Holyhead

Teach What Matters

CCTV Policy

Review Date:	**Spring 2021**
To Be Reviewed:	**Spring 2024**
Approved:	**Governors' Finance & General Purposes, Spring 2021**
Ratified	**Full Governors, Spring 2021**
Reviewer:	**S Laundon**

Holyhead
Teach What Matters

1. Policy Statement

This document provides a framework for the use of Closed-Circuit Television (CCTV) within Holyhead School. It demonstrates compliance with relevant acts of Parliament, codes of practice and other legal precedents to provide security for the safe operation and monitoring of CCTV.

2. Scope

2.1 Holyhead School has a comprehensive CCTV surveillance system on site for the purpose of the prevention and detection of crime, and the promotion of health and safety, which includes traffic management.

2.2 The system is owned by Holyhead School and controlled by authorised personnel. Images from the cameras are controlled and monitored at a Control Desk within the Facilities and IT Support Office.

2.3 This policy is applicable to all Holyhead School employees, governors, volunteers, contractors on site and visitors.

2.4 This policy has been prepared from the standards set out in the Information Commissioner's CCTV Code of Practice for the guidance of managers and the operators of the CCTV system and for the information of all members of Holyhead School community. (See Annex B). Its purpose is to ensure that the CCTV system is used to create a safer environment for staff, students and visitors to the School and to ensure that its operation is consistent with the obligations on the School imposed by the Data Protection Act 1998 and the new General Data Protection Regulation 2018 (GDPR). The policy is freely available for perusal and reviewed regularly.

2.5 Monitoring of the system will be permitted only to:

- Assist in the prevention and detection of crime
- Support the promotion of health and safety
- Facilitate the identification, apprehension and prosecution of offenders in relation to vandalism, crime and public order and as an aid to safety
- Assist with the management of internal traffic and car parking
- Assist in the detection of poor behaviour

2.6 The operation of the CCTV system will be in a manner consistent with due regard and respect for the privacy of individuals.

2.7 The Principal is responsible for ensuring compliance with this policy.

2.8 Breaches of the policy by staff monitoring the system may constitute matters of discipline under the relevant conditions of employment, but it is also recognised that other members of the School may have queries, concerns or complaints in respect of the operation of the system. Any concerns in

respect of the systems' use or regarding compliance with this policy should, in the first instance, be addressed to the Facilities Manager, who will follow the complaints procedure and any relevant policy guidelines and procedure.

3. Legislation

3.1 Secret surveillance could breach an employee's right to privacy under the Human Rights Act 1998 and could also breach the implied duty of mutual trust and confidence between employer and employee. It can only be justified in extreme situations (if an employee is suspected of stealing, for example) and must be both reasonable and proportionate to the circumstances. When installing CCTV, Holyhead School needs to comply with legal requirements under the Data Protection Act 1998 and GDPR 2018. These include notifying the Information Commissioner and having a clear policy in place to manage the data collected.

3.2 This CCTV policy demonstrates compliance with the Data Protection Act of 1998 and provides security for safe operation of monitoring of CCTV across site. (See Annex D).

3.3 Standards followed are set out in the Information Commissioner's CCTV Code of Practice. (See Annex B).

4. CCTV System

4.1 The autonomous system of CCTV surveillance applies to Holyhead School site. It will also encompass all other CCTV images that, in due course, are added to the system and monitored at the relevant Control Desk. References in this policy to the "CCTV system" or "the system" should be read and understood accordingly.

4.2 The system is operational in real-time and images are capable of being monitored for 24 hours-a day throughout the whole year. The system is also operational in non-real-time and images are capable of being stored for periods of time.

4.3 Holyhead School is the party responsible for processing images. The public is made aware of the presence of the system and its ownership by appropriate signage and the publication of this policy.

4.4 To ensure privacy, wherever practicable, the cameras are prevented from focusing or dwelling on domestic accommodation; and this will be demonstrated on request to affected local residents. Where neighbouring vicinities are affected (such as residential gardens) about those areas which are intended to be covered by the scheme the appropriate Facilities Manager will consult with the owners of the affected area to discuss what images may be recorded. Where it is not practicable to prevent the cameras from focusing or dwelling on such areas, appropriate training will be given to the system operators to ensure that they are made aware that they should not be monitoring such areas. Similarly, those domestic areas adjacent to the areas which are intended to be covered will be given due consideration.

