HOE VALLEY SCHOOL
CCTV POLICY

Person Responsible:	Board of Governors
Date Adopted:	March 2019
Date of last review:	Autumn 2020
Date of next review:	Autumn 2022

INTRODUCTION

The school recognises that CCTV systems can be privacy intrusive.

For this reason, the school has carried out a data protection impact assessment with a view to evaluating whether the CCTV system in place is a necessary and proportionate means of achieving the legitimate objectives set out below.

The result of the data protection impact assessment has informed the school's use of CCTV and the contents of this policy.

Review of this policy shall be repeated regularly and whenever new equipment is introduced a review will be conducted and a risk assessment put in place. We aim to conduct reviews no later than every two years.

The purpose of this Policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at the school.

1. OBJECTIVES

The purpose of the CCTV system is to assist the school in reaching these objectives:

- To protect pupils, staff and visitors against harm to their person and/or property
- To increase a sense of personal safety and reduce the fear of crime
- To protect the school buildings and assets
- To support the police in preventing and detecting crime
- To assist in identifying, apprehending, and prosecuting offenders
- To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence
- To assist in managing the school

2. CCTV system

The CCTV system used by the school are listed in appendix 1

3. STATEMENT OF INTENT

3.1 Notification has been submitted to the Information Commissioner and the next renewal date has been recorded.

3.2 The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice.

3.3 The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

3.4 The system has been designed to deny observation on adjacent private homes, gardens and other areas of private property.

3.5 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

3.6 Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system 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.

3.7 Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

3.8 Recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated. In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 30 days.

4. SYSTEM MANAGEMENT

4.1 Access to the CCTV system and data shall be password protected.

4.2 The CCTV system will be administered and managed by the IT Manager, who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager the system will be managed by the School Business Manager.

4.3 The system and the data collected will only be available to the Systems Manager, his/her replacement and appropriate members of the senior leadership team as determined by the Headteacher.

4.4 The CCTV system is designed to be in operation for 24 hours each day, every day of the year, though the school does not guarantee that it will be working during these hours.

4.5 The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

4.6 Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images.

4.7 Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned in paragraph 4.3 above, requests access to the CCTV data or system, the System Manager must satisfy himself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused.

Details of all visits and visitors will be recorded in a system log book including time/data of access and details of images viewed and the purpose for so doing.

5. DOWNLOADING CAPTURED DATA ONTO OTHER MEDIA

5.1 In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events from the hard drive must be prepared in accordance with the following procedures: -

- Each download media must be identified by a unique mark.
- Before use, each download media must be cleaned of any previous recording.
- The System Manager will register the date and time of download media insertion, including its reference.
- Download media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a download media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.
- If download media is archived the reference must be noted.

5.2 Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his replacement and the Headteacher and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable if possible, for that person to withhold viewing of the data until asked to do so by the police.

5.3 A record will be maintained of the viewing or release of any download media to the police or other authorised applicants. Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the download media (and any images contained thereon) remains the property of the school, and download media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.

5.4 The police may require the school to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police. Applications received from outside bodies (e.g. solicitors or parents) to view or release images will be referred to the school's Data Protection Officer and a decision made by a senior leader of the school in consultation with the school's data protection officer.

6. COMPLAINTS

Any complaints in relation to the school's CCTV system should be addressed to the Headteacher.

7. REQUEST FOR ACCESS FROM THE DATA SUBJECT

The Data Protection Act provides Data Subjects – those whose image has been captured by the CCTV system and can be identified - with a right to data held about themselves, including those obtained by CCTV. Requests for such data should be made to the School Business Manager

8. PUBLIC INFORMATION

Copies of this policy will be available to the public from the school office.

