Ysgol Bryn Castell

CCTV POLICY

Date: December 2025
Review Date: December 2028
Based on WG Model Policy

Next review due: December 2028 (or when a legal change / update is required)

CCTV Policy

The school recognises that Closed Circuit Television (CCTV) systems can be privacy intrusive.

For this reason, the school has carried out a Data Protection Impact Assessment (DPIA) 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 DPIA 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 three years.

Objectives

The purpose of this policy is to regulate the management, operation and use of the CCTV system at the school.

The school's CCTV system is intended to assist the school in reaching these objectives:

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

Purpose of This Policy

The purpose of this policy is to regulate the management, operation and use of the CCTV system at the school. The CCTV system used by the school comprises of:

Floor	Location	Internal/ External
YBC	KS4 Corridor leading from Coffee Shop	Internal
YBC	KS4 Corridor Music room	Internal
YBC	KS4 Corridor Lift area	Internal
YBC	KS4 Corridor Leading to main doors to yard	Internal
YBC	KS4 Main doors to yard	External
YBC	KS4 Main doors	External
YBC	KS4 CAD Room Fire Doors	Internal
YBC	KS4 CAD Room Fire Doors	External

Floor	Location	Internal/ External
YBC	KS4 D&T Room Fire Doors	Internal
YBC	KS4 Art / Common Room Fire Doors	Internal
YBC	KS4 Coffee shop seating area Fire Doors	Internal
YBC	KS4 Coffee shop Kitchen Fire Doors	Internal
YBC	KS4 Science Prep room Fire Doors	Internal
YBC	KS4 Laundry room Fire Doors	Internal
YBC	KS4 Rear Car Park/ Construction area	External
YBC	KS4 Rear walkway to school Rt.	External
YBC	KS4 Rear walkway to school Left.	External
YBC	KS3 Corridor from KS4 area	Internal
YBC	KS3 Corridor outside shared area	Internal
YBC	KS3 Library area	Internal
YBC	KS3 Corridor outside Heads Office	Internal
YBC	KS3 Corridor Leading to stairs	Internal
YBC	Post 16 corridor leading to fire exit stairs	Internal
YBC	ASD Corridor leading to KS3	Internal
YBC	ASD classroom Fire Exit	Internal
YBC	ASD classroom Fire Exit	External
YBC	ASD main corridor Fire Exit	Internal
YBC	ASD main corridor Fire Exit leading to tower	External
YBC	KS3 ground floor stairs to fire door	Internal
YBC	KS3 ground floor entrance leading from Reception	Internal
YBC	KS2 Entrance by Office	Internal
YBC	KS2 fire door exit	Internal
YBC	KS2 Main Corridor	Internal
YBC	Main reception desk	Internal
YBC	Main entrance to external main door	Internal
YBC	Main entrance to KS3 stairs	Internal
YBC	Main entrance to KS2 doors	Internal
YBC	KS3 main entrance to KS2 Fire Exit	External
YBC	KS3 Main entrance to front of school	External
YBC	Main entrance to hall stairs	Internal
YBC	Main hall stairs to entrance to reception	Internal
The Bridge	Corridor leading from TBAP to main hall	Internal
The Bridge	Main Corridor leading to yard exit	Internal
The Bridge	Main Corridor yard exit	External
The Bridge	Main Corridor to internal fire doors – post 16	Internal
The Bridge	Vulnerable groups main entrance leading to main corridor	Internal
The Bridge	TBAP main entrance Courtyard area	Internal
The Bridge	TBAP main entrance Courtyard area	External
The Bridge	Vulnerable groups Fire Exit leading to main Courtyard	Internal
The Bridge	Vulnerable groups Fire Exit leading to main Courtyard	External
The Bridge	Vulnerable groups Fire Exit leading to Playground	Internal

