"Everyone can achieve, everyone can learn, everyone belongs"

Surveillance and CCTV Policy

Date adopted: May 2023
Review Period: 3 years
Next Review: May 2029

History of most recent policy reviews:

Date	Review	Who is Responsible?
May 2026	Updated in line with current guidance and new recommendations from Protection Officer (Judicium)	Finance Committee

Contents:

1. Legal framework
2. Definitions
3. Roles and responsibilities
4. Purpose and justification
5. Data Protection
6. Protocols
7. Security
8. Code of practice
9. Access
10. Monitoring and review

Statement of intent

At Air Balloon Hill Primary School, 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 school and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with the UK GDPR.
- The images that are captured are useable for the purposes we require them for.
- 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:

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

The surveillance system will be used to:

- Maintain a safe environment.
- To protect the personal safety and welfare of pupils, staff, volunteers, visitors and members of the public.
- To prevent bullying
- To increase a sense of personal safety and reduce the fear of crime by deterring criminal acts against persons and property, including to reduce the incidence of crime and anti-social behaviour (including theft and vandalism)
- Assist the police in identifying persons who have committed an offence. To protect the school buildings and assets both during and after school hours
- To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders
- To assist in managing the school and ensure that the school rules are respected.

The purpose of this policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at the school. CCTV cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities, etc

The CCTV system used by the school comprises of:

Camera Type	Location	Sound	Recording Capacity	Swivel/Fixed
CCTV Camera	Main Gate	N	Y	F
CCTV Camera	Front Yard and Gate Area	N	Y	F
CCTV Camera	Sensory Garden	N	Y	F
CCTV Camera	Main Entrance Doors	N	Y	F
CCTV Camera	Boardwalk area towards Year 6 Building	N	Y	F
CCTV Camera	Main reception area	N	Y	F
CCTV Camera	Middle Playground	N	Y	F
CCTV Camera	Space Cadets Entrance	N	Y	F
CCTV Camera	Front Playground	N	Y	F
CCTV Camera	Front Playground Climbing Frame	N	Y	F
CCTV Camera	Sombrero Hall	N	Y	F
CCTV Camera	Stratos Hall	N	Y	F
CCTV Camera	Messier Hall	N	Y	F
CCTV Camera	Year 6 Terrace Area	N	Y	F
CCTV Camera	Rear Gate near Climbing Frame	N	Y	F
CCTV Camera	Reception Garden	N	Y	F
CCTV Camera	Side Entrance to New Building (Sky Class)	N	Y	F
CCTV Camera	Side Entrance near Mars Class	N	Y	F
CCTV Camera	Sensory Room	N	Y	F
CCTV Camera	Staff Car Park Gates	N	Y	F
CCTV Camera	Staff Car Park	N	Y	F
CCTV Camera	Reception Area (outside Classrooms)	N	Y	F
CCTV Camera	Ballcourt	N	Y	F

CCTV cameras are installed in such a way that they are not hidden from view. We do not covertly record anyone. Signs are predominantly displayed where relevant so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV .

The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice.

The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design have endeavoured to ensure that the system will give 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.

Warning signs, as required by the Code of Practice of the Information Commissioner, will be clearly visible on the site.

1. Legal framework

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

- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- The UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- 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
- School Standards and Framework Act 1998
- Children Act 1989
- Children Act 2004
- Equality Act 2010

This policy operates in conjunction with the following statutory and non-statutory guidance:

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2022) 'Video Surveillance'

This policy operates in conjunction with the following school policies:

- Online Safety and Social Media Policy
- Freedom of Information Policy
- Data Protection Policy (including the use of photographs and video images)

2. Definitions

For the purpose of this policy the following definitions are given for the below terms:

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage e.g. real-time recordings and live streams. For the purpose of this policy only video and audio footage will be applicable.
- **Overt surveillance** – Surveillance which is clearly visible and signposted around the school and does not fall under the Regulation of Investigatory Powers Act 2000.
- **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.

