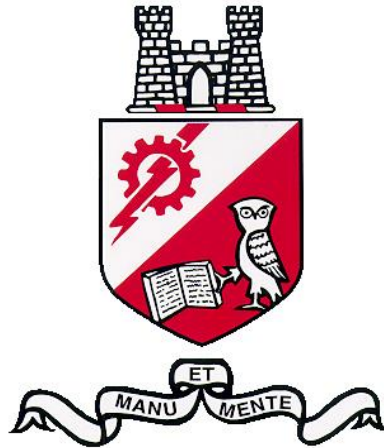


WEST HATCH HIGH SCHOOL



THE BEST THAT I CAN BE

CCTV Policy

Policy reviewed:

January 2023

A handwritten signature in black ink, likely belonging to the Headteacher, is placed above the title 'Headteacher'.

Signed:

Headteacher

Review Date:

January 2024

Contents

Policy Statement	3
1. Introduction.....	3
2. Statement of Intent.....	3
3. Siting the Cameras.....	4
4. Covert Monitoring.....	4
5. Storage and Retention of CCTV images	4
6. Access to CCTV images	4
7. Subject Access Requests (SAR)	5
8. Access to and Disclosure of Images to Third Parties.....	5
9. Complaints.....	5
Further Information	5
APPENDIX 1.....	6
CCTV – PROTOCOL FOR USE AND DISCLOSURE OF IMAGES	6
APPENDIX 2.....	7
CCTV – Request to View	7
APPENDIX 3.....	9
CCTV - Results Release Form	9

West Hatch High School

Policy Statement

This document sets out the appropriate actions and procedures, which must be followed to comply with the Data Protection Act in respect of the use of CCTV (closed circuit television) surveillance systems managed by West Hatch High School.

1. Introduction

- 1.1 West Hatch High School uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to help prevent the loss or damage to school property.
- 1.2 The system comprises of a number of static cameras.
- 1.3 The system does not have sound recording capability.
- 1.4 The CCTV system is owned and operated by the school and the deployment of which is determined by the school's leadership team.

Responsible Person: Data Controller

The person who has been appointed to oversee the system and procedure is the Headteacher.

- 1.5 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.
- 1.6 Routine checks are made to ensure that the system is operating in accordance with the terms of this policy, and that information relating to the recordings (date, time etc.) are accurate; these details are entered into the CCTV Viewing Log.
- 1.7 Procedures for managing the saved data is detailed in the CCTV Viewing Log – staff are trained to understand the administrative regime to control the use of the images.

2. Statement of Intent

- 2.1 The school complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at:

<https://www.gov.uk/government/publications/update-to-surveillance-camera-code>

- 2.2 CCTV warning signs are clearly and prominently placed around the school.
- 2.3 The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3. Siting the Cameras

- 3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the ICO Code of Practice.
- 3.2 The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.
- 3.3 CCTV will not be used in classrooms with the exception of the ICT rooms.
- 3.4 CCTV will be placed in communal areas located in the toilets but not covering the cubicles or urinals.
- 3.5 Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

4. Covert Monitoring

- 4.1 The school may in exceptional circumstances set up covert monitoring. For example:
- i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
 - ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.
- 4.2 In these circumstances authorisation must be obtained from the Headteacher.
- 4.3 Covert monitoring must cease following completion of an investigation.
- 4.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets. We will however site cameras in the main communal areas located in the toilets but will not cover cubicles and urinals.

5. Storage and Retention of CCTV images

- 5.1 Digital media is used to record images. Recorded data will normally be retained for a minimum of two weeks, unless an incident occurs which necessitates extraction and retention of said piece of evidence. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.
- 5.2 All retained data will be stored securely in a central area and can only be accessed by those who are authorised to do so.

6. Access to CCTV images

- 6.1 Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.
- Downloading images is strictly controlled and limited to the following staff:
- | | |
|----------------|-------------------|
| Head Caretaker | view and download |
|----------------|-------------------|

IT Network Manager	view and download
Behaviour Manager	view and download

The following staff are permitted to view footage alongside one of the above-authorized staff:

Headteacher and Senior Leadership Team	view only
Heads of Year and Pastoral Managers	view student related incidents only
Named individuals approved by the Headteacher	view only

6.2 A minimum of two staff listed above should be present when viewing communal toilet footage to safeguard staff.

6.3 The CCTV Viewing Log should be promptly completed every time footage is accessed, viewed or downloaded. A physical version of Appendix 2 and 3 should be completed and signed when CCTV is transferred outside of West Hatch High School.

