Meadowhead School Academy Trust

Surveillance Camera System Policy and Operator Code of Practice

This is a policy of Meadowhead School. Meadowhead School is a Foundation School and a member of the Meadowhead Community Learning Trust

Policy Lead	Kevin Elliott
Date written	September 2023
Review date	September 2024
Approval by governors	20th November 2023

1. Objectives

Meadowhead School Academy Trust has a surveillance system consisting of a number of cameras mounted externally and internally that constantly record moving images for reviewing by authorised personnel.

The Trust records these images for the prevention, identification of crime and anti-social behaviour, to monitor the Trust buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to Trust property.

The purpose of this policy is to manage and regulate the use of the surveillance camera systems at the Trust and ensure that;

- We comply with data protection legislation, including the Data Protection Act 2018 and the General Data Protection Regulation (UK GDPR)
- Authorised staff operating the system are clear on their responsibilities around data protection and handling.
- The system is fit for purpose and the images that are captured are usable for the purposes we require them for
- We can reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

2. Definitions

For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

Surveillance camera system - The system of cameras and recording devices.

Why not call it CCTV? CCTV stands for ‘closed circuit television’. It originated when such systems worked on a closed circuit (as opposed to broadcast television which everyone could receive). These days most “CCTV” systems are in fact cameras connected to networks, neither on a ‘closed circuit’ or a ‘television’ in the common definition. Whilst still in common use, the term ‘CCTV’ is no longer accurate, can be misleading and may lead to data risks not being highlighted.

Surveillance – Monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.

Overt surveillance – Any surveillance where the subject is made aware of the cameras and purpose of the recording. The cameras are clearly visible and signage informs data subjects of their presence.

Covert surveillance – Any use of surveillance which is intentionally **not** shared with the subjects it is recording. Cameras are hidden or not obvious. Subjects are not informed of such surveillance.

Data Controller - An organisation that is responsible for gathering and processing personal data (including video images) as defined by the data protection act 2018

3. Legal framework

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

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)

This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2021) '*The Surveillance Camera Code of Practice*'
- ICO guidance on the use of surveillance camera systems (this replaced the 'ICO code of practice')

This policy operates in conjunction with the following Trust policies:

- Privacy notices for staff, pupils and parents
- Safeguarding Policy
- Freedom of Information Policy
- Data Protection Policy

4. Roles and responsibilities

Meadowhead School Academy Trust, as the corporate body, is registered with the ICO as a **data controller** and is responsible for any recorded footage that may count as personal data under the DPA 2018

The governing board of Trust therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with the regulations.

The surveillance camera system is owned and managed by the Trust and images from the system are strictly controlled and monitored by authorised personnel only.

In addition to the internal system, Kier Ltd, the trusts PFI provider, own and operate a separate system that covers the external areas around the school building including the carpark. With permission the trust has access to this separate system but Kier own and operate this system. This policy does not cover the Kier external system.

The role of the **data controller** includes:

- Collecting surveillance camera footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance camera footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Processing surveillance camera footage legally and fairly.
- Ensuring that any surveillance camera footage identifying an individual (personal data) is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

The role of the data protection officer (DPO) includes:

- Reviewing the Surveillance Camera System Policy to ensure it is compliant with current legislation.
- Advising on freedom of information requests (FOIR) and subject access requests (SAR).
- Ensuring that authorised operators at the Trust handle and process surveillance camera footage in accordance with data protection legislation.
- Ensuring that surveillance camera footage is obtained in line with legal requirements.
- Ensuring that surveillance camera footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Informing data subjects of how their data captured in surveillance camera footage will be used by the Trust, their rights for the data to be destroyed and the measures implemented by the Trust to protect individuals' personal information.
- Monitoring the performance of the systems data protection impact assessment (DPIA), and providing advice where requested.
- Monitoring legislation to ensure the Trust is using surveillance fairly and lawfully.
- Communicating any changes to legislation to data leads.

5. The data protection principles

In line with the Data Protection Act 2018 all data collected from the surveillance camera system will be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical

purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. Data protection by design and default: The trust along with the DPO will complete a DPIA on any installation of a new system, or changes to an existing system including, upgrading, expansion, increase in the number of users, change in purpose of system. This will be used to justify any changes, highlight and address security and data protection risks, these risks will be communicated to the installers and operators. They must be addressed and the risks minimised or eliminated before the system is commissioned and signed off.

