Initial Policy date	April 2020	Next scheduled review	June 2025
Governor approved	June 2024	Key person/people	Senior Site & Facilities Strategic Lead
Model Policy		Model localised	Yes
Pupil leadership team review		~~Y / N /~~ N/A	

CCTV Policy and Code of Practice.

1. Introduction.

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 our properties.

CCTV is primarily installed at The Westgate School premises for the purposes of employees, premises security, and in the interest of child safety. Cameras are located at various places within the internal and external area around the premises, and images from the cameras are recorded. Internal and external signage are displayed stating the presence of CCTV.

The CCTV system will be operational 24 hours a day, 365 days a year. Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

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 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 Westgate School is the Controller of the personal data processed through use of the school CCTV system.

In order to comply with these requirements, the school will need a lawful basis for each of these processing purposes, data must be:

- Fairly and lawfully processed
- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate

- Not kept for longer than is necessary
- Processed in accordance with individuals' rights
- Secure

2. Statement of Intent

As the Data Protection Officer, the Senior Site & Facilities Strategic Lead is the appointed individual with responsibility for the school's CCTV use, management and oversight.

The purpose of our CCTV system is to:

- Make members of the school community feel safe
- Protect members of the school community from harm to themselves or to their property
- Deter criminatlity 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 an disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defence of an litigation proceedings

The CCTV system will not beused to:

- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heighted expectation of privacy
- 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.

3. Relevant legislation and guidance.

This policy is based on:

3.1 Legislation:

- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- 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 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
- The School Standards and Framework Act 1998

- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

3.2 Guidance

- Surveillance Camera Code of Practice (2021)

4. Storage of CCTV footage.

Footage will be retained up to 14 days. At the end of the retention period, the files will be overwritten automatically.

On occasion footage may be retained for longer than 14 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

In such cases recordings will be downloaded and encrypted, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required.

The system does not have an automatic power backup facility which may operate in the event of a main supply power failure.

5. Control of access to images.

It is important that access to, and disclosure of, images recorded by CCTV and similar surveillance equipment 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.

6. Roles and responsibilities and access to images by authorised Employees.

Access to recorded images is restricted to the approved appointed roles, who will decide whether to disclose images and recordings following receipt of requests for access by data subjects and/or third parties (see serial 8), and in accordance with the law.

The appointed roles are:

- **Members of the governing body**: on a need to know only basis and for ensuring CCTV system is operated within the parameters of this policy
- **The Headteacher:** liaise with the DPO to ensure use of CCTV system is in accordance with the stated scope of this policy
- **Data Protection Officer (DPO):** Monitor compliance within this policy in accordance with UK data protection law. Deal with subject access requests in line with the Freedom of Information Act (2000)
- **The system managers** : Oversee security and maintenance of system.
- **Senior Leadership Team:** is authorised to view footage in response to an incident
- **Authorised employees.** Any authorised colleagues under express permission of the Headteacher

Viewing of images must be documented as follows:

- The name of the person removing from secure storage, or otherwise accessing, the recordings
- The date and time of removal of the recordings
- The name(s) of the person(s) viewing the images (including the names and organisations of any third parties)
- The reason for the viewing
- The outcome, if any, of the viewing
- The date and time of replacement of the recordings

7. Removal of image for use in legal proceedings.

In cases where recordings are removed from secure storage for use in legal proceedings, the following must be documented:

- The name of the person removing from secure storage, or otherwise accessing, the recordings
- The date and time of removal of the recordings
- The reason for removal
- Specific authorisation of removal and provision to a third party
- Any crime incident number to which the images may be relevant
- The place to which the recordings will be taken
- The signature of the collecting police officer, where appropriate
- The date and time of replacement into secure storage of the recordings

8. Access to images by third parties.

Requests for access to images will be made using the 'Application to access to CCTV images' form (which is at Appendix 1).

The data controller will assess applications and decide whether the requested access will be permitted. Release will be specifically authorised. Disclosure of recorded images to third parties will only be made in limited and prescribed circumstances. For example, in cases of the prevention and detection of crime, disclosure to third parties will be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry – upon recipient of a data request form
- Prosecution agencies
- Relevant legal representatives
- The press/media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)

All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented as above.

9. Access by data subjects.

Under UK data protection laws, individuals have a right to access and receive a copy of their personal data, and other supplementary information. Using the 'Application to access to CCTV images' form (found at Appendix one).

10. Subject Access Request (SAR).

All requests for access by Data Subjects will be dealt with by the Data Protection Officer (DPO).

Upon receiving the request, the school will immediately issue a receipt and will then respond within 30 days during term time. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate employees.

The data controller will locate the images requested. The data controller will determine whether disclosure to the data subject would entail disclosing images of third parties, and where appropriate consent will be sought.

The data controller will need to determine whether the images of third parties are held under a duty of confidence. In all circumstances The Westgate School indemnity insurers will be asked for advice on the desirability of releasing any information.

If third party images are not to be disclosed, the data controllers will arrange for the third party images to be disguised or blurred. If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out. If an editing company is used, then the data controller must ensure that there is a contractual relationship between them and the editing company, and:

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images
- The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the data controllers
- The written contract makes the security guarantees provided by the editing company explicit

An individual is only permitted to have access to data or information that is about or relates to themselves. If others are present in the footage, then generally these should be redacted unless there is clearly no risk to that individual from being disclosed.

Where possible, The Data Controller will consider whether it is possible to comply with the request without disclosing information that identifies another individual.

The DPO will provide an acknowledgement of receiving the request setting out the data controllers' decision on the request.

A copy of the request and response should be retained.

11. Complaints.

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

12. 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.

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 on how to carry out the DPIA.

If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

Appendix one. Application for CCTV Data Access.

Appendix one. Application for CCTV Data Access.

ALL Sections must be fully completed. Attach a separate sheet if needed.

Name and address of Applicant	
Name and address of "Data Subject" – i.e. the person whose image is recorded	
If the data subject is not the person making the application, please obtain a signed consent from the data subject opposite	Data Subject signature…….
If it is not possible to obtain the signature of the data subject, please state your reasons.	
Please state your reasons for requesting the image.	
Date on which the requested image was taken.	
Time at which the requested image was taken.	
Location of the data subject at time image was taken (i.e. which camera or cameras.)	
Full description of the individual, or alternatively, attach to this application a range of photographs to enable the data subject to be identified by the operator.	
Please indicate whether you (the applicant) will be satisfied by viewing the image only.	

OFFICE USE ONLY	**OFFICE USE ONLY**
Access granted (tick)	
Access **not** granted (tick)	Reason for not granting access:
Data Controller's name: Signature: Date:	