



SURVEILLANCE CAMERA SYSTEM POLICY AND OPERATOR CODE OF PRACTICE

Policy control table			
Policy title:		Surveillance Camera System Policy And Operator Code Of Practice	
Author:		David Thorpe	
Policy Version:		1	
Approved on:			
Approved by:			
Date Reviewed		Review Date: July 2025, Sept 2026	
Document History			
Version	Date	Author	Note of revisions
1	October 2024	David Thorpe	

Contents

Objectives.....	3
2. Definitions.....	3
Legal framework.....	4
Roles and responsibilities	4
The data protection principles.....	5
System protocols	6
Security of hardware and recorded images	76
Code of practice for authorised operators.....	7
Access to recordings.....	8
Storage and retention	9
Complaints.....	9
Policy monitoring and review	9
Appendix 1: Technical details of system – Rawmarsh.....	10
Technical details of system – Hutton Park.....	10
Technical Details - Catcliffe.....	11
Appendix 2: Authorised Users	12
Appendix 3:	13
Location of Cameras Hutton Park.....	13
Location of cameras Rawmarsh.....	14
Location of Cameras at Catcliffe	15
Appendix 4: Review Log.....	17
Appendix 5: Data request by third party	18

Objectives

Rotherham Aspire has a surveillance system consisting of a number of cameras mounted externally and internally that constantly record moving images for reviewing by authorised personnel.

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

The purpose of this policy is to manage and regulate the use of the surveillance camera systems at Rotherham Aspire 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 recorded video, audio or live footage.

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

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, or iris recognition.

Facial recognition – the process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and facial recognition technology software produces a biometric template.

Automated biometric recognition system – a system which uses technology to measure an individual's physical or behavioural characteristics by using equipment that operates automatically.

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 school policies:

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

Roles and responsibilities

Rotherham Aspire, 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. This is carried out annually via DD recurring. (<https://ico.org.uk/ESDWebPages/Entry/ZA555613>)

The Management Committee of the school 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 Rotherham Aspire and images from the system are strictly controlled and monitored by authorised personnel only.

Commented [1]: A PFI contractor should have a policy for any system they control

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 Rotherham Aspire 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 Rotherham Aspire, their rights for the data to be destroyed and the measures implemented by Rotherham Aspire 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 Rotherham Aspire is using surveillance fairly and lawfully.
- Communicating any changes to legislation to data leads.

The data protection principles

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

- Processed lawfully, fairly, and in a transparent manner in relation to individuals.
- 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.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 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.
- 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.
- 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.
- Data protection by design and default: The school 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.

System protocols

- The surveillance system is registered with the ICO in line with data protection legislation.
- 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.
- Signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Guidance.
- Rotherham Aspire cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.
- The system will not be used for **covert** surveillance, or
- The system will not be used for **overt** surveillance except for specific cases regarding safeguarding. here the surveillance officer must gain permission from the Head of School or the Deputy Head of School.-
- Cameras will be located in general classrooms but will not be used for the live monitoring of pupils or staff on a day-to-day basis. However, all areas may be subject to live monitoring for short periods of time for reasons of safeguarding. This is a justifiable action and will be carried out when deemed essential by the senior leader in charge of each centre, to ensure student and staff safety is maintained.
- The assessment of teachers will only ever be carried out using the IRIS system as per the joint union agreement but this is not currently used at Rotherham Aspire. At no point will live surveillance be used for the assessment or monitoring of teachers or other staff.
- Cameras will not be located in toilets or changing facilities or other areas where recording would have an unacceptable impact on privacy.
- Rotherham Aspire 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.
- The system will be transparent and include a contact point, which is the Rotherham Aspire data lead to whom people can access information and submit complaints to be passed to the Head Teacher/Management Committee.
- The system will have clear responsibility and accountability procedures for images and information collected, held and used.
- The system will restrict access to retained images and information with clear rules on who can gain access. (See section 10)
- The system will be subject to stringent security measures to safeguard against unauthorised access. (See section 8)
- The system will 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 system will be accurate and well maintained to ensure information is up-to-date. For example, checking any date and time stamp is accurate.
- Software will be updated regularly to maintain system integrity.
- Faulty cameras or equipment will be replaced quickly

Commented [2]: IT classrooms?