7. System protocols

1. The surveillance system is registered with the ICO in line with data protection legislation.
2. The surveillance system is a digital video system which will not be used to record audio. Where the system has this feature it will be disabled.
3. Signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's **Code of Practice**.
4. The Trust cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.
5. The system will not be used for **covert** surveillance.
6. Cameras will not be located in general classrooms for monitoring of pupils or staff. In certain specialist areas such ICT suites cameras may be used for the security of equipment. In other specialist areas such as 'The Bridge' including but not limited to the ISR, SEN areas and engagement centres, cameras are located for the safety of students and staff.
7. Cameras will not be located in changing facilities or other areas where recording would have an unacceptable impact on privacy. Some cameras are located to capture washing areas where the school has had issues of vandalism and attempted arson. These cameras are carefully positioned to avoid capturing the inside of toilet cubicles.
8. The Trust makes every effort to position cameras so that their coverage is restricted to the school premises and inclusion of adjacent private buildings and property is minimised.
9. The system will be transparent and include a contact point, the Trust data lead, through which people can access information and submit complaints.
10. The system will have clear responsibility and accountability procedures for images and information collected, held and used.
11. The system will restrict access to retained images and information with clear rules on who can gain access. (See section 10)
12. The system will be subject to stringent security measures to safeguard against unauthorised access. (See section 8)
13. The system will only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff, visitors and volunteers, and law enforcement.
14. The system will be accurate and well maintained to ensure information is up-to-date. For example checking any date and time stamp is accurate.
15. Software will be updated regularly to maintain system integrity.
16. Faulty cameras or equipment will be replaced quickly

8. Security of hardware and recorded images

1. Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.
2. The trust's authorised system operators are detailed in Appendix 2:
3. All factory set default passwords will be changed.
4. All passwords will be complex and will be kept secure.
5. Remote access will be securely protected using two factor authentication.
6. The location of the system recording devices will be kept locked when not in use.
7. The surveillance camera system will be tested for security flaws regularly to ensure that they are being properly maintained at all times.
8. Display monitors are only visible located in the reception area.
9. Where an external third party company is engaged to maintain the system they will not be allowed to review footage beyond basic testing of the system using footage of their own employees.

9. Code of practice for authorised operators

1. The Trust understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.
2. The Trust notifies all pupils, staff and visitors of the purpose for collecting surveillance data via privacy notices and clear signage.
3. Only authorised operators will have access to the system
4. All surveillance footage will be kept for around one month depending on the system capacity;
5. Operators will only review footage with a clear purpose which must be recorded.
6. Where possible, reviewing of the footage should be done in the presence of two authorised operators. Footage must not be reviewed in an area where other unauthorised persons can observe.
7. Access to any footage must be logged with data, reason for access and the names of the observers.
8. Any footage taken offline will be stored securely and only on Trust devices or systems.
9. Any footage shared with 3rd parties must be shared securely using encryption, password protection or other secure method.
10. Authorised operators will keep their account credentials secure at all times and will not share their account with anyone else.
11. Operators will report any technical issues quickly so any down time of the system is minimised

10. Access to recordings

1. Under the data protection act 2018, individuals have the right to obtain confirmation that their personal information is being processed.
2. All disks containing images belong to, and remain the property of, the Trust.
3. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data including recordings.
4. The Trust will verify the identity of the person making the request before any information is supplied.

5. A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.
6. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
7. Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the trust lead, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.
8. Where a request is manifestly unfounded, excessive or repetitive, it may be refused or a reasonable fee will be charged.
9. All fees will be based on the administrative cost of providing the information.
10. All requests will be responded to without delay and at the latest, within one month of receipt.
11. Where recorded footage contains the identifiable images of any persons other than the data subject, then it may not be possible to release the footage/images unless it is possible to anonymise the identities of the other individuals featured.
12. In the event of numerous or complex requests, the period of compliance may be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
13. Where a request is manifestly unfounded or excessive, the Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.
14. In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.
15. It is important that access to, and disclosure of, the images recorded by surveillance camera 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.
16. 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:
    a. The police – where the images recorded would assist in a specific criminal inquiry
    b. Prosecution agencies – such as the Crown Prosecution Service (CPS)
    c. Relevant legal representatives – such as lawyers and barristers
    d. Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation
17. Any third party must complete a data request form (See Appendix 5)
18. Requests for access or disclosure will be recorded and the Trust lead will make the final decision as to whether recorded images may be released to persons other than the police.

