CCTV Policy

Updated May 22nd 2023

Policy reference:	A39
This policy is to be reviewed:	3 yearly
The next review date is:	May 2026
Review is the responsibility of:	Trust Board

Review History

Review ratified:	April 2018, June 2019
Review ratified:	May 2022
Review ratified:	May 2023

Authorised by: Full Trust Board

Revisions made:		
Date:	**Page no.**	**Description of changes:**
April 2018		Changes made by JH (Operations Director)
May 2018		With Trustees for approval
June 2019		Amended which staff are permitted to review CCTV, storage and retention arrangements, wording of the CCTV notices, and removed Do's and Do Not's.
May 2022	Various	Changes includes all legislative requirements and a change to process for applying to access the CCTV
May 2023	P6	Objectives added

INTRODUCTION

The purpose of this policy is to regulate the management, operation, and use of the CCTV system at Aspire Learning Trust.

Statement of Intent

At Aspire, we take our responsibility towards the safety of staff, visitors, and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our schools and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems within the Trust schools and ensure that:

a. We comply with the GDPR
b. The images that are captured are useable for the purposes we require them for
c. We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

a. Observing what an individual is doing
b. Taking action to prevent a crime
c. Using images of individuals that could affect their privacy

Objectives of the CCTV Setup

a. Maintain a safe environment for learning and the purposes of running an educational and recreational establishment
b. Ensure the welfare of pupils, staff, visitors, and customers
c. Deter criminal acts against persons and property
d. Assist the police in identifying persons who have committed an offence

Legal Framework

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

a. Human Rights Act,
b. Regulation of Investigatory Powers Act (RIPA).
c. The Regulation of Investigatory Powers Act 2000
d. The Protection of Freedoms Act 2012
e. The General Data Protection Regulation (GDPR) The Data Protection Act 1998
f. The Freedom of Information Act 2000
g. The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
h. The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
i. The School Standards and Framework Act 1998
j. The Children Act 1989
k. The Children Act 2004
l. The Equality Act 2010

Failure to comply with these Acts or the related codes would cause the Trust to be in breach of the Law, render any evidence as inadmissible or carry penalties for the Trust, as the CCTV user, or individual members of staff.

Key staff have been provided with the necessary induction in the use of the CCTV systems and only those members of staff have access to the recordings within the system:

a. Area IT Manager
b. 2nd Line IT Technician
c. The Senior Leadership Team
d. Year Leaders
e. Safeguarding and Pastoral Support Staff
f. Aspire Learning Trust CEO
g. Aspire Learning Trust Operations Director

Definitions

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

a. Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio, or live footage
b. Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.
c. Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

Aspire does not condone the use of covert surveillance when monitoring the trust's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

Roles & Responsibilities

a. The role of the Trust data protection officer (DPO, Paul Stratford, The ICT Service) includes:
    1. Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.
    2. Ensuring that all data controllers at the Trust handle and process surveillance and CCTV footage in accordance with data protection legislation.
    3. Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
    4. Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
    5. 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.
    6. Informing data subjects of how their data captured in surveillance and CCTV 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.

b. Aspire, as the corporate body, is the data controller. The Board of Trustees of Aspire therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

c. The Local Senior Management team at each school:

   a. Will ensure that by adoption of this policy they will support the Board of Trustees fulfil their legal obligations.
   b. The SLT member/s reviewing CCTV footage is responsible for deleting the footage once it is no longer required.
   c. No footage shall be kept no longer than 30 days unless there are legal obligations restricting the deletion of the footage. i.e., Police investigation.
   d. If the footage is not required for legal purposes but the SLT member has a justified reason to keep the footage longer than the 30 days, this will need to be authorised by the Trust and reviewed every 14 days until the footage is no longer required and can be deleted.
   e. All CCTV footage must be stored on a secure drive with restricted access and must not be stored locally on individual devices.

d. The trust's IT Area Manager deals with the day-to-day matters relating to data protection within the trust and thus, for the benefit of this policy, will act as the data controller.

e. The role of the data controller includes:
   1. Processing surveillance and CCTV footage legally and fairly
   2. Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly
   3. Collecting surveillance and CCTV footage that is relevant, adequate, and not excessive in relation to the reason for its collection
   4. Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary
   5. Protecting footage containing personal data against accidental, unlawful destruction, alteration, and disclosure – especially when processing over networks
   6. Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation

f. The role of the CEO/headteacher includes:
   1. Meeting with the IT Area Managers to decide where CCTV is needed to justify its means. Conferring with the DPO about the lawful processing of the surveillance and CCTV footage.
   2. Monitoring legislation to ensure the Trust is using surveillance fairly and lawfully.
   3. Communicating any changes to legislation with all members of staff.

