Beechwood Park School

CCTV POLICY

Website: www.beechwoodpark.com

Policy Number:	Version 1.0
Policy Applicable To:	Whole School – including EYFS
Policy Revised By:	ARI
Last Review Date:	April 2022
SLT Reviewed Date:	April 2022
Governors Reviewed Date:	n/a
Next Review Date:	August 2025

OVERVIEW:

The purpose of this policy is to regulate the management and operation of the Closed Circuit Television (CCTV) and Automatic Number Plate Recognition (ANPR) systems at Beechwood Park (the School). It also serves as a notice and a guide to data subjects (including pupils, parents, staff, volunteers, visitors to the School and members of the public) regarding their rights in relation to personal data recorded via the CCTV and ANPR systems (the System).

The System is administered and managed by the School, who act as the Data Controller. This policy is subject to review, and should be read with reference to the School's Privacy Notice.

All fixed cameras are in plain sight on the School premises and the School does not routinely use CCTV for covert monitoring or monitoring of private property outside the School grounds.

The School's purposes of using the System are set out below and, having fully considered the privacy rights of individuals, the School believes these purposes are all in its legitimate interests.

Data captured for the purposes below will not be used for any commercial purpose.

Objectives of the System

- To protect pupils, staff, volunteers, visitors and members of the public with regard to their personal safety.
- To protect the School buildings and equipment, and the personal property of pupils, staff, volunteers, visitors and members of the public.
- To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders.
- To monitor the security and integrity of the School site and deliveries and arrivals, including car parking and number plate recognition.
- To monitor staff and contractors when carrying out work duties.

Positioning

- The School has selected locations in and out of School in order to achieve its security objectives.
- The School has placed adequate signage in prominent positions to inform staff and pupils that they are entering monitored areas, identifying the School as the Data Controller and giving contact details for further information regarding the System.
- No images will be captured from areas in which individuals would have a heightened expectation of privacy, including boarding, changing and washroom facilities.
- No images of public spaces will be captured except to a limited extent at site entrances.

Maintenance

- The System will be operational 24 hours a day, every day of the year.
- The System Manager (defined below) will check and confirm that the System properly records and that cameras are functioning correctly, on a regular basis.
- The System Manager will check and (to the extent necessary) service the system no less than annually.

Supervision of the System

- Staff authorised by the School to conduct routine supervision of the System may include IT and maintenance staff, day or night security and relevant staff on duty.

- The School will view and/or monitor images in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

Storage of Data

- The day-to-day management of images will be the responsibility of the Bursar who will act as the System Manager, or such suitable person as the System Manager shall appoint in his or her absence.
- The School will store images will be stored for a maximum of 4 weeks, and automatically over-write them unless the School considers it reasonably necessary for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party such as the police or local authority.
- Where such data is retained, it will be retained in accordance with the Act and the School's Data Protection Policy. Information including the date, time and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the System log book.

Access to Images

- The School will only provide access to stored images to authorised persons, under the supervision of the System Manager, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).
- Individuals also have the right to access personal data the School holds on them (please see the School's Privacy Notice), including information held on the System, if it has been kept. The School will require specific details including at least time, date and camera location before it can properly respond to any such requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.
- The System Manager will verify the identity of any person wishing to view stored images or access the System and the legitimacy of the request. The following are examples when the System Manager may authorise access to System images:
    - Where required to do so by the Head, the Police or some relevant statutory authority;
    - To make a report regarding suspected criminal behaviour;
    - To enable the Designated Safeguarding Lead or his/her appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern;
    - To assist the School in establishing facts in cases of unacceptable pupil behaviour, in which case, the parents/guardian will be informed as part of the School's management of a particular incident;
    - To data subjects (or their legal representatives) pursuant to an access request under the Act and on the basis set out above;
    - To the School's insurance company where required in order to pursue a claim for damage done to insured property; or
    - In any other circumstances required under law or regulation.
- Where images are disclosed as described above a record will be made in the System log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).
- Where images are provided to third parties as described above, wherever practicable steps will be taken to obscure images of non-relevant individuals.

Other CCTV systems

- The School does not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this is in line with the objectives of the School's own CCTV policy.

- Pupils travel to School on coaches provided by third party contractors and a number of these coaches are equipped with CCTV systems. The School may use these in establishing facts in cases of unacceptable pupil behaviour, in which case the parents/guardian will be informed as part of the School's management of a particular incident.

Complaints and queries

- Any complaints or queries in relation to the School's CCTV system, or its use of CCTV, or requests for copies, should be referred to the Bursar.
- For any other queries concerning the use of your personal data by the School, please see the School's applicable Privacy Notice.

CCTV/ANPR FOOTAGE ACCESS REQUEST FORM

The following information is required before the school can provide copies of or access to CCTV/ANPR footage from which a person believes they may be identified.

Please note that CCTV footage may contain the information of others that needs to be protected, and that the school typically deletes CCTV/ANPR recordings after a 4 week period.

Name and address: (proof of ID may be required)	
Description of footage (including a description of yourself, clothing, activity etc.)	
Location of camera	
Date of footage sought	
Approximate time (give a range if necessary)	

Signature*.....

Print Name..... Date .....

* N.B. if requesting CCTV footage of a child under 13, a person with parental responsibility should sign this form. For children 13 or over, the child's authority or consent must be obtained except in circumstances where that would clearly be inappropriate and the lawful reasons to provide to the parent(s) outweigh the privacy considerations of the child.