BORDEN GRAMMAR SCHOOL

CCTV Policy

Review Responsibility:	Headteacher
Frequency of Review:	2 years
Date Approved:	Sep 25
Approved By:	Board of Trustees
Next Review Due By:	Sep 27

Contents

1. Aims

This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

1.1 Statement of Intent

The purpose of the CCTV system is to:

- Make members of the school community feel safe (both students and staff)
- Protect members of the school community from harm to themselves or to their property
- To ensure the behaviour policy is upheld
- 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 defense 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 inside 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 list of uses of CCTV is not exhaustive and other purposes may be or become relevant.
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 the 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.

2. Relevant Legislation and Guidance

Schools can use CCTV lawfully under the "public task" basis if the processing is necessary for performing a task in the public interest or exercising official authority, often for safety and security purposes, or under the "legitimate interests" or "vital interests" basis for broader needs like deterring crime, safeguarding or protecting assets. Since pupils are minors, extra care will be taken to comply with the ICO's 'Children and Data Protection Guidance'.
This policy is based on the 12 guiding principles of transparency, specified purpose, pressing need, proportionality, accountability, regular review, information security, disclosure, storage restriction, restricted access, standards and effective use (Appendix 1). It is also based on the following legislation.

2.1 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 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

2.2 Guidance

- Surveillance Camera Code of Practice (2021)

3. 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

4. Covert Surveillance

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 (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law. Additionally, the proper authorisation forms from the Home Office will be completed and retained where necessary.

5. Location of the Cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).
Cameras are located in:

- Most school corridors (including outside of the toilets but not inside)
- Covering all external areas of the school site including social areas, entrances and exits to the school
- Computer based classrooms (including the music room)
- The main hall/dining area
- The school Library and 6th form workspace
- The inclusion hub, including the reflection space

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 and data controller of the CCTV system.
Cameras are not and will not be aimed off school grounds into public spaces or people's private property.
Cameras will not ordinarily be used to monitor normal teacher/student activity in the school.
Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

6. Roles and Responsibilities

6.1 The Trust Board

The governing board has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

6.2 The Headteacher

The headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the data protection officer (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 having 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

6.3 The Data Protection Officer (DPO)

The DPO will:

- Ensure staff are trained to recognise a subject access request
- Deal with subject access requests in line with the UK GDPR and Data Protection Act 2018
- 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 (ICO)
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Keep accurate records of all data processing activities and make the records public on request
- Through the school's Data Privacy Notice, 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
- Receive and consider requests for third-party access to CCTV footage

6.4 The System Manager

The system manager 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
- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Conduct data protection impact assessments
- Ensure footage is destroyed when it falls out of the retention period
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces

- Carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period

7. 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 school will only record audio having completed a DPIA justifying the specific need, consulted with the DPO and having consulted with stakeholders.
Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

8. Storage of CCTV Footage

Footage will be retained for 30 days. At the end of the retention period, the files will be overwritten automatically.
On occasion footage may be retained for longer than 30 days, for example where a behaviour incident has been formally investigated and a sanction put in place or information needs to be shared with a law enforcement body investigating a crime. If this is the case there will be a review every additional 15 days to check that retention is still necessary.
Recordings will be downloaded onto a password protected secure drive, 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.

9. Access to CCTV Footage

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage. The headteacher will allow access to specified trained staff only and access will be password protected with logs kept.
Access to such footage by individuals will be logged with their name, date and time.
Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

9.1 Staff Access

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

- The headteacher / deputy headteacher:
- The DPO:
- The system manager:
- Senior staff responsible for safeguarding and behaviour
- The pastoral support team.

CCTV footage will only be accessed from authorised personnel's 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.

9.2 Subject Access Requests (SAR)

According to the UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves.

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.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it. This will be shared using an encrypted zip file with the password shared separately or through a similar third party encrypted file sharing system.

Individuals wishing to make an SAR should refer to the school's GDPR & Data Protection Policy on the website for more information.

9.3 Third-party Access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (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).

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 the UK GDPR.

The school will not share CCTV footage with parents/carers. The only exception will be in exceptional circumstances where it is deemed necessary by the headteacher. The school will only show CCTV footage to students where they themselves are the object of the footage with permission of the headteacher. Any footage shown will be redacted prior or there has been prior consent from parents/carers of students in the footage.

All disclosures will be recorded by the designated person.

10. 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 its replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

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 and lead the carrying out the DPIA.

Those whose privacy is most likely to be affected, consultation will be considered where proportionate and appropriate, and any appropriate safeguards will be put in place.

A new DPIA will be done annually and/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.

11. Security

- The system 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

12. Complaints

Complaints should be directed to the headteacher or the DPO and should be made according to the school's complaints policy.

13. Monitoring

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

14. Links to Other Policies

- GDPR & Data Protection policy
- Searching, Screening & Confiscation Policy
- Behaviour Policy
- Safeguarding Policy

Appendix 1 - Guiding Principles

System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.