Author	Lisa Yates	Target group	All employees, consultants and volunteers
Issued	May 2025		
Approved by	Executive Team	Next review	May 2027

CCTV Policy

Aims

This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

Statement of intent

The purpose of the CCTV system is to:

- make members of the school community feel safe
- protect members of the school community from harm to themselves or to their property
- deter misbehaviour and criminality in the school
- protect school assets and buildings
- assist police to deter and detect crime
- determine the cause of accidents
- assist in the effective resolution of any disputes which may arise in the course of complaints, disciplinary and grievance proceedings
- assist in the defence of any litigation proceedings

The CCTV system will not be used to:

- encroach on an individual's right to privacy
- monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- follow particular individuals, unless there is an ongoing emergency incident occurring
- pursue any other purposes than the ones stated above

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime. The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

Relevant legislation and guidance

This policy is based on:

Legislation

UK General Data Protection Regulation

Data Protection Act 2018

Human Rights Act 1998

European Convention on Human Rights

The Regulation of Investigatory Powers Act 2000

The Protection of Freedoms Act 2012

The Freedom of Information Act 2000

The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

The School Standards and Framework Act 1998

The Children Act 1989

The Children Act 2004

The Equality Act 2010

Guidance

Surveillance Camera Code of Practice (2021)

ICO guidance for the use of CCTV

Definitions

Surveillance: the act of watching a person or a place
CCTV: closed circuit television; video cameras used for surveillance
Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.

Location of the cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in the above Statement of intent).
Cameras are located in:

The front of the school, front door and rear playground.

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance. The signage:

- Identifies the school as the operator of the CCTV system
- Identifies the school as the data controller
- Provides contact details for the school

Cameras are not and will not be aimed off school grounds into public spaces or people's private property. Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

Roles and responsibilities

The Headteacher

The Headteacher will:

- take responsibility for the overall leadership and management of the CCTV system (day-to-day management may be delegated to a Designated System Manager)
- liaise with the school Data Protection Lead to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- ensure that the guidance set out in this policy is followed by all staff
- ensure all persons with authorisation to access the CCTV system and footage have received proper training in the use of the system and in data protection
- sign off on any expansion or upgrading to the CCTV system, after having taken advice from the Anthem Head of IT, Head of Estates and Procurement Manager and taken into account the result of a data protection impact assessment
- decide, in consultation with the School Data Protection Lead, whether to comply with disclosure of footage requests from third parties.

The school Data Protection Lead

The school Data Protection Lead will:

- ensure all staff recognise a subject access request
- deal with subject access requests in line with the UK GDPR and Data Protection Act 2018
- monitor compliance with UK data protection law
- conduct data protection impact assessments
- ensure data is handled in accordance with data protection legislation

- ensure footage is obtained in a legal, fair and transparent manner
- ensure footage is destroyed when it falls out of the retention period
- keep accurate records of all data processing activities and make the records public on request
- inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information
- carry out termly checks to determine whether footage is being stored securely and being deleted after the retention period
- receive and consider requests for third-party access to CCTV footage
- responds to enquiries received by the school about the CCTV system.

The Designated System Manager

The Designated System Manager is: [insert name(s)]

The Designated System Manager will:

- ensure persons with authorisation to access the CCTV system and footage receive support and appropriate training in the use of the system and in data protection
- ensure that the CCTV systems are working properly and that the footage they produce is of sufficiently high quality so that individuals pictured in the footage can be identified
- ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- take care of the day-to-day maintenance and operation of the CCTV system
- oversee the security of the CCTV system and footage
- check the system for faults and security flaws termly
- ensure the data and time stamps are accurate, through adjustment when clocks change and termly checks.

The IT Support Team / CCTV Contractor

The IT Support Team / CCTV Contractor will:

- ensure security measures are in place to protect the footage
- apply any security updates published by the equipment's manufacturer.

Operation of the CCTV system

- The CCTV system will be operational 24 hours a day, 365 days a year.
- The system is registered with the Information Commissioner's Office.
- The system will not record audio.
- Recordings will have date and time stamps.

Storage of CCTV footage

Footage will be retained for 30 days where systems allow. At the end of the retention period, the files will be overwritten automatically.

Where a law enforcement body is investigating a crime, the school is investigating an incident such as those leading to a suspension or PEX, accident, complaint or claim, the footage will be retained for a minimum period of 3 months or as long as necessary to give the opportunity to view the images as part of an active investigation.