11. Storage and retention

Footage will be stored for 28 days. After this period the system is set to automatically overwrite the footage. Any footage exported for the investigation of an incident will be kept securely until after the incident is resolved. Then it will either be destroyed or kept permanently depending on the nature of the incident.

12. Complaints

Complaints and enquiries about the operation of surveillance systems within the Trust should be directed to the school business manager in the first instance.
If you are not satisfied with the response provided you have the right to contact the ICO: https://ico.org.uk/make-a-complaint/

13. Policy monitoring and review

1. This policy will be monitored and reviewed on a biennial basis by the DPO and the trust lead
2. The DPO will be responsible for monitoring any changes to legislation that may affect this policy, and recommending that the Trust make the appropriate changes accordingly.
3. The trust lead will communicate changes to this policy to all members of staff.

Appendix 1: Technical details of system

System type	NVR
Manufacturer	Hikvision
Owner/Operator	Meadowhead School Academy Trust
Software	Hikvision
Update/patching interval	monthly/termly/annually
Date of installation	
Number of cameras	32 cameras on each NVR
Type of cameras	fixed/dome/PTZ
Internal/external or both	All internal cameras except one external camera
Constant recording	24/7/365 or movement detection only
Access type	Software client/direct control
Installation/maintenance contractor	
Maintenance review period	Monthly/Annually
Remote monitoring allowed	Trust staff / 3rd party security company
Retention period	28 days

Appendix 2: Authorised Users

Name	Job Title
	Head Teacher
	Business Manager
	Safeguarding Lead

Appendix 3: Location of cameras

Camera location and type	Internal or external	Audio enabled or disabled	Live monitoring allowed?
Fixed camera above main entrance	External	Disabled	No
PTZ camera in main carpark	External	Disabled	No
ADT Staircase to Fire Exit	Internal	Disabled	No
ADT Looking towards D05 D06	Internal	Disabled	No
ADT Outside D05	Internal	Disabled	No
ADT Thin Corridor Outside D04	Internal	Disabled	No
ADT Thin Corridor Outside D02	Internal	Disabled	No
ADT Outside Toilets	Internal	Disabled	No
ADT Looking towards Offices	Internal	Disabled	No
ADT Outside Toilets Looking towards Fire Exit	Internal	Disabled	No
ADT Girls Toilets	Internal	Disabled	No
ADT Boys Toilets	Internal	Disabled	No
ADT Near Cafe	Internal	Disabled	No
Languages Boys Toilets	Internal	Disabled	No
Languages Girls Toilets	Internal	Disabled	No
Languages Looking towards offices	Internal	Disabled	No
Languages Outside L03	Internal	Disabled	No
Languages Outside L04	Internal	Disabled	No
Languages Outside L14	Internal	Disabled	No
Languages Outside Faculty office	Internal	Disabled	No
Languages Staircase to Fire Exit	Internal	Disabled	No
Languages Outside L07	Internal	Disabled	No
Science facing internal staircase	Internal	Disabled	No
Science Facing towards S06	Internal	Disabled	No
Science Outside Prep Room	Internal	Disabled	No
Science Outside S08	Internal	Disabled	No

Science Facing NSS Office	Internal	Disabled	No
Science Outside S08	Internal	Disabled	No
Science Boys Toilets	Internal	Disabled	No
Science Girls Toilets	Internal	Disabled	No
Science Outside Toilets	Internal	Disabled	No
Science Back Stairs	Internal	Disabled	No
Science Facing S12	Internal	Disabled	No
Humanities Boys Toilets	Internal	Disabled	No
Humanities Girls Toilets	Internal	Disabled	No
Humanities Pastoral Office	Internal	Disabled	No
Humanities Outside H07	Internal	Disabled	No
Humanities Outside Toilets	Internal	Disabled	No
Humanities Facing Open End	Internal	Disabled	No
Humanities Back Stairs	Internal	Disabled	No
Humanities Facing H03	Internal	Disabled	No
Humanities Facing Offices	Internal	Disabled	No
PE Facing Fire Exit	Internal	Disabled	No
PE Facing Sports Hall	Internal	Disabled	No
PE Staircase	Internal	Disabled	No
PE Outside Fitness Suite	Internal	Disabled	No
PE Outside Activity Hall 2	Internal	Disabled	No
PA Facing Practice rooms	Internal	Disabled	No
PA Facing PA1	Internal	Disabled	No
PA Engagement Center	Internal	Disabled	No
Kitchen Corridor	Internal	Disabled	No
Maths Outside Toilets	Internal	Disabled	No
Maths Girls Toilets	Internal	Disabled	No
Maths Boys Toilets	Internal	Disabled	No
Maths Facing Offices	Internal	Disabled	No
Maths Staircase to Fire Exit	Internal	Disabled	No