Security of hardware and recorded images

- Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.
- The school's authorised system operators are detailed in Appendix 2:
- All factory set default passwords will be changed.
- All passwords will be complex and will be kept secure.
- Each authorised operator will have their own account.
- The location of the system recording devices will be kept locked when not in use.
 - Hutton Park – Secure mentors room in A block.
 - Catcliffe - Secure office.
 - Rawmarsh - Secure Cupboard classroom 4.
- The surveillance camera system will be tested regularly. Any issues or faults will be fixed quickly and any faulty hardware will be replaced promptly to ensure consistent operation of the system.
- Where applicable the surveillance camera system software will be updated and patched regularly to ensure security is maintained.
- Display monitors are only located and visible in a secure location. They may only available to be viewed by the authorised operator and senior leaders at all sites.
- 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.

Code of practice for authorised operators

- Rotherham Aspire understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.
- Rotherham Aspire notifies all pupils, staff and visitors of the purpose for collecting surveillance data via privacy notices and clear signage.
- Only authorised operators will have access to the system.
- Staff will not use live monitoring cameras unless there is a clear justification for doing so such as a specific safeguarding concern. In some instances certain cameras such as gate cameras or entrance cameras may be live monitored by specific staff for short periods of time to check who is entering the premises and building.
- All surveillance footage will be kept for 28 days to allow review subsequent to any reported incident.
- Operators will only review footage with a clear purpose which must be recorded.
- All reviewing of the footage must be done only in the presence of **two or more** authorised members of staff (see appendix 2). Footage must not be reviewed in an area where other unauthorised persons can observe.
- Recordings can only be reviewed with the agreement of the Head Teacher or the Deputy Head Teacher, or an Assistant Head Teacher if the Head Teacher is unavailable. This is to ensure two members of the SLT team support the review.
- Recordings where multiple students are visible other than students appearing on their own will not be shared with parents or guardians.
- Access to any footage must be logged with date, reason for access and the names of the observers.
- Any footage taken offline will be stored securely and only on school devices or systems.

Commented [3]: Be cautious with cameras where live monitoring of a 'public space' such as a public highway/pavement is possible, operators may require a license <https://www.gov.uk/public-space-surveillance-cctv-licence>

- Any footage shared with 3rd parties must be shared securely using encryption, password protection or other secure method.
- Authorised operators will keep their account credentials secure at all times and will not share their account with anyone else.
- Operators will report any technical issues quickly so any down time of the system is minimised

Access to recordings

- Under the data protection act 2018, individuals have the right to obtain confirmation that their personal information is being processed.
- All disks containing images belong to, and remain the property of, the school.
- Individuals have the right to submit a subject access request (SAR) to gain access to their personal data including recordings, this will be a viewing only.
- Rotherham Aspire will verify the identity of the person making the request before any information is viewed.
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format for viewing only and not distributed.
- Requests by persons outside the school for viewing only of recordings, will be assessed by the school, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.
- Where a request is manifestly unfounded, excessive or repetitive, it may be refused or a reasonable fee will be charged.
- All fees will be based on the administrative cost of providing the information.
- All requests will be responded to without delay and at the latest, within one month of receipt.
- 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.
- 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.
- Where a request is manifestly unfounded or excessive, Rotherham Aspire holds the right to refuse 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.
- In the event that a large quantity of information is being processed about an individual, Rotherham Aspire will ask the individual to specify the information the request is in relation to.
- 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.
- 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 solicitors and barristers

- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation
- Any third party must complete a data request form (See Appendix 5)
- 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.

Storage and retention

Footage will be stored for 28 days at the Hutton Park and Catcliffe sites and 18 days at the Rawmarsh site. 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.

Complaints

Complaints and enquiries about the operation of surveillance systems within Rotherham Aspire should be directed to the Headteacher/Management Committee 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/>

Policy monitoring and review

- This policy will be monitored and reviewed on a biannual basis by the DPO and the Compliance Manager.
- The DPO will be responsible for monitoring any changes to legislation that may affect this policy, and recommending that Rotherham Aspire make the appropriate changes accordingly.
- The school will communicate changes to this policy to all members of staff.

