



CCTV Policy

Policy number	BS017
Applies to	Whole School
Endorsed by	Vice Master
Responsibility	Vice Master
Date reviewed	March 2021
Next review	March 2022

The purpose of this policy is to regulate the management and operation of the Closed Circuit Television (CCTV) System at Bedford School, a member school of the Harpur Trust. 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 system (the system).

The system is administered and managed by the School, who act as the Data Controller, delegated by the Harpur Trust. This policy will be subject to review from time to time, and should be read with reference to the School's Data Protection Policy which can be found on the School's website.

For further guidance, please review the Information Commissioner's CCTV Code of Practice which is accessible [here](#).

The School's purposes of using the CCTV system are set out below and, having fully considered the privacy rights of individuals, the School believes these purposes are all within its legitimate interests. Data captured for the purposes stated below as objectives will not be used for any commercial purpose.

1. Objectives of the System

- To protect pupils, staff, volunteers, contractors, 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, contractors, visitors and members of the public
- To support the police and community in preventing and detecting crime and to assist in the identification and apprehension of offenders
- To monitor the security and integrity of the School site and deliveries and arrivals
- To monitor and uphold discipline among pupils in line with the School Rules, which are available to parents and pupils of the School
- To monitor staff and contractors for compliance related to employment and contractual obligations
- To record system data (recorded video footage) for a set period of time to enable retrospective reviewing of any incidents where CCTV data may assist investigations.

2. Positioning

- Locations have been selected, both inside and out, that the School reasonably believes require monitoring to address the stated objectives. The locations, at the date of writing, are listed in Appendix 1.

- Adequate signage has been placed in prominent positions to inform those who enter the School premises that they are entering a monitored area, identifying the School as the Data Controller and giving contact details for further information regarding the system.
- 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.
- No images will be captured from areas in which individuals would have a heightened expectation of privacy including, but not limited to, changing, washroom facilities and bedrooms.
- No images of public spaces will be captured except as background to cameras installed for a legitimate purposes such as at site entrances
- The School for the purposes of this policy includes all School grounds in De Parys Ave, sports fields including Gordon Fields, Ickwell conservation area, boarding houses and other properties owned or managed by the School.

3. Operation & Maintenance

- The system will be operational 24 hours a day, every day of the year.
- The System Manager will check, or arrange for the checking, and confirm that the system is properly recording and that cameras are functioning correctly on a regular basis.
- The system will be formally checked and to the extent necessary serviced no less than annually.
- The System Manager shall be the Deputy Bursar assisted by the IT Manager who will provide oversight for technical support and network connectivity.

4. Viewing of System Data

- The following staff shall have the right to view system data at any time: - the Head Master, the Vice Master, the Headmaster, the Bursar and Deputy Bursar.
- Other staff may be authorised to conduct routine viewing of system data on occasions where authorisation is provided by the Head Master, Vice Master, Bursar or Deputy Bursar.
- Staff checking and servicing the system and network may, from time to time inadvertently see recording but shall not purposefully access the system other than for the express purpose of checking and serving the system and network

- All viewing of system data will be in a suitably secure and private area to minimise the likelihood of or opportunity for access by unauthorised persons
- Viewing, in this context, will include both real time and retained footage

5. Storage of Data

- The day-to-day management of system data will be the responsibility of System Manager or such suitable person as the System Manager shall appoint in his or her absence.
- Subject to Clause 5.3, system data will be stored for no more than 30 days and automatically over-written unless the School considers it reasonably necessary for the pursuit of the objectives outlined above to retain the system data for longer, or is lawfully required to do so by an appropriate third party such as the police or local authority. Such data shall be limited to the footage relevant to the purposes for which it is being retained.
- Where such data is retained, it will be retained in accordance with legislation and the School's own Data Protection Policy and Data Retention Policy.
- Where system data is retained a log will be kept including the date, time and length of the recording, an outline of the purpose of the retention, the locations covered and where identifiable the names of groups or individuals recorded (See Appendix 3).
- All retained system data will be stored in one central, secure location determined by the IT Manager and wherever possible meet or exceed encryption and security standards recommended by ICO.

