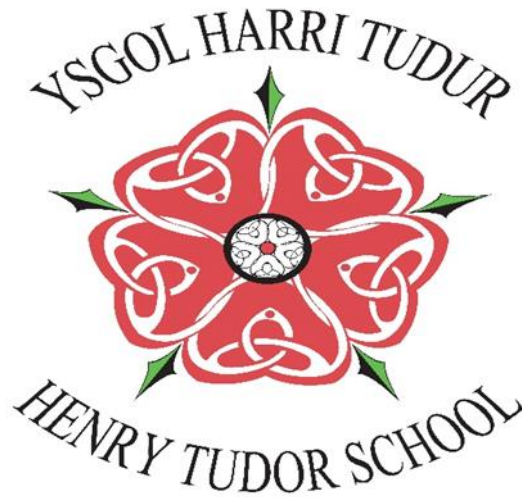


Ysgol Harri Tudur



Henry Tudor School

CCTV Policy

Spring 2019: Observation - The Governors Resources committee delegated oversight for the distribution of CCTVs throughout Ysgol Harri Tudur / Henry Tudor School to the School Business Manager

Adopted by Resources Committee:
Last Reviewed: Autumn 2020
Review annually
Next Review: Autumn 2021

POLICY FOR THE USE OF C.C.T.V. SYSTEMS AT YSGOL HARRI TUDUR / HENRY TUDOR SCHOOL

This Code of Practice is issued by the Ysgol Harri Tudur/Henry Tudor School (YHT) Governing Body. It is intended to provide guidance as to good practice for users of the CCTV (closed circuit television) systems at YHT.

This code is based upon the Code of Practice published by the Information Commissioner, which sets out the standards and requirements of the Data Protection 1998 Act and the General Data Protection Regulation (GDPR) 2018 to be met. In particular data should be:

- ❖ *Fairly and lawfully processed;*
- ❖ *Processed for limited purposes and not in any manner incompatible with those purposes;*
- ❖ *Adequate relevant and not excessive;*
- ❖ *Accurate;*
- ❖ *Not kept for longer than is necessary;*
- ❖ *Processed in accordance with individuals' rights;*
- ❖ *Secure;*
- ❖ *Not transferred to countries without adequate protection.*

The Governor nominated for Data Protection will have oversight of the operation of this aspect of the policy.

YSGOL HARRI TUDUR/HENTRY TUDOR SCHOOL

PROCEDURES

CCTV SYSTEMS

1. Owner Operator Data and Controller of the Scheme – F. Kite, Headteacher, Ysgol Harri Tudor/Henry Tudor School (YHT), Pembroke SA71 4RL.
2. YHT considers that the CCTV Scheme can contribute to security and the health and safety of pupils, staff and visitors.
3. The purposes of the CCTV Scheme in YHT are to provide monitoring systems to assist with the protection of the public property, law enforcement, traffic management, community safety, the reduction of crime and disorder and support safeguarding.
4. The general management of CCTV in YHT is provided by the School Business Manager (SBM).
5. The day to day management of the CCTV system is the responsibility of the School Facilities Manager (SFM).

Siting of Cameras

The Governing Body Resources Committee in conjunction with the Local Authority and YHT building design authority has considered the proper location of CCTV cameras, where they exist, in and around YHT. The recording of sound may be provided in the future.

Standards

1. All CCTV equipment installed in YHT will only be sited in such a way that it only monitors those spaces that are intended to be covered by the equipment.
2. If domestic areas such as gardens or areas not intended to be covered by the scheme border those spaces which are intended to be covered by the equipment, then the users should consult with the owners of such spaces if images from those spaces might be recorded. In the case of back gardens, this would be the resident of the property overlooked.
3. The employees and pupils will be made aware of the purpose (s) for which the scheme has been established and notices to this effect will be displayed in the school reception area and the school hall foyer. Parents will be informed through the school prospectus.
4. The operators will only use the equipment in order to achieve the purpose(s) for which it has been installed.
5. Cameras that are adjustable by the operators will not be adjusted or manipulated by them to overlook spaces which are not intended to be covered by the scheme, other than as described in 6 below.
6. If it is not possible physically to restrict the equipment to avoid recordings from those spaces not intended to be covered by the scheme, then operators will be trained in recognising the privacy implications of such spaces being covered.

