 HOLYPORT COLLEGE	CCTV Policy	
	Effective Date: 09 Jan 2023	Version No: v1.3


Title	CCTV Policy
Persons responsible for policy formulation, implementation, maintenance and evaluation	IT Network Manager
Persons consulted	Bursar Head Master Satswana
Created on	16 May 2018
Revised version adopted	Jan 23
Date of future review	Jan 26

REVISION STATUS TABLE

Revision No	Effective Date	Summary of Revision	Reviewed		Approved	
			By	Date	By	Date
v1.0	16.05.2018	New Policy	SLT		FGB	16.05.2018
v1.1	Autumn 2018	Review				
v1.2	Mar 2020	Review and update in accordance with updated GDPR regulations	SLT	02 Mar. 2020	GFC	05.03.2020
v1.3	09.01 23	Review	SLT	09.03.23	SLT	09.03.23

POLICY DOCUMENT REVIEW

This Policy document is subject to a review (every 3 years) by Holyport College that is formally documented to ensure its continuing suitability, adequacy and effectiveness. Areas subject to review include, but are not limited to, follow-up action from previous reviews, policy conformity, review of complaints, status of corrective and preventive actions, and improvements for the forthcoming year. Holyport College reserves the right to amend this Policy by notice following such review in circumstances in which it considers such change to be necessary or appropriate.


 HOLYPORT COLLEGE	CCTV Policy	
	Effective Date: 09 Jan 2023	Version No: v1.3

Contents

INTRODUCTION	2
STATEMENT OF INTENT	3
SITING THE CAMERAS	3
COVERT MONITORING	4
STORAGE AND RETENTION OF CCTV IMAGES	5
ACCESS TO CCTV IMAGES	5
SUBJECT ACCESS REQUESTS (SAR)	5
ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES	6
COMPLAINTS	6
FURTHER INFORMATION	6
APPENDIX A – CCTV CHECKLIST	7
ANNEX B – CCTV SIGNAGE	9

INTRODUCTION

1. Holyport College (“the College”) uses closed circuit television (CCTV) and the images produced to prevent or detect crime, vandalism and to monitor the College buildings and grounds in order to provide a safe and secure environment for its pupils, staff and visitors, and to prevent loss or damage to school property and surrounds. This policy outlines the College’s use of CCTV and how it complies with the General Data Protection Regulation; it is to be read in conjunction to the College’s data protection policy.
 - a. The system comprises a number of fixed and dome cameras.
 - b. The system does not have sound recording capability. However, it is not utilised.
 - c. The system is not linked to staff or pupil attendance records.
 - d. The system is not linked to automated facial recognition or number plate recognition software thus all individuals’ images are anonymous until viewed.
2. The CCTV system is owned and operated by the College, the deployment of which is determined by the College’s Senior Leadership Team.
3. The CCTV is monitored securely from various locations around the site. The College digital recorders store the images and is retained on-site. Access to the images is controlled by the Bursar, or in their absence, the IT Network Manager / IT technician and is password protected.
4. The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and members of the College community.

 HOLYPORT COLLEGE	CCTV Policy	
	Effective Date: 09 Jan 2023	Version No: v1.3


5. The College's CCTV Scheme is included in the College's registration with the Information Commissioner as a data processor.
6. All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. Through this policy, all operators are made aware of their responsibilities in following the CCTV Code of Practice. The College's 'Data Controller' is the Bursar, who will ensure that all employees are aware of the restrictions in relation to access to and disclosure of, recorded images by publication of this policy.

STATEMENT OF INTENT

7. The College complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure that CCTV is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at:
 - a. <https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-ofpractice.pdf>
8. The College's CCTV surveillance cameras are a passive technology that only records and retains images. They are not linked to automated decision making or facial or number plate recognition software. Transmission is by cable direct to the server.
9. CCTV warning signs are clearly and prominently placed at the main external entrance to the College, including further signage in other outdoor areas in close proximity to camera positions. Signs will contain details of the purpose for using CCTV (see annex B). In areas where CCTV is used, the College ensures prominent signs are placed within the controlled area.
10. The recordings will be filed with accurate metadata noting the camera location and time of the recording.
11. The original planning, design and installation of CCTV equipment endeavoured to ensure that the scheme would deliver 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.

SITING THE CAMERAS

12. Cameras are sited so that they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated.
13. The College will make every effort to position cameras so that their coverage is restricted to the College premises, which includes outdoor/indoor areas. The system design is sympathetic to the privacy of surrounding public and does not monitor public space outside the legitimate areas of interest for the College.
14. CCTV will not be used in classrooms or to monitor behaviour but in limited areas within the College building that may be identified to review access to the building.


 HOLYPORT COLLEGE	CCTV Policy	
	Effective Date: 09 Jan 2023	Version No: v1.3

15. Cameras are currently sited as follows:

<u>Location</u>	<u>No of cameras</u>
Front gate	2 external on standalone system
Winton	5 external on Honeywell system 1 internal on Honeywell system (reception entry and exit)
Brunel and Turing	8 external on Honeywell system 8 internal on Serage system (common areas entry and exit)
Fawcett and Johnson	8 external on Honeywell system 8 internal on Serage system (common areas entry and exit)
Sports hall	4 external on Honeywell system 2 external on robotics

COVERT MONITORING

16. It is not the College's policy to conduct 'Covert Monitoring' unless there are 'exceptional reasons' for doing so. Any such monitoring would be temporary and be justified as 'exceptional'. The covert surveillance activities of public authorities are governed by the Regulation of Investigatory Powers Act (RIPA) 2016. Such type of recording is covert and directed at an individual or individuals. The College may, in exceptional circumstances, determine a sound reason to covert monitor via CCTV. For example:
- a. 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;
 - b. Where notice about the monitoring would seriously prejudice the reason for making the recording.
17. In these circumstances authorisation must be obtained from the Head Master and/or the Bursar and the College's 'Data Controller' advised before any commencement of such covert monitoring.
18. Covert monitoring must cease as soon as necessary, such as following completion of an investigation.

