CCTV Policy

Policy

CCTV Policy

Policy Review Dates

Review Date	Changes made	By whom	Date shared with staff
June 2025	Update to point 7.2.1	CST	June 2025
Jan 2026	Updated to 3 year review cycle. No other changes.	CST	Jan 2026
July 2026	Addition of new type of camera to be used on site.	CST	July 2026
October 2026	Policy updated following governance review: covert monitoring, DPIA, audio recording, data retention, disclosure and review arrangements.	CST	October 2026

Date ratified by Governors	Review Date
October 2026	January 2029

CCTV POLICY

1. Introduction

1.1. This policy is written in accordance with the General Data Protection Regulation ("GDPR") which came into force on 25 May 2018 and the Data Protection Act 2018.

1.2. Bedale High School (BHS) uses Closed Circuit Television ("CCTV") across its site for the following purposes:

1.2.1. To assist in providing a safe and secure environment for all students, staff and visitors.

1.2.2. To assist in the prevention and detection of crime and to assist law enforcement with investigations and criminal proceedings.

1.2.3. To assist in the prevention and detection of theft and criminal damage to all assets within BHS.

1.2.4. All cameras will be used to support positive behaviour in all schools and providing visual evidence of any incident as well as crime prevention and detection, including bullying.

1.3. This policy is intended to provide protection against the misuse of CCTV systems within BHS.

1.4. The CCTV system will never be used as part of any Performance Management process, for routine monitoring of staff performance or productivity, or for minor disciplinary matters. Any monitoring of staff must be necessary, proportionate and use the least intrusive means reasonably available.

2. CCTV Systems

2.1. BHS uses a variety of CCTV systems across the site. These systems consist of both analogue and IP cameras.

2.2. The cameras used on all systems consist of fixed cameras and movable cameras. These may also include cameras with the ability to zoom.

2.3. In remote locations such as school playing fields, the school uses solar powered 4G (Sim Card) cameras. These connect via a secure external APP.

2.4. CCTV is also in place on the school minibus. This system records to a separate facility on the school minibus and can only be accessed by authorised members of staff.

2.5. At the discretion of the Headteacher, Bedale High School may also install 'dummy' cameras – these do not have the functionality to record any data (image or audio) and are installed for the purposes of discouraging incidents.

Camera Locations

2.6. CCTV cameras are located both inside and outside of the school buildings:

2.6.1. All cameras will be visible and in prominent areas.

2.6.2. Cameras will not routinely be placed in offices or classroom. They may, however, be in place in some specialist learning spaces where staff supervision is low, or the nature of the students in the space creates a higher level of risk. In these instances, staff, students and visitors will be informed and clear signage displayed.

2.6.3. Cameras will not be installed in areas where additional privacy is expected such as changing rooms or toilets, however, sink areas may be monitored where appropriate and where the cameras cannot see into any areas of additional privacy.

2.6.4. BHS will do everything possible to ensure any area outside of the grounds of the school establishment is not visible on the cameras or recordings.

2.6.5. Signage will be displayed around the site ensuring staff, students and visitors are aware of the CCTV monitoring and how to find out more information.

2.6.6. Audio recording will be disabled by default. Audio will only be recorded in exceptional circumstances where there is a clearly documented necessity and lawful basis, and where the recording is proportionate to the identified purpose.

3. Covert Recordings

3.1. The school may, in exceptional circumstances, undertake covert monitoring where there are documented and reasonable grounds for suspecting criminal activity or gross misconduct, there is no reasonably available less intrusive way of investigating the matter, and informing the individual(s) concerned would seriously prejudice the purpose of the monitoring.

3.1.1. Covert monitoring means monitoring carried out in a manner calculated to ensure that the individuals subject to it are unaware that it is taking place.

3.1.2. Covert monitoring must be necessary and proportionate to a specified purpose, strictly targeted, and limited to the shortest practicable period.

3.2. Before covert monitoring begins, a Data Protection Impact Assessment (DPIA) must be completed, the advice of the school's Data Protection Officer (DPO) sought and recorded, and written authorisation obtained from the Co-Chair of Governors.

3.2.1. The written authorisation must record the suspected activity, the purpose of the monitoring, why covert monitoring is necessary, why less intrusive methods are inadequate, the area and persons to be monitored, the duration and review date, whether audio recording is proposed, who may access the footage, and the arrangements for retention and deletion.

3.2.2. Where proposed covert monitoring may fall within a statutory regime governing directed or covert surveillance, appropriate legal advice must be obtained before the monitoring commences.

3.3. Covert monitoring must cease as soon as the authorised purpose has been achieved, the authorised period has expired, or the investigation has concluded, whichever occurs first. Any extension must be specifically justified, reviewed and authorised.

4. Storage of Data

4.1. All data, with the exception of the solar paneled 4G cameras, is stored directly on the Network Digital Video Recorder (NDVR) which is physically secured and accessible only to authorised members of staff.

