Policy Document for: CCTV
Approved:
Due for Review: September 2025

Additions/amendments in this version

	Updated to changes references to include HT and changing to BA MAT policy
	All schools added to the policy – all contacts for the schools updated

Introduction

Bourne Alliance MAT schools use closed circuit television (CCTV) and the images produced to prevent or detect crime and to monitor the school buildings and grounds in order to provide a safe and secure environment for its pupils, staff and visitors, and to prevent loss or damage to school property and surrounds. This policy outlines the school's use of CCTV and how it complies with the General Data Protection Regulation; it is to be read in conjunction to the Trust data protection policy.

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 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 disciplinary and grievance proceedings
- To 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 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.

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.

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

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 Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- 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)

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

How the CCTV is used

- CCTV System at each school:
  - The system comprises a number of fixed and dome cameras.
  - The system does not have sound recording capability.
  - The system is not linked to staff or pupil attendance records.
  - The system is not linked to automated facial recognition or number plate recognition software thus all individuals' images are anonymous until viewed.
- The CCTV system is owned and operated by the school, the deployment of which is determined by the school's leadership team / Site Manager.
- The CCTV is monitored securely from the Admin office (Bobbing/Iwade), Estates Manager office (Grove Park/Aspire)
- The school server stores the images and is retained on-site. Access to the images are controlled by the Site Manager.
- The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and members of the school community.

- The school's CCTV Scheme is included in the School's registration with the Information Commissioner as a data processor.
- All authorised operators and employees with access to images are aware of these procedures that need to be followed when accessing the recorded images. Through this policy, all operators are made aware of their responsibilities in following the CCTV Code of Practice. The school's 'Data Controller' (Chief Executive Officer) will ensure that all employees are aware of the restrictions in relation to access to and disclosure of, recorded images by publication of this policy.
- The school complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure that CCTV is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
- The School's CCTV surveillance cameras are a passive technology that only records and retains images. They are not linked to automated decision making or facial or number plate recognition software. Transmission is by cable direct to the server.
- CCTV warning signs are clearly and prominently placed at the main external entrance to the school, including further signage in other outdoor areas in close proximity to camera positions. Signs will contain details of the purpose for using CCTV. In areas where CCTV is used, the school ensures prominent signs are placed within the controlled area.
- The recordings are filed with accurate metadata noting the camera location and time of the recording.
- The original planning, design and installation of CCTV equipment endeavored to ensure that the scheme will deliver maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Siting the cameras

- Cameras are sited so that they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated.
- 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.
- CCTV will not be used in classrooms or any internal school areas.
- Members of staff will have access to details of where CCTV cameras are situated.

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

Covert Monitoring

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, the proper authorisation forms from the Home Office will be completed and retained.

Roles and responsibilities

The Operations Committee

The Trust Board, via the Operations Committee, has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation is complied with.

The Headteacher/Head of School

The Headteacher/Head of School will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the Data Protection Offier (DPO), 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
- Review the CCTV policy to check that the school is compliant with legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO 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 DPO and taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

The data protection officer

The data protection officer (DPO) will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Train all staff to recognise a subject access request
- Deal with subject access requests in line with the Freedom of Information Act (2000)
- Monitor compliance with UK data protection law
- Advise on and assist the school with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office
- 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
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- Receive and consider requests for third-party access to CCTV footage

Site Team/IT Technician

Between them, these staff will

- 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 termly
- Ensure footage is stored accurately and being deleted after retention period termly

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. This will be checked by the IT Technician termly and when the clocks change.

Storage and Retention of CCTV images

- Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded. This retention process is in line with the Trust retention policy.
- All retained data will be stored securely at all times and permanently deleted as appropriate / required.
- Recorded images will be kept for no longer than 30 days, except where there is lawful reason for doing so, such as discipline investigations. Images are recorded over on the inserted disc.
- On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them 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, so that it can be used as evidence if required.
- The DPO will carry out termly checks to determine whether footage is being stored accurately and being deleted after the retention period.