 HOLYPORT COLLEGE	CCTV Policy	
	Effective Date: 09 Jan 2023	Version No: v1.3

19. Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles, changing areas etc.

STORAGE AND RETENTION OF CCTV IMAGES


20. Recorded data will not be retained for longer than is necessary. 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.
21. All retained data will be stored securely at all times and permanently deleted as appropriate / required.
22. Recorded images will be kept for no longer than 3 months, except where there is lawful reason for doing so, such as discipline investigations. Images are deleted from both the server and back-up server.

ACCESS TO CCTV IMAGES

23. Access to stored images will only be granted in the case of an incident. To be viewed in the course of the incident's investigation.
24. Any access to recorded images is required to be approved by the Head Master, Bursar or Deputy Head before the IT Network Manager reviews CCTV images.
25. The IT Network Manager maintains a log of all investigations.

SUBJECT ACCESS REQUESTS (SAR)

25. Individuals have the right to request access to CCTV footage that constitutes their personal data, unless an exemption applies the General Data Protection Regulations.
26. All requests should be made in writing to the Head Master. 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.
27. The College will respond to requests within one month of receiving the written request and any fee where disproportionate effort is required to adhere to the request.
28. Disclosure of information from surveillance systems must be controlled and consistent with the purpose(s) for which the system was established. When disclosing surveillance images of individuals, particularly when responding to subject access requests, the College will consider whether the identifying features of any of the other individuals in the image need to be obscured. In most cases the privacy intrusion to third party individuals will be minimal and obscuring images will not be required. However, consideration will be given to the nature and context of the footage
29. The subject will be supplied with a copy of the information in a permanent form. There are limited circumstances where this obligation does not apply. The first is where the data subject agrees to receive their information in another way, such as by viewing the footage.

 HOLYPORT COLLEGE	CCTV Policy	
	Effective Date: 09 Jan 2023	Version No: v1.3

The second is where the supply of a copy in a permanent form is not possible or would involve disproportionate effort, whereby the disproportionate effort may incur an administration fee.

30. Further guidance on SARs is within the Data Protection Policy.

ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES


31. 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 College where these would reasonably need access to the data (e.g. investigators).
32. Requests for images and data should be made in writing to the Head Master. Still images will be redacted in order to ensure compliance with the GDPR.
33. The data may be used within the College's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.
34. Data transfer will be made securely and using encryption as appropriate.

COMPLAINTS

35. Complaints and enquiries about the operation of CCTV within the College should be directed to the Head Master in the first instance.

FURTHER INFORMATION


www.ico.org.uk

 HOLYPORT COLLEGE	CCTV Policy	
	Effective Date: 09 Jan 2023	Version No: v1.3


APPENDIX A – CCTV CHECKLIST

This CCTV system and the images produced by it are controlled by the IT Network Manager who is responsible for how the system is used under direction from the College’s ‘Data Controller’. The College notifies the Information Commissioner about the CCTV system, including any modifications of use and/or its purpose. The College has considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of the College’s community. It will not be used for other purposes. The College will conduct regular reviews of our use of CCTV.

Checklist item	Checked (Date)	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.	Yes.	IT Network Manager	Jan 26
There is a named individual who is responsible for the operation of the system.	Yes.	IT Network Manager	Jan 26
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.	Yes.	IT Network Manager	Jan 26
Staff and members of the College community will be consulted about any proposal to install / amend CCTV equipment or its use as appropriate.	Yes.	IT Network Manager	Jan 26
Cameras have been sited so that they provide clear images.	Yes.	IT Network Manager	Jan 26
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.	Yes.	IT Network Manager	Jan 26
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	Yes.	Estates Manager	Jan 26
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	Yes.	IT Network Manager	Jan 26
The 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.	Yes.	IT Network Manager	Jan 26

 HOLYPORT COLLEGE	CCTV Policy	
	Effective Date: 09 Jan 2023	Version No: v1.3

Checklist item	Checked (Date)	By	Date of next review
Unless individually approved, images will not be provided to third parties.	Yes.	IT Network Manager	Jan 26
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the data controller knows to seek advice from Data Protection Officer.	Yes.	IT Network Manager	Jan 26
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	Yes. (Daily)	IT Network Manager	Daily

 HOLYPORT COLLEGE	CCTV Policy	
	Effective Date: 09 Jan 2023	Version No: v1.3

ANNEX B – CCTV SIGNAGE

It is a requirement of the General Data Protection Regulation to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The College is to ensure that this requirement is fulfilled.

The College's CCTV signage includes the following information:-

- That the area is covered by CCTV surveillance and images are recorded
- The purpose of using CCTV
- The name of The College
- The contact information for any enquiries



An example of a sign located at Holyport College.