4.2. Images are retained on the NDVR for no longer than 14 calendar days and no less than 5 calendar days. In the event of a Hard Disk or NDVR Failure, BHS will attempt to recover footage, but the same data retention would apply.

4.3. Where data is stored externally by third parties, this is stored on a secure password protected application. Data will only be accessed by authorized members of staff via school devices. If BHS has reason to believe there is a significant threat to a site's security and may require recorded footage to be retained for longer than 14 calendar days, this will require approval from the Co-Chair of Governors and must have a specified end date.

4.4. Any images required longer than BHS retention period can be electronically held for review and must be deleted as soon as there is no longer basis to retain the data.

4.4.1. Where the school is legally required to retain images and data for longer than BHS' retention period for the purpose of evidential records, the school shall do so in a secure manner.

4.5. CCTV footage must not be retained merely because it may become relevant at some future point. Footage that is no longer required for the purpose for which it was obtained must be securely deleted in accordance with the school's retention arrangements.

4.6. Where monitoring captures information about individuals or activities unrelated to the

authorised purpose ('collateral intrusion'), the school will take reasonable steps to minimise such collection. Unrelated material will normally be disregarded and securely deleted unless it reveals a matter which the school could not reasonably be expected to ignore.

5. Privacy

5.1. The installation or relocation of any camera will first be subject to a documented impact assessment to ensure that the proposed monitoring is necessary and proportionate and complies with data protection requirements. Where the proposed processing is likely to result in a high risk to individuals, a formal Data Protection Impact Assessment (DPIA) will be completed before the processing begins. The school's DPO will be consulted where appropriate and records of the assessment and decision will be retained.

6. Access Management

6.1. Access to the CCTV recordings is controlled via assigned user accounts, which can only be used by designated members of staff.

6.2. The physical NDVR is kept securely locked away, preventing physical access.

7. Viewing of CCTV

7.1. Any viewing of footage is logged recording a minimum of date, time, person(s) accessing the footage, person supporting the viewing, reason for reviewing the footage, footage reviewed and a copy of the electronic authorisation form.

7.2. Viewing of CCTV will require an access form to be completed by the member of staff needing to review footage and then approved by the Headteacher prior to any footage being viewed **(Please see Appendix 1).** These forms must be retained.

7.2.1. In the event that the Headteacher is the requestor, a report must be provided to the Co-Chair of Governors at the earliest opportunity to state that the CCTV has been viewed and outline the reasons.

7.3. Viewing of the images should only be done for the purpose of items *1.2.1, 1.2.2, 1.2.3, 1.2.4.*

7.4. Routine access to the CCTV system by the following is authorised to enable them to carry out their daily duties.

7.4.1. IT Services – Maintenance of the physical system and software to ensure continued and reliable functionality.

7.4.2. Site Team – Access to cameras to maintain site security and daily functionality tests.

7.4.3. Contracted CCTV Monitoring Company – to monitor and maintain the security of the academy sites out of school hours.

7.5. **Viewing of live images**

7.5.1. Should only be done in line with item 3.1 or where there is suspicion that improper conduct may be carried out at a particular time.

7.5.2. Should only be in a controlled space with authorised personnel and monitors should not be left on unattended.

7.5.3. The privacy of staff and students going about their normal legitimate business must be respected at all times.

7.5.4. Viewing of live images should only be used where there is an immediate safeguarding risk to students or staff on site.

7.5.4.1. The use of access control entry systems is excluded. Entry systems will be used by members of staff to authorise visitor entry to the trust sites, no footage is recorded and is only live for the duration of the interaction between the visitor and the member of staff.

8. Disclosure

8.1. Images may be disclosed where there is a lawful basis to do so, including in response to a valid Subject Access Request, to law enforcement agencies where appropriate, where required by a court or other legal obligation, or to another party where disclosure is otherwise permitted by law.

8.1.1. Where an individual makes a Subject Access Request for CCTV footage, the school will consider the data protection rights of any other identifiable individuals shown in the footage. Where disclosure of unedited footage would adversely affect the rights and freedoms of others, the school will consider whether the footage can lawfully be disclosed and, where appropriate and reasonably practicable, whether alternative arrangements can be made to facilitate disclosure.

8.2. Images will not be disclosed where disclosure would be unlawful or where an applicable exemption permits the school to withhold the information, including where appropriate to avoid prejudicing the prevention or detection of crime or an ongoing criminal investigation.

8.3. All requests for disclosure will be recorded, where a request is declined the reason will also be recorded.

9. Complaints

9.1. Complaints regarding the procedures laid down in this policy will follow that set out in the school Complaint's Policy.

9.2. Complaints relating to information handling may be referred to the Information Commissioner.

10. Monitoring, Evaluation and Review

10.1. This policy will be reviewed at least every three years, or sooner where required.

10.2. Any amendments to legislation may instigate a review of this policy at any time.