Maths Facing M07	Internal	Disabled	No
Maths Facing M03	Internal	Disabled	No
Maths Facing M13	Internal	Disabled	No
Bridge Facing IER	Internal	Disabled	No
Bridge IER	Internal	Disabled	No
Bridge EC Office	Internal	Disabled	No
Bridge EC Classroom	Internal	Disabled	No
Bridge Fire Escape	Internal	Disabled	No
Bridge Facing Toilets	Internal	Disabled	No
Sixth form Common Room	Internal	Disabled	No
Sixth form Common Room Facing Office	Internal	Disabled	No
Sixth Form Facing Café	Internal	Disabled	No
Sixth Form Entrance	Internal	Disabled	No
Sixth Form Ground Floor Stairs	Internal	Disabled	No
Sixth Form First Floor Stairs	Internal	Disabled	No
Sixth Form Rear Entrance	Internal	Disabled	No
Sixth Form Work Area 1	Internal	Disabled	No
Sixth Form Work Area 2	Internal	Disabled	No
Café Lift	Internal	Disabled	No
Café Facing PE	Internal	Disabled	No
Café Pronto	Internal	Disabled	No
Café Tills	Internal	Disabled	No
Café Facing Rosling	Internal	Disabled	No
Café Vending Machines	Internal	Disabled	No
Mezzanine 1	Internal	Disabled	No
Mezzanine 2	Internal	Disabled	No
Outside Finance	Internal	Disabled	No
Outside Heads Office	Internal	Disabled	No
LRC Facing Office	Internal	Disabled	No
Rosling Outside English Lift	Internal	Disabled	No

Rosling Outside Humanities	Internal	Disabled	No
Rosling Outside Staff Room	Internal	Disabled	No
Rosling Outside Safeguarding Office	Internal	Disabled	No
Rosling Outside Science	Internal	Disabled	No
Rosling Main Entrance	Internal	Disabled	No
Rosling Facing Rosling from Entrance	Internal	Disabled	No
Rosling Facing English Stairs	Internal	Disabled	No
Rosling Outside Maths	Internal	Disabled	No
Hall Facing Stage	Internal	Disabled	No
Hall Facing Right Fire Exit	Internal	Disabled	No
Hall Facing Left Fire Exit	Internal	Disabled	No
Rosling Middle	Internal	Disabled	No
Rosling Outside Cafe	Internal	Disabled	No
English Boys Toilets	Internal	Disabled	No
English Girls Toilets	Internal	Disabled	No
English Pastoral Office	Internal	Disabled	No
English Outside E07	Internal	Disabled	No
English Facing Open End	Internal	Disabled	No
English Back Stairs	Internal	Disabled	No
English Facing E03	Internal	Disabled	No
English Facing Offices	Internal	Disabled	No
English Outside IT office	Internal	Disabled	No

Appendix 4: Review Log

Any authorised staff who requires to review footage needs to have a second authorised staff member with them and must complete this form detailing why the review is required.

Date	Reason for review	Staff name 2	Staff name 1

Appendix 5: Data request by third party

Person requesting: Police Officer / Data Subject or Third Party name	
Police Station / Third Party Address	
Contact number	
Contact email	
Crime / Incident no / Reason for Access	
Reason for request	Legal Proceedings / Subject Access / Other
Date of incident or footage	
Time of incident or footage	
Location of incident or cameras applicable	
Decision to comply with request or reason for refusal?	
Secure method of provision	Upload to secure portal / encrypted removable media
Authorised staff	
Date footage provided	
Signature of recipient	
Date of destruction / return	
Method of Destruction	
Operator	