Floor	Location	Internal/ External
The Bridge	Vulnerable groups Fire Exit leading from Playground	External
The Bridge	Playground area, looking at Lift	External
The Bridge	Playground area, looking at Lift	Internal
Sports Hall	Sports Hall to Main Entrance	External
Sports Hall	Rear Sports hall to allotment area	External
Sports Hall	Sports Hall to outdoor shelter	External
Sports Hall	Sports Hall to Boiler House	External
Sports Hall	Sports Hall to Car Park	External
Sports Hall	Main entrance from Canteen	External
Main Hall	Main Hall to double fire doors	Internal
Main Hall	Main Hall double fire doors to sports hall	External
Main Hall	Main Hall to Single fire door	Internal
Main Hall	Main Hall Single fire door	External
Tower 1	Main car park	External
Tower 2	Main car park entrance	External

Statement of Intent

CCTV cameras are installed in such a way that they are not hidden from view. We do not covertly record anyone. Signs are predominantly displayed where relevant so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

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.

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

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

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

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 have 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.

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.

CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 30 days.

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 6 months.

System Management

Access to the CCTV system and data shall be password protected and will be kept in a secure area.

The CCTV system will be administered and managed by an appropriate, designated member of staff 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 headteacher

The system and the data collected will only be available to the System Manager, his/her replacement, appropriate members of the Senior Management team, Learning Recovery Manager team and other staff as determined by the headteacher.

The CCTV system is designed to be in operation continuously throughout the year, though the school does not guarantee that it will be working during these hours.

The System Manager will ensure that the equipment is properly recording and that cameras are functional, via a maintenance agreement with the Local Authority.

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.

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 above requests access to the CCTV data or system, the System Manager must satisfy him/herself 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 logbook including time/data of access and details of images viewed and the purpose for so doing.

Only authorised staff are able to view the CCTV cameras, a signed CCTV Confidentiality Agreement is required prior to access

Downloading Captured Data on to Other Media

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

(a) Each downloaded media must be identified by a unique mark.
(b) Before use, each downloaded media must be cleaned of any previous recording.
(c) The System Manager will upload any CCTV footage recorded on to the CCTV team. Access to this team is restricted to the headteacher and the System Manager. The footage is saved in a separate folder stating the date and or location of the incident
(d) Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a secure place. Footage requested by the police should be securely transferred by a secure link sent to the System Manager or the headteacher. Information of the transferred data is noted and filed.
(e) If downloaded media is archived, the reference must be noted.

Images may be viewed by the police for the prevention and detection of crime and by the System Manager, his/her replacement and the headteacher and other authorised senior managers. 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.

A record will be maintained of the viewing or release of any downloaded 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 downloaded media (and any images contained thereon) remains the property of the school and downloaded 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.

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 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 manager of the school in consultation with the school's Data Protection Officer.

Requests for Access by 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 access data held about themselves, including those obtained by CCTV. Requests for such data should be made to the headteacher.

Please refer to our Data Protection Policy and Subject Access Request (SARs) for further details.

If we cannot comply with the request, the reasons for not being able to comply will be documented and the data subject will be advised of these in writing.

The assigned manager responsible for the CCTV system will liaise with the Data Protection Officer, Judicium Consulting, and the school's Designated Safeguarding Lead to determine whether disclosure of the images will reveal third-party information, to assess the risks involved with disclosure and the reasonableness in disclosure.

Particular care should be exercised when images of other people are included in the materials for disclosure. Images of other individuals will, if possible, be redacted unless there would be an expectation that their images would be released in such circumstances. Non-disclosure will be appropriate in most circumstances. If there is any doubt about what information must be provided to enquirers, please contact the school's Data Protection Officer, Judicium Consulting.

Complaints

Complaints and enquiries about the operation of our CCTV systems should be made by staff in line with our Resolution Policy which is available on the staff intranet or by parents/carers, pupils and visitors, under our complaints procedure, available on the school website: Ysgol Bryn Castell - Policies .

If a member of staff believes that there has been a breach of the Data Protection Act, or any other legal obligations, they should contact the headteacher as a matter of urgency in accordance with the data breach reporting process set out in our Data Breach Policy.

Public Information

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