6. Access to Data

- Individuals have the right to access personal data the School holds on them (please see the Data Protection Policy), including information held on the system, if it has been retained.
- In line with Subject Access Requests under GDPR, the System Manager must satisfy themselves of the identity of any person wishing to view stored images or access the system and the legitimacy of the request.
- A CCTV Data Access request Form is available (See Appendix 2)
- The following are examples when the System Manager may authorise access to CCTV 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 may be informed as part of the School's management of a particular incident;
 - To provide recordings on data subjects (or their legal representatives) pursuant to an access request under the Act and on the basis set out in 6.2 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 there is, in the Head Masters opinion, a belief that accessing the data will assist in achieving any of the stated objectives of the system.
- A CCTV Log will be maintained to record all access requests, retained footage and viewings other than those listed in Clause 4.1 (See Appendix 3)
 - Where images are disclosed under Clause 6.3 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 or other reference number if applicable.
 - Where images are provided to third parties under Clause 6.3 above, practical steps will be taken to obscure images of non-relevant individuals.

7. Other CCTV systems

The School does not own or manage any 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, has legitimate and direct relevance to the operations of the School or is necessary as part of an investigative or process.

For example, while investigating an incident on a bus, CCTV footage from the bus' CCTV system may be relevant.

8. 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 System Manager or Bursar in the first instance.

Appendix 1 – CCTV Camera Locations

Camera number	Building	Location	Focus
1	School House	Front elevation	Entrance gate
2		Rear elevation	Patio doors
3		North elevation	Side access
4	Phillpotts House	Front elevation	HM entrance gate
5		West elevation	Boys entrance
6	Pemberley House	West elevation 17 side	Side gate
7		Front elevation 17 side	HM entrance gate
8		West elevation 15 side	Vehicle gate
9		Front elevation 15 side	AHM entrance gate
10	Chapel	Chapel path post	Pemberley pedestrian gate
11	Music School	North elevation	Music School gate
12		North elevation	Music School path
13	Science	Rear L1	Science path
14	Bursary	Rear elevation	Bursary car park
15		Rear elevation	Kitchen goods door
16	CCF	Entrance elevation	Main School side gates
17	Main School	North West corner	Glebe pedestrian gate
18		North West corner	Main School North porch
19		South side	Rec Centre path North
20	Mem Hall	South elevation	Drive way approaching Mem Hall
21	Burnaby	Burnaby Rd elevation	Phillpotts gates
22	1 Burnaby Road	Burnaby Rd elevation	Security Barrier
23		Burnaby Rd elevation	Main Entrance Road
24		South elevation	St Peters DH entrance door
25	Browns	Burnaby Rd elevation	Main entrance gates
26	Talbots House	Front elevation 27 side	HM entrance gates
27		East elevation 25 side	AHM entrance gates
28	Spare		
29	Rec Centre	Entrance lobby	Entrance door
30		Drinks corridor	Door lobby/drinks corridor
31		Changing room corridor	Rear entrance door
32	Wells Building	Bridge	Looking North
33		Bridge	Looking South
34		South West corner	North end of Palmers entrance
35	Eagle	East side	HM side gates
36		Tisdalls Front elevation	HM entrance gates
37	Palmers	Rear elevation	Entrance drive looking North
38		East elevation	Palmers gates
39	Inky	South elevation	Inky gate
40	Quarry Theatre	Front elevation	Looking North to entrance door
41		Front elevation	Looking South to entrance door
42		Public entrance lobby	Entrance doors
43		Vestry Lobby	School entrance doors
44		West elevation	Boys entrance
45		West elevation	School entrance

46	Fitzpatrick Building	North elevation	Art arch way
47		North elevation	Crescent gates
48	Redburn House	North elevation	Vehicle entrance gates
49		North elevation	Boys entrance gate
50		East elevation	HM entrance gate
51	Sandersons House	East elevation	HM entrance gate
52		South elevation	HM vehicle gates
53	Grounds Shed	Tractor store	Entrance door

This list is current as at March 2021 but may not be exhaustive or accurate as cameras are installed, removed or moved from time to time for operational reasons.

Appendix 2 – CCTV Data Access Request

The following information is required before the school can provide copies of or access to CCTV 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 recordings after 1 month.

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)	
Reason for request:	

Signature*

Print Name.....

Date.....

***NB 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.**

