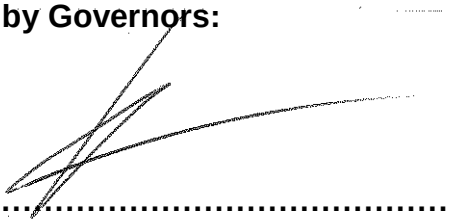
CCTV POLICY

Agreed by Governors:



……

(Signed by Chair)

June 2019

Scheme due for review

June 2020

If you would like a copy of this document in an alternative format or your own language, please contact:

Argoed High School

Tel: 01352 756414

Email: contact@argoedhs.co.uk

CCTV Policy

Review date: June 2020

Full Governing Body,

Argoed is a happy, caring school where high standards are expected at all times. We believe that school should be a place where children enjoy their education; where there is an atmosphere of happiness, security and confidence; where they are educated and where they are relaxed and confident in their relationships.

Data Protection

- Any personal data processed in the delivery of this policy will be processed in accordance with the school Data Protection policy.

1. Policy Statement

1.1 Argoed High School uses Close Circuit Television (CCTV) within the premises of the School. The purpose of this policy is to set out the position of the School as to the management, operation and use of the CCTV at the School.

1.2 This policy applies to all members of our staff, visitors to the School premises and all other persons whose images may be captured by the CCTV system.

1.3 This policy takes account of all applicable legislation and guidance, including:

- General Data Protection Regulation (GDPR);
- Human Rights Act 1998
- Surveillance Camera Commissioner – Code of Practice (12 Principles) (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/368115/Leaflet_v6_WEB.pdf)
- ICO – Code of Practice for surveillance cameras and personal information. (https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf)
- Home Office – Surveillance Camera Code of Practice (https://www.gov.uk/government/publications/surveillance-camera-code-of-practice)

1.4 This policy sets out the position of the School in relation to its use of CCTV and should be read in conjunction with the School Data Protection Policy.

1.5 The system comprises a number of internal and external day and night cameras and does **not** use any sound recording capability, facial recognition or ANPR(Automatic Number Plate Recognition) systems. The CCTV system is owned and operated by the School and the deployment of it is determined by the Senior Leadership Team. The Data Protection Officer (DPO) or their representative has overall responsibility as delegated by the Data Controller (Board of Governors).

1.6 Access and viewing is restricted and all authorised operators with access to images will be aware of the procedures they are required to follow and their responsibilities under this policy. All employees will be aware of the restrictions in relation to access to, and disclosure of, recorded images. The further introduction of, or changes to, CCTV monitoring will be subject to consultation with staff where appropriate.

2. Purpose of CCTV

2.1 The School uses CCTV for the following purposes:

- To provide a safe and secure environment for pupils, staff and visitors;
- To protect the school buildings and assets;
- To assist in reducing the fear of crime and for the protection of private property;
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.

3. Policy Intent

3.1 The school will:

- Notify the Information Commissioners Office of its use of CCTV as part of the annual data protection registration;
- Complete a CCTV Privacy Impact Assessment ("PIA") for the use of surveillance CCTV and will update this as appropriate when the system is upgraded or significantly modified;
- Treat the system and all information processed on the CCTV system as data which is covered by the Data Protection Act/GDPR;
- Use cameras to monitor activities within the school grounds to identify potential criminal activity for the purpose of securing the safety and well-being of the school, as well as for monitoring student behaviour;
- Not direct cameras outside of the school site at private property, an individual, their property or a specific group of individuals. The exception to this would be where an authorisation was obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000;
- Display CCTV warning signs will be clearly and prominently placed at all external entrances of the school site where CCTV is operational, including the school gates as coverage includes outdoor areas. The school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area which will contain details of the purpose for using CCTV.
- Not guarantee that a system will or can cover or detect every single incident taking place in the areas of coverage;
- Not use materials or knowledge for any commercial purpose. Recorded materials will only be released for use in the investigation of a specific crime and with the written authority of the Police and in accordance with the Data Protection Act/GDPR.
- Regularly review the use of CCTV within school to ensure it is sufficient in meeting the school's requirements and that no other alternatives are available which better meet the requirements.

4. Siting Cameras

4.1 Cameras will be sited so 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. For example, cameras will not be placed in areas which are reasonably expected to be private such as in toilets. The school will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act/GDPR requirements

4.2 CCTV is not sited in classrooms and will not be used in such, except in exceptional circumstances, for example, the ICT classrooms and other high value areas.

4.3 Members of staff, on request can access details of CCTV camera locations.

5. Storage, Retention and Security of CCTV images

5.1 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.