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

3. Roles and responsibilities

The role of the Headteacher includes:

- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.
- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Determine which members of staff will be given access to the CCTV footage and ensuring that they act as appropriate data controllers for that data.

The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual 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 School Business Manager includes:

- Dealing with freedom of information requests and subject access requests (SARs) in line with legislation, including the Freedom of Information Act 2000.
- 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.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Preparing reports and management information on the school's level of risk related to data protection and processing performance.
- Monitoring the performance of the school's Data Protection Impact Assessment (DPIA) and providing advice where requested.

The school, as the corporate body, is the data controller. The governing board therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

4. Purpose and justification

The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors.

Surveillance will be used as a deterrent for violent behaviour and damage to the school.

The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility.

5. Data protection

Data collected from surveillance and CCTV will be:

- Processed lawfully, as determined by a DPIA. In less common circumstances, lawful processing will be determined by a legitimate interests assessment (LIA).
- Processed fairly, in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people.
- Processed in a transparent manner, meaning that people are informed when their data is being captured.
- Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:
    - Further processing for archiving data in the public interest
    - Scientific or historical research
    - Statistical 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 is inaccurate, having regard to the purposes for which they are processed, is 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 is processed.
- 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.

The use of surveillance cameras and CCTV, will be critically analysed using a DPIA, in consultation with the DPO.

A DPIA will:

- Describe the nature, scope, context, and purposes of the processing.
- Assess necessity, proportionality, and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues.

Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before they use CCTV, and the school will act on the ICO's advice.

The school will ensure that the installation of the surveillance and CCTV systems will always justify its means. If the use of a surveillance and CCTV system is too privacy intrusive, the school will seek amendments.

Surveillance and CCTV systems will not be intrusive. Pupils, staff and visitors will be made aware of the following:

- Whenever they are being monitored by a surveillance camera system
- Who is undertaking the activity
- The purpose for which the associated information is being used

The use of any video conferencing technology will be fair and transparent. Any pupils and staff who are part of any video conference calls will be informed of its purpose, and recording and publication of any video to an indefinite audience will be consented to and will not be used outside of the intended purpose.

6. Protocols

The school is registered with the Information Commissioner's Office (ICO) under the terms of the Data Protection Act 2018 and the General Data Protection Regulations (GDPR). The school complies with the ICO's CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its use. A copy of the Code of Practice can be found on the ICO's website: https://ico.org.uk/media/1542/cctv-code-of-practice.pdf.

The surveillance system is a closed digital system.

Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice. Warning signs will be more prominent in areas where surveillance is less expected to be in operation, and when using systems that can capture a large amount of personal data at one time.

The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

Locations of the surveillance system have been selected, both inside and outside, that the school reasonably believes require monitoring to address the objectives stated.

The school will make every effort to position the camera so that their coverage is restricted to the school premises, which includes indoor and outdoor areas. CCTV will not routinely be used in classrooms.

The surveillance system will not be used to focus on a particular group or individual unless an immediate response to an incident is required.

The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

7. Security

Access to the surveillance system, software and data will be strictly limited to authorised operators, and will be password protected, and where appropriate, will be encrypted.

In exceptional cases where large amounts of information need to be collected and retained, the school will consider using cloud storage. This will be secure and only accessible to authorised individuals.

The school's authorised CCTV system operators are:

- Mr T Browse - Headteacher.
- Mr A Lea – Site Manager
- Mrs S King – School Business Manager
- Miss J Liley – Deputy Headteacher
- Mrs J Knight – Assistant Headteacher (Pastoral and Safeguarding)
- Mrs L Hennessy – Assistant Headteacher (Inclusion)

The Headteacher may grant other appropriate members of staff access to the CCTV footage, in the presence of one or more of the above members of staff in order for them to support the identification of individuals in the footage. Where a person other than those mentioned above requests access to the CCTV data or system, the Headteacher must satisfy himself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists, access will be refused.