Recordings will be downloaded and encrypted, so that the data will be secure and its integrity maintained, and to be used as evidence if required. The recording will be saved onto a designated SharePoint folder only accessible to the school authorised users.

The school DP Lead will carry out termly checks to determine whether footage is being stored securely, accurately, and being deleted after the retention period.

Access to CCTV footage

Access will only be given to authorised persons for the purpose of pursuing the aims stated above or if there is a lawful reason to access the footage.

Access by authorised staff members
The following members of staff have authorisation to access live and recorded CCTV footage:

- The Headteacher
- The Deputy Headteacher or a nominated member of the SLT, Hannah Golding.
- The school Data Protection Lead
- The Designated System Manager
- The IT Support Team / CCTV Contractor

CCTV footage will only be accessed by authorised members of staff from authorised personnel's work devices, or from the visual display monitors.

Authorised members of staff will have their own unique username and password to access the CCTV system. They must not share these details with anybody else.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the CCTV Access Log (see Appendix 1). Records of all access must be kept for period of one year.

Any visual display monitors used to monitor CCTV will be positioned so only authorised personnel will be able to see the footage.
All members of staff who have access will undergo training to ensure proper handling of the system and footage. Any member of staff who misuses the surveillance system may be committing a criminal offence and could face disciplinary action.

The above personnel will consult with the school Data Protection Lead prior to disclosing any CCTV footage with non-school staff members.

Requests to access CCTV footage

Requests made by staff members who are not authorised CCTV Users

Requests made to authorised users by other staff members must be recorded in the CCTV Access Log (Appendix 1). There must be clear rationale for the request that meets the intended use of the system (see Stated Intent) and all requests must be reviewed and approved by the Headteacher before footage is viewed.

If the request is approved by the Headteacher, the Authorised CCTV User will:

- retrieve and view the CCTV footage
- save the relevant portion of footage in the designated secure folder – please refer to the section above 'Storage of CCTV footage'
- record all details on the CCTV Access Log (Appendix 1)

It will not always be necessary to allow the member of staff who has made the CCTV access request to view footage, but it may be appropriate in cases where clarification or identification of persons is necessary or when a formal investigation is being carried out. When it is deemed necessary for that member of staff to view the footage, then this should be done under the supervision of the Authorised User. Only the relevant portion should be viewed, and details of this access must be recorded in the CCTV Access Log (Appendix 1). No copies of the footage must be made.

For additional support, the Anthem IT Team can be contacted; however, not all Anthem schools' CCTV systems are known to the Anthem IT Team. Requests for support should be raised via the IT Service Desk: IT@anthemtrust.uk

Subject Access Requests (SARs)

According to UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Requests should be directed to the school Data Protection Lead. Contact details for the school Data Protection Lead and information on how the school will handle these requests can be found on the Data Protection Policy, available on the Anthem and school website.

A SAR can be made verbally or in writing, including by social media. When making a request, individuals should provide the school with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage.

On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals need to be obscured to prevent unwarranted identification before sharing them. The school will liaise with the Anthem IT Team about the redaction of any CCTV footage, when support is needed. If this is not possible to blur out faces or

redact parts of the footage, the school may seek third party consent before releasing the footage or the still images may be released instead.

Schools are encouraged to invite individuals to watch the CCTV footage in the school premises and not to share it via email. Footage that is disclosed in a SAR will be shared securely to ensure only the intended recipient has access to it.

The school Data Protection Lead will add the details of the SAR onto the school Data Protection log.

Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out above (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).
All requests for access should be directed to the school Data Protection Lead.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access. The Headteacher in consultation with the school DP Lead will consider very carefully how much footage to disclose and seek legal advice if necessary.

The school DP Lead will ensure that any disclosures that are made are done in compliance with UK GDPR and Data Protection Act 2018 and recorded on the Data Protection log.

Data protection impact assessment (DPIA)

The school follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading. The system is used only for the purpose of fulfilling its aims.

When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate. The DPIA will be carried out by the school DP Lead and approved by the Anthem Data Protection Officer or Deputy Data Protection Officer.

If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

Monitoring

The policy will be reviewed every two years by the Anthem National Team.

Links to other policies

- Data Protection policy
- Privacy notices
- Child Protection & Safeguarding policy