5.2 All retained data will be stored securely.

5.3 Recordings are kept for 31 days. Specific recordings which the school wishes to retain after this time will be logged in the schools own recording system (School Engine) and will be deleted as soon as the incident is deemed to be suitable resolved.

5.4 The recordings of all CCTV footage are stored as electronic files on the encrypted central CCTV Console. Access by staff to specific recordings are outlined below in section 8.

5.5 The Data Protection Act/GDPR does not prescribe any specific minimum or maximum retention periods that apply to all systems or footage. Rather, retention should reflect the organisation's purposes for recording information, which should be informed by the purpose for which the information is collected, and how long it is needed to achieve this purpose. Storage availability is also a factor to be considered in the ability to retain recordings.

5.6 Any request for footage to be extracted from the CCTV Console will be recorded and the recordings will be stored on the local school server using strict access policies managed by the IT Manager. The footage will only be accessible by a limited number of staff involved with the content of the recording.

5.7 The CCTV system meets or exceeds the current technology standards and uses the latest equipment which is regularly updated and maintained to provide continuous security.

6. Disclosure of Images to Data Subjects (Subject Access Requests)

6.1 Any Individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has the right to request access to those images.

6.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the School's Subject Access Request Policy.

6.3 All requests should be made in writing to the Head Teacher or Data Protection Officer or their representative. 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.

6.4 When such a request is made a member of the Senior Leadership Team will review the request, and once its approved, the request will be passed to the IT manager to extract the relevant footage from the system. The Senior Leadership Team will then review the CCTV footage produced to ensure it meets the request criteria as well as data protection regulations. Once completed the footage will be passed to the requestee.

6.4.1 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Senior Leadership Team as the CCTV system administrators must take appropriate measures to ensure that the footage is restricted in this way.

6.4.2 If the footage contains images of other individuals then the School must consider whether:

- The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;
- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

- If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

6.5 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

6.6 A record must be kept in the schools own recording system (School Engine), and held securely, of all disclosures which sets out:

- When the request was made;
- The process followed by the I.T. team (as the CCTV system administrators) in determining whether the images contained third parties;
- The considerations as to whether to allow access to those images;
- The individuals that were permitted to view the images and when; and
- Whether a copy of the images was provided, and if so to whom, when and in what format.

7. Disclosure of Images to Third Parties

7.1 The School will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

7.2 Third parties acting behalf of a duty subject will be handled in accordance with the School's Subject Access Request Policy.

7.3 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

7.4 If a request is received form a law enforcement agency for disclosure of CCTV images then the School must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

7.5 The information above must be recorded in relation to any disclosure.

7.6 If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

8. Access to CCTV Images

8.1 The ability to view live and historical CCTV data available via network software is only to be provided at designated locations and to authorised persons only. Direct access to recorded data is limited to the Senior Leadership Team, Progress Leaders and the IT Manager. Anyone outside of these groups who believes they need to view recordings or live feeds will have to make an official request to the IT Manager via the schools internal recording systems (SchoolEngine). Access will only be granted if the request meets this policy's requirements and only the requested section will be viewable to the requestee while the IT Manager is present, no footage will be exported or downloaded for members outside the groups mentioned above. The flow of information and the CCTV viewing/downloading procedures can be found in a flow chart in Appendix 1 of the schools CCTV Data Protection Impact Assessment.

8.2 Restricted live monitoring is provided to Administration staff for the purpose of security and incident management.

8.3 Progress Leaders and the Senior Leadership Team will have access to the live feeds and will be able to view recordings via the network software, for the purpose of incident management, evidence collection and security.

8.4 The IT Manager (as the system administrator) will be able to view live feeds, view recordings, export recordings and access the CCTV systems settings for the purpose of managing the system and processing requests from staff and third parties.

8.5 The school caretakes will have access to the live feed from the administration office for the purpose of building security and site safety.

8.6 Data from CCTV may be used within the school's' discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

9. **Complaints and enquiries**

- Complaints and enquiries about the operation of CCTV within the school should be directed to the Head Teacher or Data Protection Officer via the school office in the first instance.

Argoed High School
Bryn Road
Bryn-Y-Baal
Flintshire
CH7 6RY
01352 756414 | contact@argoedhs.co.uk

10. Further Information

For further information on CCTV and its use please see below:

- Data Protection Act 1998
- General Data Protection Regulation (GDPR)
- CCTV Code of Practice (ICO website https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/)

This policy has been written in conjunction with and approved by the schools data protection officer, David Bridge (GDBR)