7. Subject Access Requests (SAR)

7.1 Individuals have the right to request access to CCTV footage relating to themselves under The General Data Protection Regulation (EU) 2016/679 ("GDPR").

7.2 All requests should be made in writing to the Headteacher as a Subject Access Request. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

7.3 The school will respond to requests within the timeframe set under the regulation.

7.4 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

8. Access to and Disclosure of Images to Third Parties

8.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

8.2 Requests should be made in writing to the Headteacher by way of a Subject Access Request.

8.3 The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

9. Complaints

9.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

Further Information

Further information on CCTV and its use is available from the following:

- Surveillance Camera Code of Practice (Published June 2013, Amended November 2021)
- www.ico.gov.uk
- Regulation of Investigatory Powers Act (RIPA) 2000

- The General Data Protection Regulation (EU) 2016/679 ("GDPR")

APPENDIX 1

CCTV – PROTOCOL FOR USE AND DISCLOSURE OF IMAGES

Legitimate public concerns exist over the use of CCTV and many of the specific guidelines are designed to satisfy the community that the use of cameras is subject to adequate supervision and scrutiny. It is of fundamental importance that public confidence is maintained by fully respecting individual privacy. All employees that are authorised to view the CCTV images within West Hatch High School must read this protocol alongside the CCTV Policy and confirm that they understand and agree to abide by the policy and protocol.

CCTV images may only be view by named individuals.

All authorised employees viewing the CCTV images will act with utmost probity at all times.

All images viewed by authorised employees must be treated as confidential.

All authorised employees are to ensure that whilst viewing CCTV images, unauthorised employees or visitors cannot view the images.

All authorised employees are responsible to ensure that CCTV images are not left on any screen without an authorised employee being left in charge. An authorised employee should log out of the programme when leaving the screen.

Every viewing of the images will accord with the purposes and key objectives of the CCTV system and shall comply with the CCTV Policy.

All named individuals viewing CCTV images are responsible for their every viewing of the images, which must be justifiable.

Any breach of the CCTV Policy or CCTV Protocol will be dealt with in accordance with existing discipline regulations. Individuals must recognise that any such breach may amount to gross misconduct, which could lead to dismissal.

Any breach of the The General Data Protection Regulation (EU) 2016/679 ("GDPR") will be dealt with in accordance with that legislation. All authorised employees viewing CCTV images must be aware of their liability under this act.

I understand and agree to abide by the CCTV Policy and the CCTV Protocol.

Print Name	Job Title
Signature	Date

--	--

APPENDIX 2 – Completed Electronically for all requests to view.**CCTV – Request to View**

Applicants Name:

Date of Request:

Reason for Request			
Named Individual dealing:			
General Data Protection Request/Subject Access Request:		Yes / No	
Daily/Periodical Security Check		Yes / No	
System Check		Yes / No	
Necessary for one or more of the purposes e.g.: Crime / Emergency / Child – Staff Safety / Protection of others (please circle)			
Issue being investigated:			
Date of incident:		Time of incident:	
Justification in the circumstances			
Crime / Serious Incident / Preserving Evidence / Persons' Safety / Legal Request (please circle) Other:			
Proportionality (This involves balancing the extent of the intrusiveness of the interference with an individual's right of respect for their private life against a specific benefit to the investigation)			
Urgent need / only way of detection (please circle) / Other:			
Privacy/Collateral Intrusion (Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity)			
Named individual only viewing	Yes / No	Reviewed in private area	Yes / No (If No – detail overleaf)
Name (s) of others present :		Reason: Assist with identification / knowledge of incident / SLT / Police (please circle)	
CI will be dealt with by: (Give any other details)		Review time reduced to a minimum Yes / No If No state reason:	
Any copies made (If Yes – please complete relevant result / release form!)		Yes / No	

Name of Staff reviewing:

Signature:

Date and time:

CCTV – Request to View

Additional Notes:

APPENDIX 3

Results Release Form	
Named Individual dealing:	
Date and Exact Time of CCTV Footage	
Cameras Reviewed	
Result i.e. CCTV shows nil, incident in question, identifies offender, etc. Please detail in brief.	
Has the recording been saved?	Yes / No
File name and location stored.	
If yes, by whom?	
Any copies taken?	Yes / No
Who possesses these?	
Was this part of a Subject Access Request?	Yes / No
If Yes, what was the SAR Reference Number?	
Authority to release by Data Controller Signature, Date and Time	
Person releasing copy Signature, Date and Time	
Person receiving copy Include name, Company and contact details Signature, Date and Time	It is my responsibility to comply with Data Protection Legislation in relation to any further disclosures