4.5 Images captured on camera will be transmitted to the Control Desk in the appropriate secure office (e.g. Principal, Vice Principal, Facilities, Administrative or Technical (IT) Support Office) where they will be recorded for use in accordance with this policy. Although every effort has been made in

the planning and design of the CCTV system to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

4.6 For the purposes of the Data Protection Act 1998 and GDPR 2018, the Data Controller is Holyhead School; and legally responsible for the management and maintenance of the CCTV system. (See Annex C)

5. CCTV Control Desk

5.1 Images captured by the system will be monitored at the Control Desk by the Facilities, Administration or Technical (CCTV) Controller. The CCTV Controller is to work in a secure room where the monitor on the Control Desk must not be observable from outside the room, having regard to the purposes set out above.

5.2 No unauthorised access to the system at the Control Desk is allowed at any time. Normal access is strictly limited to the CCTV Controller, authorised staff members and the Principal. Police Officers (and other law-enforcement personnel and legal agencies) may enter with the explicit consent of the Principal.

5.3 Persons other than those specified may be authorised to access the CCTV monitor on the Control Desk on a case-by-case basis. Written authorisation is required by the Principal. Each separate visit will require individual authorisation and will be supervised at all times by the CCTV Controller, Principal or Vice Principal. Visitors will not be given access to any data which falls within the scope of the Data Protection Act. (See Annex D).

5.4 In an emergency, and where it is not reasonably practicable to secure prior authorisation, access may be granted verbally to persons with a legitimate reason to access the CCTV monitor by the CCTV Controller.

5.5 Before granting access to the CCTV monitor on the Control Desk, the CCTV Controller(s) must satisfy themselves of the identity of any visitor, and ensure that the visitor has the appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include their name, department or the organisation they represent, the person who granted authorisation for their visit and the times of their entry to, and exit from, the CCTV monitor on the Control Desk. A similar record shall be kept of the CCTV Controller on duty at the Control Desk at any given time.

5.6 An incident log will be maintained at the Control Desk and details of incidents will be noted, together with any consequential action taken (see Annex G).

5.7 It is recognised that the images obtained comprise personal data and are subject to the law on Data Protection. All copies will be handled in accordance with the summary procedures outlined in Annexes A-F of this policy and are designed to ensure the integrity of the system. The site Facilities

Manager will be responsible for the development of, and compliance with, the working procedures at the Control Desk.

5.8 Recorded images will only be reviewed with the authority of the Principal and the Vice Principals. Copies of digital images may be made for the purpose of crime detection, evidence in relation to

all matters affecting safety, evidence for the purpose of traffic management or where otherwise required by law. CCTV images may be used as evidence dependent on the circumstances.

6. CCTV Staff

6.1 All staff involved in the operation of the CCTV system will, by training and access to this policy, be made aware of the sensitivity of handling CCTV images and recordings.

6.2 The Facilities Manager will ensure that all staff, including relief staff, are fully briefed in respect of all functions, operational and administrative, arising within the CCTV control operation.

6.3 Current staff permitted to view the CCTV are the following:

- Principal
- Vice Principal
- I.T Manager
- I.T Support
- Facility Manager

7. CCTV Recording

7.1 The CCTV Control Desk system is supported by digital recording facilities which will function throughout operations in real time. Each disk will be uniquely identified and all activities relating to each disk. E.g. date and hours of recording, viewing for specific purpose, copies taken, disks retained for evidence, disks erased and reused, etc., will be recorded in the Log book. As the images are recorded digitally, the process of identifying retrieval dates and times will be computerised. Images will be cleared automatically after a set time.

7.2 Unless required for evidential purposes or the investigation of crime, recorded images will be retained for no longer than 14 days from the date of recording. However, the School recognises that, in accordance with the requirements of the Data Protection Act, no images should be retained for longer than is necessary. Accordingly, some recorded images may be erased after a shorter period (for example where it can be determined more quickly that there has been no incident giving rise to the need to retain the recorded images). Digital images will be automatically erased after a set period.