Purpose and Justification

a. The trust will only use surveillance cameras for the safety and security of the trust and their staff, pupils, and visitors
b. Surveillance will be used as a deterrent, investigate inappropriate behaviour and damage to the trust
c. The trust will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in any changing facilities
d. If the surveillance and CCTV systems fulfil their purpose and are no longer required, the trust will deactivate them

Objectives

The surveillance system will be used to:

a. Maintain a safe environment for learning and the purposes of running an educational and recreational establishment
b. Ensure the welfare of pupils, staff, visitors and customers
c. Deter criminal acts against persons and property
d. Assist the police in identifying persons who have committed an offence

Protocols

a. The surveillance systems will be registered with the ICO in line with data protection legislation
b. The surveillance systems are a closed digital system
c. Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.
d. The surveillance system has been designed for maximum effectiveness and efficiency; however, the trust cannot guarantee that every incident will be detected or covered and 'blind spots' may exist
e. The surveillance systems will not be focused on individuals unless an immediate response to an incident is required
f. The surveillance system will not be focused on property outside the perimeter of the school's

Security

a. Access to the surveillance system, software and data will be strictly limited to authorised operators
b. The Trusts authorised CCTV system operators are cited as above
c. The Trust staff authorised to record and retain images are cited above
d. The main control facility is kept secure within locked equipment racks or locked rooms
e. If, in exceptional circumstances, covert surveillance is planned, this must have written permission from the Chief Executive Officer and the Data Protection Officer
f. Surveillance and CCTV systems will be tested for security flaws regularly to ensure that they are being properly always maintained
g. Surveillance and CCTV systems will not be intrusive by design
h. Any unnecessary footage captured will be securely deleted from the Trust's system as specified in this policy

Privacy by design

a. The use of surveillance cameras and CCTV will be critically analysed using a PIA – under the GDPR this will become a DPIA, but it will follow the same principles of a PIA
b. A PIA will be carried out prior to the installation of any surveillance and CCTV system
c. If the PIA reveals any potential security risks or other data protection issues, the Trust will ensure they have provisions in place to overcome these issues
d. Where the Trust identifies a high risk to an individual's interests, and it cannot be overcome, the trust will consult the ICO before they use CCTV, and the trust will act on the ICO's advice

e. The trust will ensure that the installation of the surveillance and CCTV systems will always justify its means
f. If the use of a surveillance and CCTV system is too privacy intrusive, the trust will seek alternative provision

Code of Practice

a. The trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles
b. The trust notifies all pupils, staff, and visitors of the purpose for collecting surveillance data via notice boards, letters, and signage
c. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose
d. All surveillance footage will be kept for a maximum of three months for security purposes; the trust and IT Area Manager are responsible for keeping the records secure and allowing access
e. The trust 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
f. The surveillance and CCTV system is owned by the Trust and images from the system are strictly controlled and monitored by authorised personnel only
g. The Trust will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils, and visitors to the trust, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the Trusts website
h. The surveillance and CCTV system will:
    1. Be designed to consider its effect on individuals and their privacy and personal data
    2. Be transparent and include a contact point, the DPO, through which people can access information and submit complaints
    3. Have clear responsibility and accountability procedures for images and information collected, held, and used
    4. Have defined policies and procedures in place which are communicated throughout the trust
    5. Only keep images and information for as long as required
i. Restrict access to retained images and information with clear rules on who can gain access
j. Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law
k. Be subject to stringent security measures to safeguard against unauthorised access
l. Be regularly reviewed and audited to ensure that policies and standards are maintained
m. 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
n. Be accurate and well maintained to ensure information is up to date

Access

a. Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed
b. All disks containing images belong to, and remain the property of, the Trust
c. Individuals have the right to submit an SAR to gain access to their personal data to verify the lawfulness of the processing
d. The Trust will verify the identity of the person making the request before any information is supplied
e. 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
f. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format
g. Requests by persons outside the Trust for viewing or copying disks, or obtaining digital recordings, will be assessed by the trust, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation
h. Where a request is manifestly unfounded, excessive, or repetitive, a reasonable fee will be charged
i. All fees will be based on the administrative cost of providing the information
j. All requests will be responded to following the GDPR policy
k. In the event of numerous or complex requests, the period of compliance will 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
l. 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
m. If 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
n. 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
o. Instances of access to recordings will be recorded in a log which can be produced on demand to the DPO, an authorised manager or Auditor/ Regulator and will be a complete record of access activity (Appendix B).
   This log should state:
   1. dates of access
   2. the period and location covered by the recording, the reason for access and
   3. name, position, and authority of those who have accessed recordings whether copies were made
p. 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:

1. The police – where the images recorded would assist in a specific criminal inquiry
2. Prosecution agencies – such as the Crown Prosecution Service (CPS) Relevant legal representatives – such as lawyers and barristers, where a court order requires it
3. 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

q. 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.

Code of Practice

a. This CCTV Policy will be reviewed every 3 years.
b. The CCTV system is owned and operated by the Trust.
c. The footage may only be viewed by authorised members of staff as listed above.
d. Images required as evidence will be removed from the DVR and stored in a secure location.

Breaches of the code

a. Any breach of the Code of Practice by the school will be initially investigated by the CEO, for them to take the appropriate disciplinary action.
b. Any serious breach of the Code of Practice will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach.

Appendix A

CCTV IN OPERATION

24 hour recording in operation across this Site.

Images are recorded for security, safety, and child protection.

This scheme is operated by Aspire Learning Trust.

For further information, contact - 01733 703991

Appendix B – Example of table

Form Response									
ID	Start time	Completion time	Email	Name	Name of Requester	Date of Incident	Area of the School to review	Comments	Reason for the request - Outline the incident