7. Signs, of no less than the minimum standard, will be placed so that the public are aware that they are entering a zone that is covered by CCTV.
8. The signs should be clearly visible and legible to members of the public.
9. The size of signs will vary according to circumstances.
10. The signs should contain the following information:
 - a. *Identity of the person or organisation responsible for the scheme;*
 - b. *The purposes of the scheme;*
 - c. *Details of whom to contact regarding the scheme;*
 - d. *Any other information that may become a statutory requirement.*

Quality of Images

Standards

1. Upon installation an initial check will be undertaken to ensure that the equipment performs properly. Regular checks will be made thereafter to ensure that the system is operating properly.
2. Images are retained on a hard disc drive for a period of 31 days. Copies can be made for investigation purposes.
3. Checks will be made to ensure the accuracy of any features such as the location of the camera and/or date and time reference. Where the time/date etc are found to be out of sync with the current time/date, the operators will take such remedial action as is continued in the operations manual to correct the error. A note of such changes will be recorded in the daily occurrence log.
4. Cameras will only be situated so that they will capture images relevant to the purpose for which the scheme has been established.
5. When installing cameras, consideration must be given to the physical conditions in which the cameras are located.
6. Cameras are to be properly maintained and serviced to ensure that clear images are recorded. Servicing will be carried out at least annually.
7. Cameras should be protected from vandalism in order to ensure that they remain in working order.
8. A maintenance log will be kept in the monitoring centre of the system concerned.
9. The SFM is responsible for ensuring that damaged equipment is repaired within a specified time frame and monitors the quality of the work.

Recording Process

Standards

1. Images or sound should not be retained for longer than is necessary and unless required for specific investigation or evidential purposes, deleted after 31 days have passed.
2. Once the retention period has expired, the recordings should be removed or erased.
3. Recordings that are to be retained for evidential purposes will be retained in a secure place to which access is controlled.
4. Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed or be capable of being viewed by anyone other than authorised persons.
5. Access to the recordings should be restricted to a manager or designated member of staff who will decide whether to allow requests for access.
6. Viewing of the recordings should take place in a restricted area, for example, in a manager's or designated member of staff's office. Other employees should not be allowed to have access to that area when a viewing is taking place.
7. Removal of the medium on which recordings are recorded, for viewing purposes, should be documented as follows: (Appendix A)
 - a. *The date and time of removal;*
 - b. *The name of the person removing the recordings;*
 - c. *The name(s) of the person(s) viewing the recordings;*
 - d. *The reason for the viewing;*
 - e. *The outcome, if any, of the viewing;*
 - f. *The date and time the recordings were returned to the system or secure place, if they have been retained for evidential purposes.*
8. All operators and employees with access to recordings should be aware of the procedure that needs to be followed when accessing the recorded recordings.
9. All operators should be trained in their responsibilities under the Code of Practice, i.e. they should be aware of:
 - a. *The user's security policy e.g. procedures to have access to recorded recordings;*
 - b. *The user's disclosure policy.*

Access to and disclosure of recordings to third parties

Standards

All employees should be aware of the restrictions set out in this code or practice in relation to access to, and disclosure of, recordings.

1. Access to recorded recordings will be restricted to those persons who need to have access in order to achieve the purpose(s) of using the equipment.
2. All access to the medium on which the recordings are recorded should be documented.
3. Disclosure of the recordings to third parties should only be made in limited and prescribed circumstances. Subject to paragraph 1 above, in disclosure will be limited to the following classes of persons/agencies.
 - *Law enforcement agencies, where the images recorded would assist in a specific enquiry;*
 - *Highways authorities in respect of traffic management matters;*
 - *Law enforcement agencies where the recordings would assist a specific criminal enquiry;*
 - *Prosecution Agencies;*
 - *Relevant legal representatives*
4. All requests for access or for disclosure should be recorded, if access or disclosure is denied, the reason should be documented,
5. If access to or disclosure of the recordings is allowed, then the following will be documented. (Appendix B)
 - *The date and time at which access was allowed or the date on which disclosure was made;*
 - *The identification of any third party who was allowed access or to whom disclosure was made;*
 - *The reason for allowing access or disclosure;*
 - *Location of the recordings*
 - *Any crime incident number to which recordings may be relevant*
 - *Signature of person authorised to collect the medium – where appropriate.*
6. Recordings will not be made more widely available – for example they should not be routinely made available to the media or placed on the Internet.
7. If it is intended that recordings will be made more widely available, that decision should be made by the Headteacher or designated member of staff and the reason for that decision should be documented.
8. If it is decided that recordings will be disclosed to the media (other than in the circumstances outlined above), the images of individuals will need to be disguised or blurred so that they are not readily identifiable.

Storage of CCTV Images

It may be necessary to save CCTV images for transfer to investigating agencies such as police and social services. Images should only be transferred to the secure hard drive that is kept in the school safe. One of the authorised users (i.e. one of the staff who have the system password) must be present at the time of the viewing and transfer to disc.