7.3 In the event of the digitally recorded image being required for evidence, or the investigation of crime, it will be retained for a period of time until it is no longer required for evidential purposes or

any investigation into an allegation, offence or crime (this list is not exhaustive)has been completed. External agencies (such as the police) may keep a copy as required for their investigations, which falls outside the scope of this policy.

8. CCTV Monitoring

8.1 CCTV Controllers, who will be members of the School support and administration staff, will be available to work at the Control Desk as and when directed to do so through their Line Manager.

8.2 The control of the system will always remain with Holyhead School but, at the Principal's discretion, the cameras may be operated in accordance with requests made by the police during an incident for the purposes of:

- Monitoring potential public disorder or other major security situation
- Assisting in the detection of crime
- Facilitating the apprehension and prosecution of offenders in relation to crime and public order

8.3 On each occasion that the police obtain assistance with their operations, a report setting out the time, date and detail of the incident shall be submitted to the Principal.

9. Toilets

Any desire to install CCTV cameras in Holyhead School must be a Principal and Governors decision. Such a decision will be based on vandalism; bullying or any other harm caused i.e. poor behaviour. Such cameras will only be in the wash room area and not in the cubicles or facing the urinals directly.

10. Control and Management of Digital Recordings

All CCTV media disks belong to, and remain the property of, Holyhead School. Disk handling procedures (i.e. CD, DVD or otherwise) are in place to ensure the integrity of the image information held.

11. Access to recordings

Requests by persons outside of Holyhead School for viewing or copying of disks or obtaining digital recordings will be assessed on a case by case basis. Requests from the police or other authorised bodies may arise in a number of ways, including:

- Immediate action relating to live incidents, e.g. actual pursuit of culprit
- For incidents that occurred when images may have been recorded continuously
- Individual police officers seeking to review recorded images on the monitor of the Control Desk itself
- Requests for a review of possible recordings in order to trace incidents that have been reported as crimes

11.1 Requests for access to recorded images from persons other than the police or the data subject (that is, the person whose image has been captured by the CCTV system) will be considered on a case by case basis. The Principal shall consider such requests if a minimum of 48 hours' notice is given. Access to recorded images in these circumstances will only be granted where it is consistent

with the obligations placed on the School by the Data Protection Act 1998 (DPA) and, in particular, with the purposes set out in Section 1 of the DPA. (See Annex D).

12. Standards

It is important that access to, and disclosure of, the images recorded by CCTV 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. Users of CCTV will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images. These aspects of the policy reflect the Second and Seventh Data Protection Principles of the Data Protection Act 1998 (at Annex D).

12.1 All CCTV Controllers and associated Control Desk staff should be aware of the restrictions set out in this policy in relation to access to, and disclosure of, recorded images. Access to recorded images will be restricted to staff who need to have access in order to achieve the purposes of using the equipment. **Being inquisitive is not a reason to view live or recorded CCTV images**.

12.2 All access to the disks on which the images are recorded will be documented. Disclosure of the recorded images to third parties will be made only in the following limited and prescribed circumstances and to the extent required or permitted by law:

· Law enforcement agencies where the images recorded would assist in a specific criminal inquiry
· Prosecution agencies
· Other relevant legal representatives
· People whose images have been recorded and retained and disclosure is required by virtue of the Data Protection Act 1998

12.3 All requests for access or disclosure will be recorded. The Principal shall make decisions on access to recorded images by persons other than police officers. Requests by the police for access to images will not normally be denied, provided they are accompanied by a written request signed by a Police Officer who must indicate that the images are required for the purposes of a specific crime enquiry. This must be signed off by the Principal.

12.4 Where it is essential to remove any connected equipment from the site, any images of students or information that is covered by the Data Protection Act 1988 & GDPR should be transferred to an

appropriate backup system held in the School. Upon return of the equipment to site, the information should be reloaded and deleted from the temporary backup system.