Access to CCTV images

- Access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available.
- Access to stored images will only be granted in the case of an incident. To be viewed in the course of the incident's investigation.
- Access will only be given to authorised persons, for the purpose of pursuing the aims stated in or if there is a lawful reason to access the footage.
- Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log.
- Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

Staff access

The following members of staff have authorisation to access the CCTV footage

Bobbing

- The Head of School – Tim Harwood
- The DPO – Nicola Usher
- The Site Manager – Pat Daly
- The Estates Manager – Keith Rowbottom
- The Office Manager – Jacky Presnell
- Anyone else with express permission from the Trust CEO – Diane Browning

Iwade

- The Head of School – Katrine Stewart
- The DPO – Nicola Usher
- The Site Manager – Pat Daly
- The Estates Manager – Keith Rowbottom
- The Office Manager – Emma Edwards
- Anyone else with express permission from the Trust CEO – Diane Browning

Grove Park

- The Head of School – Lauren Flain
- The DPO – Nicola Usher
- The Site Manager – Pat Daly
- The Estates Manager – Keith Rowbottom
- The Office Manager – Sam Thorne
- Anyone else with express permission from the Trust CEO – Diane Browning

Aspire

- The Headteacher – Neil Dipple
- The DPO – Nicola Usher
- The Site Manager – Pat Daly
- The Estates Manager – Keith Rowbottom
- The Office Manager – Emma Magson
- Anyone else with express permission from the Trust CEO – Diane Browning

- CCTV footage will only be accessed from authorised work devices, or from the visual display monitors.
- 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 will face disciplinary action.

Subject Access Requests (SAR)

- According to UK GDPR and DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves.
- Upon receiving the request the school will immediately issue a receipt and will then respond within 30 days during term time. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.
- All staff have received training to recognise SARs. When a SAR is received staff should inform the DPO in an email so the DPO can make contact regarding the SAR, and/or provide the DPO email address DPO@BA-MAT.org.uk
- 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. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.
- The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded or excessive.
- Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.
- Disclosure of information from surveillance systems must be controlled and consistent with the purpose(s) for which the system was established. When disclosing surveillance images of individuals, particularly when responding to subject access requests, the school will consider whether the identifying features of any of the other individuals in the image need to be obscured. In most cases the privacy intrusion to third party individuals will be minimal and obscuring images will not be required. However, consideration will be given to the nature and context of the footage.
- The subject will be supplied with a copy of the information in a permanent form. There are limited circumstances where this obligation does not apply. The first is where the data subject agrees to receive their information in another way, such as by viewing the footage. The second is where the supply of a copy in a permanent form is not possible or would involve disproportionate effort, whereby the disproportionate effort may incur an administration fee.

Access to and Disclosure of Images to Third Parties

- CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in this policy (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). This is upon receipt of the standard Police form requesting images.
- All requests for access should be set out in writing and sent to the headteacher and the DPO.
- 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 DPO will consider very carefully how much footage to disclose, and seek legal advice if necessary.
- The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.
- All disclosures will be recorded by the DPO.
- The data may be used within the school's discipline and grievance procedures as required and will be

subject to the usual confidentiality requirements of those procedures. Data transfer will be made securely and using encryption as appropriate.

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 the 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 DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the Estates Manager – Keith Rowbottom.
- Those whose privacy is most likely to be affected, including the school community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.
- A new DPIA will be done annually, or whenever cameras are moved and/or new cameras are installed. If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

Security

- The Site Manager/Estates Manager will be responsible for overseeing the security of the CCTV system and footage
- The system will be checked for faults once a term
- Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure
- Footage will be stored securely and encrypted wherever possible
- The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use
- Proper cyber security measures will be put in place to protect the footage from cyber attacks
- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

Complaints

Complaints should be directed to the Headteacher/Head of School and should be made according to the school's complaints policy.

Monitoring

The policy will be reviewed annually by the DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.