Appendix 1: Technical details of system – Rawmarsh

System type	Analogue DVR
Manufacturer	Corbra Elite RT 16 x2 DVRs
Owner/Operator	Rotherham Aspire Rawmarsh Site
Software	Software Version 11.1.00 (0023)
Update/patching interval	Annually
Date of installation	Over 6 years
Number of cameras	26
Type of cameras	fixed/dome
Internal/external or both	Both
Constant recording	24/7/365
Access type	direct control
Installation/maintenance contractor	P & N Alarms
Maintenance review period	Annually
Remote monitoring allowed	No
Retention period	28 days

Commented [4]: Any system owned and managed by a PFI contractor should have their own policy

Technical details of system – Hutton Park

System type	Digital NVR
Manufacturer	Hikvision ACV 11.0 software
Owner/Operator	Rotherham Aspire Hutton Park Site
Software	AC V1.11
Update/patching interval	Annually
Date of installation	2019 P & N Alarms
Number of cameras	32
Type of cameras	fixed/dome

Commented [5]: Any system owned and managed by a PFI contractor should have their own policy

Internal/external or both	Both
Constant recording	24/7/365
Access type	direct control
Installation/maintenance contractor	P & N Alarms
Maintenance review period	Annually
Remote monitoring allowed	No
Retention period	30 days
System type	Digital NVR

Technical Details - Catcliffe

System type	Analogue DVR
Manufacturer	Concept
Owner/Operator	Rotherham Aspire Catcliffe Site
Software	IPIMS Client Software
Update/patching interval	Annually
Date of installation	2017
Number of cameras	32
Type of cameras	fixed/dome
Internal/external or both	Both
Constant recording	24/7/365
Access type	direct control
Installation/maintenance contractor	Installation unknown/P & N Alarms maintenance
Maintenance review period	Annually
Remote monitoring allowed	No
Retention period	28 days

Commented [6]: Any system owned and managed by a PFI contractor should have their own policy

Appendix 2: Authorised Users

Name	Job Title
Lee Morritt	Head Teacher
Nichola Plant	Safeguarding Lead
Sally Peedle	Assistant Head Teacher
Lindsey Waugh	Assistant Head Teacher
David Thorpe	Assistant Head Teacher
Mark Hepple	Head of Centre (Hutton Park)
Matt Nichols	Head of centre (Catcliffe)
Stevie Davies	Head of Centre (Rawmarsh)
Donna Hissitt	Pa to the Head Teacher/Data Controller
Phill Guillian	Assistant Head of Centre (Catcliffe)
Antony Green	Assistant Head of Centre (Rawmarsh)
Jane Pickering	Assistant Head of Centre (Hutton Park)
Alan Murray	Site Manager
Tim Jervis	Mentor
Haley Wright	Mentor
Natalie Venters	Mentor
Caroline Booth	Safeguarding Lead
Heidi Hollingsworth	Mentor
Shelley Teale	Primary Curriculum Lead and Teacher

Appendix 3:

Location of Cameras Hutton Park

Camera location and type	Internal or external	Audio enabled or disabled	Live monitoring allowed?
Fixed camera main car park near construction.	External	Disabled	No
Fixed camera main car park central.	External	Disabled	No
Fixed camera outside main reception entrance.	External	Disabled	No
Fixed camera main drive and gate entrances.	External	Disabled	No
Fixed camera driveway down to B block.	External	Disabled	No
Fixed camera B block car park.	External	Disabled	No
Fixed camera hair & beauty back room.	Internal	Disabled	No
Fixed camera rear of construction room.	Internal	Disabled	No
Fixed camera front of construction room.	Internal	Disabled	No
Fixed camera student zone main body.	Internal	Disabled	No
Fixed camera staff kitchen.	Internal	Disabled	No
Fixed camera student zone from sport room.	Internal	Disabled	No
Fixed camera English classroom.	Internal	Disabled	No
Fixed camera car park outside B block.	External	Disabled	No
Fixed camera driveway looking up from B block.	External	Disabled	No
Fixed camera gym.	Internal	Disabled	No
Fixed camera mentors office B block.	Internal	Disabled	No
Fixed camera B block corridor outside toilets.	Internal	Disabled	No
Fixed camera B block corridor towards entrance.	Internal	Disabled	No
Fixed camera sports classroom.	Internal	Disabled	No
Fixed camera mentor/safeguarding office.	Internal	Disabled	No
Fixed camera hair & bBeauty classroom.	Internal	Disabled	No
Fixed camera art classroom.	Internal	Disabled	No

