headteacher or designated person will not have access to the camera devices unless a risk assessment for access has been completed and signed off by the Chair of Governors. The headteacher may access the system in an emergency where no alternative is available and the safety of pupils, staff or other adults was compromised and a review of this decision was completed after access and signed off by the Chair of Governors.

A record of the date of any disclosure request along with details of who the information has been provided to (the name of the person and the organisation they represent), why they required it and how the request was dealt with will be made and kept, in case of challenge.

In relevant circumstances, security camera footage may be accessed:

1. By the police where the academy is required by law to make a report regarding the commission of a suspected crime;
2. Following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on school's property;
3. To the HSE and/or any other statutory body charged with child safeguarding; or
4. To assist the Headteacher or member of SLT, DSL in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed;
5. To data subjects (or their legal representatives), pursuant to a Subject Access Request;

6. To individuals (or their legal representatives) subject to a court order;
7. To the school insurance company where the insurance company requires evidence in order to pursue a claim for damage done to the insured property.

DATA RETENTION

The camera system is configured to retain footage for 30 days after which it will be automatically deleted and permanently erased.

If the footage is required specifically for an investigation or prosecution in that issue, then data will be stored in a secure environment.

Access to any data will be restricted to authorised staff only.

In certain circumstances, the recordings may also be viewed by other individuals to achieve the objectives set out above. When security camera recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

Where data requests contain the personal data of a separate individual, the rights and freedoms of others will be protected by asking for their consent, or removing specific footage where appropriate.

Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers as part of a court order
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

Requests for access or disclosure will be recorded and the headteacher will make the final decision as to whether recorded images may be released to persons other than the police.

MAINTENANCE

The responsibility for maintenance of the camera security system lies with the school site team.

MANAGEMENT & CONFIGURATION

The Headteacher/Principal should work closely with the Site Team, DSL and IT Support Team and service providers to ensure that the camera security system meets with the needs of the academy.

The responsibility for determining where cameras are located, how they operate and the configuration of systems and lies with The Headteacher/Principal.

Staff will be trained in security procedures, and sanctions will be put in place for those who misuse security system information. Staff will be made aware that they could be committing a criminal offence if they do this.

The ability to produce copies of information will be limited to the appropriate staff.

The surveillance system is a closed digital system.

Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

The surveillance system will not be used to focus on a particular group or individual unless an immediate response to an incident is required.

The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

The school will not record audio unless it has:

- Identified a particular need or issue and can evidence that this need must be addressed by audio recording;
- Considered other less privacy intrusive methods of achieving this need;
- Reviewed the other less privacy intrusive methods and concluded that these will not appropriately address the identified issue and the only way to do so is via the use of audio recording.
- Audio recording can be isolated to individual recording devices.

Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.

The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the school's website.

CONSENT AND NOTIFICATION

A copy of this policy will be provided on request to staff, students, parents and visitors to the school and will be made available on the school website.

COMPLAINTS

Complaints and enquiries about the operation of security cameras within the academy should be directed to the Principal/Headteacher in the first instance.

REVIEW AND MONITORING

The application and outcomes of this policy will be monitored and reviewed annually to ensure it is working effectively.

APPENDIX 1 – STAFF ACCESS RIGHTS

Access	Staff Members	Note
FULL	Site manager or delegated authority. Office manager or delegated authority. SNMAT IT Services CBC (CCTV provider)	2 factor authorisation. Access to be monitored and logged. For maintenance purposes only.
VIEW-ONLY	Headteacher or delegated authority. View requested and reasons stated and recorded.	Regular checks of access record for monitoring purposes.

APPENDIX 2 – CAMERA LOCATIONS & TYPES

[illegible]