Access by data subjects

Standards

1. In accordance with Section 7 of the Data Protection Act 1998 (Subject Access) and subsequent GDPR 2018 regulations, an individual who believes that their image has been captured by this scheme is entitled to make a written request to the Data Controller. Upon payment of the current fee*, and the supply of essential information, a systems search will be conducted and subject to certain conditions, the individual will be allowed access to the personal data held (current fee is £10.00).
2. All subject access requests should be referred in the first instance to the Headteacher who will liaise with the SBM and SFM.
3. All staff involved in operating the equipment must be able to recognise a request for access to recordings by data subjects and how such requests are to be dealt with.
4. Data subjects should be provided with a standard subject access request form, a copy of this form is attached at Appendix C, which:
 - a. *Indicates the information required in order to locate the recordings requested;*
 - b. *Indicates the information required in order to identify the person making the request;*
 - c. *Indicates the fee that will be charged for carrying out the search for the recordings requested.*

NB. The above form will also enquire whether the individual would be satisfied with merely viewing the recordings. The form will also indicate that the response will be provided promptly and in any event within 40 days of receiving.

5. Individuals, at the time of any subject access request, will be given a description of the type of recordings and retained and the purpose for which the recording and retention takes place.
6. Prior to any authorised disclosure, the Headteacher will need to determine whether the recordings of another “third party” individual features in the personal data being applied for and whether these third party recordings are held under a duty of confidence,
7. If third party recordings are not to be disclosed the SBM shall arrange for the third party recordings to be disguised or blurred,
8. If the Headteacher decides that a subject access request from an individual is not to be complied with, the following should be documented:
 - a. *The identity of the individual making the request;*
 - b. *The date of the request;*
 - c. *The reason for refusing to supply the recordings requested;*

d. *The name and signature of the person making the decision.*

Other rights

Under the DPA/GDPR individuals also have the following rights which may be applicable to CCTV schemes:

- *Right to prevent processing likely to cause damage or distress;*
- *Rights in relation to automated decision taking;*
- *Right to seek compensation for failure to comply with certain requirements.*

Where a request is made in relation to other rights, these shall be referred to the Headteacher who will document the request and respond to it.

Viewing Log

The viewing log for the CCTV system is to be a bound and numbered book. All viewings must be recorded.

Monitoring compliance with this code of practice

Standards

1. The contact point indicated on the sign should be available to members of the public during normal office hours. Employees staffing that contact point should be aware of the policies and procedures governing the use of this equipment.
2. Enquirers should be provided on request with one or more of the following:
 - a. *A copy of this code of practice;*
 - b. *A subject access request form if required or requested; Appendix C*
 - c. *The Complaints Procedure to be following if they have concerns about the use of the system.*
3. The SBM should undertake regular reviews of the documented procedures to ensure that the provisions of the Code are being complied with.
4. An internal annual assessment should be undertaken which evaluates the effectiveness of the system.
5. De-personalised details of complaints will be maintained and will be included in an annual report on each CCTV system.
6. A copy of the Complaints Procedure will be made available upon request from the SBM.

Use of mobile phones and cameras to record incidents

Further to Local Authority safeguarding instructions, staff with personal recording devices must not use them for this purpose. This applies to both personal and school-owned devices.

Staff must not take any photo on a personal phone, school phone or school camera of any injury sustained by a pupil or a member of staff.

C.C.T.V. - YHT

RECORDING OF VIEWING BY AUTHORISED SCHOOL STAFF

Date and Time Image Viewed:

Date: Time:

Name of Persons Viewing the Recording:

Name

Designation

.....
.....
.....
.....

Reason for the viewing:

.....
.....
.....

Outcome, if any, of the viewing:

.....
.....
.....
.....

C.C.T.V. - YHT

RECORDING OF VIEWING BY THIRD PARTY (e.g. Police)

Date and Time Access Allowed:

Date: Time:

Identification of any third party who was allowed access:

.....
.....

Names of school staff present:

.....
.....

Reason for allowing access:

.....
.....
.....

Crime incident number if applicable:

.....

Location of the recording:

.....

Signature of the person authorised to collect the medium - where appropriate:

.....

Date and time copy created for evidential purposes:

Date: Time:

C.C.T.V. - YHT

FORM TO REQUEST ACCESS TO CCTV RECORDINGS - FEE £10.00

NAME:

ADDRESS:
.....
.....
.....

DATE OF BIRTH:

TELEPHONE NUMBER:

Date image recorded:

Time image recorded:

Location:

To carry out a search for the recordings, a fee of £10.00 will be charged.

Please complete the above form and attach a £10.00 cheque made payable to Ysgol Harri Tudor/Henry Tudor School.

The Headteacher will consider the request and respond within 28 days.