Fixed camera corridor outside art classroom.	Internal	Disabled	No
Fixed camera main reception.	Internal	Disabled	No
Fixed camera back office A block.	Internal	Disabled	No
Fixed camera office at main reception.	Internal	Disabled	No
Fixed camera maths classroom.	Internal	Disabled	No
Fixed camera catering classroom/kitchen	Internal	Disabled	No
Fixed camera science classroom.	Internal	Disabled	No
Fixed camera PSHE classroom.	Internal	Disabled	No
Fixed camera outside B block entrance.	External	Disabled	No

Location of cameras Rawmarsh

Camera location and type	Internal or External	Audio enabled or disabled	Live monitoring allowed?
Fixed camera entrance pathway x 2	External	Disabled	No
Fixed camera main reception x 2	External	Disabled	No
Fixed camera main car park x 2	External	Disabled	No
Fixed camera school hall	Internal	Disabled	No
Fixed camera classroom 1	Internal	Disabled	No
Fixed social zone 1	Internal	Disabled	No
Fixed camera classroom 2	Internal	Disabled	No
Fixed camera social zone 2 x 2	Internal	Disabled	No
Fixed camera classroom 3 x 2	Internal	Disabled	No
Fixed camera kitchen	Internal	Disabled	No
Fixed camera de-escalation corridor	Internal	Disabled	No
Fixed camera classroom 4	Internal	Disabled	No
Fixed camera social zone 3	Internal	Disabled	No
Fixed camera classroom 5	Internal	Disabled	No

Fixed camera classroom 5 exit	Internal	Disabled	No
Fixed camera classroom 6	Internal	Disabled	No
Fixed camera classroom 7	Internal	Disabled	No
Fixed camera social zone 4 (Primary)	Internal	Disabled	No
Fixed camera main rear exit corridor	Internal	Disabled	No
Fixed camera (rear) poly-tunnel facing	External	Disabled	No
Fixed camera primary playground x 2	External	Disabled	No
Fixed camera outside (rear) 6 & 7	External	Disabled	No
Fixed camera secondary playground steps	External	Disabled	No
Fixed camera secondary playground mugger	External	Disabled	No
Fixed camera outside (staff room)	External	Disabled	No

Location of Cameras at Catcliffe

Camera location and type	Internal or external	Audio enabled or disabled	Live monitoring allowed?
Fixed camera classroom 1 (Camera 4)	Internal	Disabled	No
PTZ camera in main carpark (Camera 16)	External	Disabled	No
Fixed camera classroom 2 (Camera 8)	Internal	Disabled	No
Fixed camera classroom 3 (Camera 7)	Internal	Disabled	No
Fixed camera classroom 4 (Camera 13)	Internal	Disabled	No
Fixed camera kitchen (Camera 6)	Internal	Disabled	No
Fixed camera main office (Camera 5)	Internal	Disabled	No
Fixed camera corridor (Camera 14)	Internal	Disabled	No
Fixed camera corridor (Camera 11)	Internal	Disabled	No

Fixed camera corridor internal main entrance (Camera 9)	Internal	Disabled	No
Fixed camera building entrance (Camera 1)	External	Disabled	No
Fixed camera front grass area (Camera 12)	External	Disabled	No
Fixed camera side of school (Camera 3)	External	Disabled	No
Fixed camera front fence (Camera 2)	External	Disabled	No
Fixed camera side of school fire exit (Camera 15)	External	Disabled	No
Fixed camera school car park entrance (Single Screen)	External	Disabled	No
Fixed camera student & visitor entrance (Camera 10)	External	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	