12.5 Where third parties are required to access the system, the Facility Manager should be present. However, if third parties require information under the Data Protection Act 1988 section 35(2), for the purposes of obtaining legal advice, or it is deemed and necessary for the purposes of establishing, exercising or defending legal rights, this request should be made in writing to the Principal. If further access is required for repair, maintenance or for another purpose and considered

by the Principal to be essential, where possible images should be removed. Where a request has been made, the Principal should specify, in writing, who may gain access and for what purpose such access is granted setting out limitations of dates and times. The acceptance of such limitations should be signed by a person in authority at the receiving company

12.6 If access or disclosure is denied by the Principal, the reasons will be documented and forwarded to the Control Desk for action and filing. CCTV Controllers using the appropriate forms will document routine disclosure to the Police. Requests for non-Police disclosures will be forwarded to the Principal for due consideration. If access to, or disclosure of the images is allowed, then the following will be documented:

· Date when access was allowed
· Date and time on which disclosure was made
· Reason for allowing access or disclosure
· Extent of the information to which access was allowed or disclosed

13. Access by Data Subjects

All staff involved in monitoring or handling image data will proceed in accordance with the following protocol in respect of data subject access requests.

13.1 Data subjects will be provided with a standard Subject Access Request Form which requires individuals to provide:

· Dates and times when they visited the School
· Where exactly they visited, and who acted as escort
· Provision of two separate photographs of themselves, one full-face and one side-view, with the completed form
· Proof of identity (e.g. a utility bill, a driving licence or a passport)
· Statutory payment required in respect of access right request (i.e. A cheque or cash to the sum of £12.00 for which a receipt will be issued at the time of the issue of the form)

13.2 The data subject will be asked whether they would be satisfied with a view the images recorded. Recorded images on CD, DVD (or similar) disks will incur additional costs for media. Transfer onto portable drives is prohibited (e.g. USB memory sticks).

13.3 A written decision on their request will be sent to the data subject within 28 days. If access to the images is to be provided, such access will be provided within 30 days of the School receiving the request or, if later, the date when the School receives the identification evidence from the data subject. A list of typical circumstances when requests may be refused is given below.

14. Rights of Data Subjects

The procedure outlined above and the use of the subject access request form complies with Section 7 of the Data Protection Act 1998, enabling the Principal to inform individuals as to whether or not images have been processed by the CCTV system. Holyhead School is not obliged to comply with a request under this section unless it is supplied with such information as it may reasonably require in order to satisfy itself as to the identity of the person making the request, and to locate the specific information which that person seeks. (See Annexes D-F).

14.1 Where the School cannot comply with the request without disclosing information relating to another individual who can be identified (from that same information) it is not obliged to comply with the request, unless:

· The other individual has consented to the disclosure of the information to the person making the request, or

· It is reasonable in all the circumstances to comply with the request without the actual consent of the other individual(s)

15. Tracking of Computer Disks, Still Photographs and Printed Images

15.1 In the pursuance of continuity of evidence, photographs and hard-copy prints taken from digital images are subject to the same controls and principles of Data Protection as other data collected at the Control Desk. They will be treated using the same summary procedures (contained within Annex D of this policy) as digital images.

15.2 At the end of their useful life all computer disks, still photographs and hard-copy prints will be disposed of as confidential waste. Such erasure and disposal will be appropriately logged following the procedures contained within Annex B.

16. Evaluation and Review

16.1 This policy will be evaluated at irregular intervals and reviewed at least once every two years to assess its implementation and effectiveness. The policy will be promoted and implemented throughout the School.

16.2 Anything not covered specifically in this policy will be dealt with in accordance with associated rules and/or whatsoever is in the best interests of Holyhead School.

ANNEXES:

A - CCTV Operation, Set-up & Audit Checklist

B – Commissioner's Code of Practice

C - Data Controller and Data Protection Officer

D - Data Protection Principles

E - Freedom of Information Principles

F - Protection of Freedoms' Principles

G – Log Sheet

H – Subject Access Request Form

ANNEX A

CCTV OPERATION, SET-UP & AUDIT CHECKLIST

CCTV Audit Checklist	
Initial set up of CCTV or periodic audit	
Date of Initial set up (If known) & Location	
Date of last audit	
Date of this audit	

Owner of CCTV	
Name	
Address	
Telephone No	

	YES	NO
Are signs in place informing visitors of CCTV		
Are cameras prevented from surveying private residents		
Do cameras survey areas open to the public		
Is the CCTV control room secure		
Is there more than one CCTV monitor location		
Are the monitors secure? Location of monitors:		
Is the CCTV monitor out of view of windows		
Are recordings being handled in accordance with the policy		
Have all out of date recordings been securely disposed of		
Is the log book kept up to date		

Declaration	
Audit conducted by:	
Signed:	
Date:	

ANNEX B

CCTV code of practice

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 use 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.