The main control facility is kept secure and locked when not in use.

If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

Surveillance and CCTV systems will be tested for security flaws once a month to ensure that they are being properly maintained at all times.

The Headteacher will decide when to record footage, e.g. a continuous loop outside the school grounds to deter intruders.

Staff will be trained in security procedures, and sanctions will be put in place for those who misuse security system information. Staff will be made aware that they could be committing a criminal offence if they do this.

The ability to produce copies of information will be limited to the appropriate staff.

Any unnecessary footage captured will be securely deleted from the school system.

Each system will have a separate audio and visual system that can be run independently of one another. The school will not record audio unless it has:

- Identified a particular need or issue and can evidence that this need must be addressed by audio recording;
- Considered other less privacy intrusive methods of achieving this need;
- Reviewed the other less privacy intrusive methods and concluded that these will not appropriately address the identified issue and the only way to do so is via the use of audio recording.

Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

8. Code of practice

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 23 days.

Recorded images will only be retained long enough for any incident to come to light (e.g., for a theft to be noticed) and the incident to be investigated. In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 6 months.

The school 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.

The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the school's website.

The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point which enables people to request information and submit complaints via the School Business Manager
- Have clear responsibility and accountability procedures for images and information collected, held and used.

- Have defined policies and procedures in place which are communicated throughout the school.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- 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.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- 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.
- Be accurate and well maintained to ensure information is up-to-date.

9. Access

Under the UK GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

All disks and hard drives 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 in order to verify the lawfulness of the processing (please refer to the school's Data Protection Policy and Privacy Notice which is available to view or download from our website: www.abhps.com/policies).

All requests should be made in writing to the School Business Manager. To email your request, please email airballoonhillp@bristol-schools.uk and mark your message FAO School Business Manager.

To request access to images held on the CCTV system, the school will require specific details (including the date, approximate time and cameral location) before it can properly respond to any requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.

The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

Individuals have the right to have personal data erased if:

- The data is no longer necessary for the original purpose it was collected for.
- They are relying on legitimate interests as a basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue the processing.
- The data has been processed unlawfully.
- There is a specific legal obligation.

There are certain exceptions where the right to erasure cannot be exercised, these include, but are not limited to:

- Where the processing is needed for the performance of a task in the public interest or an official authority.
- Certain research activities.
- Compliance with a specific legal obligation.

As an alternative to the right of erasure, individuals can limit the way their data is used if they have issues with the content of the data held by the school or they object to way it was processed.

Data can be restricted by either:

- Moving the data to another processing system.
- Making the data unavailable to users.
- Temporarily removing published data from a website.

The school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information. The individual will not be provided with a copy of the data but will allow the applicant to view the CCTV footage if available.

Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher, who will consult the School Business Manager (or Judicium, the school's Data Protection Officer), on a case-by-case basis with close regard to data protection and freedom of information legislation.

If an order is granted by a Court for disclosure of CCTV images, then this would be complied with. However, very careful consideration must be given to exactly what the Court Order requires. If there are any concerns about the disclosure, the school's Data Protection Officer will be contacted in the first instance.

Where images or footage is disclosed to third parties, including the police, a log will be kept, including the details of the person viewing the images, time of access, reason for viewing the images, details of the images viewed and a crime incident number (if applicable).

Where images are provided to a third party, wherever practicable, steps will be taken to obscure images of non-relevant individuals.

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.

Where data requests contain the personal data of a separate individual, the rights and freedoms of others will be protected by asking for their consent, or removing specific footage where appropriate.

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 lawyers and barristers
- To the school's insurance company where required, in order to pursue a claim for damage done to the property insured
- 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

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.

10. Monitoring and review

This policy will be monitored and reviewed on a biennial basis by the School Business Manager and the Headteacher.

The Headteacher will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

The Headteacher will communicate changes to this policy to all members of staff.

The scheduled review date for this policy is May 2028