APPENDIX 1

Camera area	Model	Pointed
RUN OF SERVER 10.10.0.199		
GROUND FLOOR		
(01) GF S Stairs	DS-2CD2555FWD-I	Staircase 4
(02) GF E Stairs	DS-2CD2555FWD-I	Staircase 2
(03) GF Food	DS-2CD2555FWD-I	Food corridor to Dining Hall
(04) GF E Toilets	DS-2CD2555FWD-I	Toilet sinks East Toilets
(05) GF Dining	DS-2CD2555FWD-I	Dining Hall to Food corridor
(06) GF Dining Q	DS-2CD2555FWD-I	Canteen Shutter
(07) GF W Stairs	DS-2CD2555FWD-I	Back of Staircase 3
(08) GF W Stairs	DS-2CD2555FWD-I	Staircase 3
(09) GF S Corridor	DS-2CD2555FWD-I	Door to Staircase 3
(10) GF S Toilets	DS-2CD2555FWD-I	Toilet sinks South Toilets
(47) Worton Hall	DS-2CD6924F-I(S)(/NFC)	Worton Hall
(48) Dining Hall	DS-2CD6924F-I(S)(/NFC)	Dining Hall
(50) Admin Corridor	DS-2CD2955WD-1(S)	SLT corridor
(51) GF S Corridor	DS-2CD2555FWD-I	Food Corridor
(52) Reception	DS-2CD2555FWD-I	Reception
1st FLOOR		
(11) FF S Stairs	DS-2CD2555FWD-I	Staircase 3
(12) FF E Stairs	DS-2CD2555FWD-I	Staircase 2
(13) FF E Corridor	DS-2CD2555FWD-I	Door to Staircase 2
(14) FF E Corridor	DS-2CD2555FWD-I	English Corridor to Staircase 2
(15) FF E Toilets	DS-2CD2555FWD-I	Toilet sinks East Toilets
(16) FF E Lockers	DS-2CD2555FWD-I	Staircase 1 to English corridor
(17) FF N Stairs	DS-2CD2555FWD-I	Staircase 1
(18) FF N Corridor	DS-2CD2555FWD-I	Music to Founders Hall
(19) FF N Lockers	DS-2CD2555FWD-I	Founder Hall corridor
(20) FFW Corridor	DS-2CD2555FWD-I	Door to Staircase 3
(21) FF W Stairs	DS-2CD2555FWD-I	Staircase 3
(22) FF S Corridor	DS-2CD2555FWD-I	Humanities corridor to Staircase 4
(23) FF S Corridor	DS-2CD2555FWD-I	Door to Staircase 4
2nd FLOOR		
(24) SF E Stairs	DS-2CD2555FWD-I	Staircase 2
(25) SF E Corridor	DS-2CD2555FWD-I	Door to Staircase 2
(26) SF E Corridor	DS-2CD2555FWD-I	MLF corridor to Staircase 2
(27) SF E Toilets	DS-2CD2555FWD-I	Toilet sinks East Toilets
(28) SF N Corridor	DS-2CD2555FWD-I	Corridor to 229 Room
(29) SF N Corridor	DS-2CD2555FWD-I	Door to Staircase 1
(30) SF N Stairs	DS-2CD2555FWD-I	Staircase 1

(31) SF E Lockers	DS-2CD2555FWD-I	MFL corridor
(32) SF W Lockers	DS-2CD2555FWD-I	Science corridor
(33) SF W Corridor	DS-2CD2555FWD-I	Door to Staircase 3
(34) SF W Stairs	DS-2CD2555FWD-I	Staircase 3
(35) SF S Toilets	DS-2CD2555FWD-I	Toilet sinks South Toilets
(36) SF S Corridor	DS-2CD2555FWD-I	Maths corridor to Staircase 4
(37) SF S Corridor	DS-2CD2555FWD-I	Door to Staircase 4
(38) SF Stairs	DS-2CD2555FWD-I	Staircase 4
(49) Sixth Form	DS-2CD6924F-I(S)(/NFC)	Sixth Form
OUTSIDE		
(39) Front Door	DS-2CD6924F-I(S)(/NFC)	Outside Reception
(40) Rear Play1	DS-2CD6924F-I(S)(/NFC)	Playground
(41) Rear Play 2	DS-2CD6924F-I(S)(/NFC)	Playground
(42) Rear Play 3	DS-2CD6924F-I(S)(/NFC)	Playground
(55) Bike Sheds	DS-2DE4225IW-DE(D)	Bike Sheds
(56) Rear V Gate	DS-2DE4225IW-DE(D)	Rear gate 3
(56) Ipdome	DS-2PT3326OZ-DE3	Playground
(58) Kitchen Rear	DS-2CD6924F-I(S)(/NFC)	Kitchen Door
(59) Front	DS-2CD6924F-I(S)(/NFC)	Student gate
(60) PTZ Front	DS-2PT3326OZ-DE3	Carpark
2 further cameras	Not specified	MUGA
RUN OF SERVER 10.10.0.200		
GROUND FLOOR		
Ground Art	DS-2CD2555FWD-I	Art corridor
1st FLOOR		
Camera 01	DS-2CD2555FWD-IS	Inclusion
Camera 02		
Camera 03		
Camera 04		