ANNEX C

Data Controller and Data Protection Officer

1. The Data Controller is the person or organisation who holds personal data. They determine the manner in which any Personal Data is processed. They are responsible for establishing practises and policies to ensure compliance with the applicable law.

2. Holyhead School is the Data Controller.

3. All schools should appoint a Data Protection Officer to be responsible for data protection matters.

4. In Holyhead School it is the I.T Manager .

5. Other educational bodies such as the Department for Education hold information about individuals for specific functions and they each have a Data Protection Officer.

6. As they deal with personal information, Holyhead School must notify the Information Commissioner's Office that they are data controllers under the Data Protection Act 1998.

ANNEX D

Data Protection Principles

The data controller must ensure that processing complies with the eight data protection principles, as follows.

1. Personal data must be processed fairly and lawfully. This means: the individual has given consent the processing is necessary for a contract that involves the individual, or the processing is necessary to comply with a legal obligation, to protect the vital interest of the individual, for legal/justice reasons, or for the purposes of the organisation's legitimate interests.

2. Personal data must only be obtained and processed for specified, lawful purposes.

3. Personal data must be adequate, relevant and not excessive in relation to the specified purpose.

4. Personal data must be accurate and kept up to date.

5. Personal data must not be kept for longer than is necessary.

6. Personal data must only be processed in accordance with the individual's legal rights.

7. Appropriate technical and organisational measures must be taken to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage.

8. Personal data must not be transferred outside the EU unless an adequate level of protection for the rights and freedom of the individual is ensured.

ANNEX E

Freedom of Information Principles

1. The Freedom of Information Act 2000 gives individuals the statutory right to access information held by public authorities.

2. This includes government departments, maintained schools and academies.

[Note: Data protection legislation applies to all bodies and organisations which hold personal data about individuals. The Freedom of Information Act 2000 applies to the public sector only and it covers access to information, but this is not restricted to information about individuals. Schools are, therefore, covered by both and may receive a request for information under either. Schools can cover compliance with both sets of legislation in one policy, but they will need separate procedures for data protection and freedom of information requests. In both cases, there are time limits for dealing with a request and a fee can be charged. Also in both cases, if the information released includes personal information about another person it may be possible to release the information by blanking out the relevant personal information.]

ANNEX F

Protection of Freedoms' Principles

The Protection of Freedoms' Act 2012 introduced:

1. Increased restrictions around the retention of DNA and fingerprints

2. The requirement for schools and colleges to obtain the consent of parents before taking fingerprints

3. Further regulation over the use of CCTV and automatic number plate recognition

4. Reform of the Vetting and Barring Scheme and DBS regime

5. Extended freedom of information to cover companies wholly owned by two or more public authorities

6. An obligation for public authorities to release datasets in a re-usable format.

[Note: The Protection of Freedoms' Bill (received Royal Assent in April 2012) provides for a new statutory CCTV Code of Practice.]

ANNEX G

Holyhead School CCTV Log Sheet

Sheet No: _______

Line No:	Date	Time	Operator	Viewing requested by	Reason viewing is required	Camera No	Action Taken	Initials

ANNEX H

Subject Access Request Form

Part A

Title	
Full Name	
Date of Birth	
Address	
Year Group (If student)	

Part B

Title	
Full Name	
Address	
Phone Number	
Email	
Identification; Passport, Driving license	
Status of Requester i.e. parent, guardian	

If you are a parent, we expect to be provided with proof of parental responsibility before releasing personal data of your child

Part C

Details – including dates, times, where visited and with whom.	

Part D Declaration

I hereby request that Holyhead School provide me with the information about the data subject above. I understand that I must provide proof to the school; verifying that I have a legal right to access the personal data requested.

Name: ……. Date: ……

Signed: .....