Ysgol Cybi

Polisi CCTV Ysgolion / *Schools CCTV Policy*

(Fersiwn 1, Ebrill 2022 / *Version 1, April 2022)*

Ynglŷn â'r polisi hwn

Mae'r polisi hwn yn amlinellu'r hyn y mae angen i'r ysgol ei wneud i reoleiddio'r gwaith o reoli, gweithredu a defnyddio'r system CCTV (Teledu Cylch Cyfyng) yn yr ysgol.

Cefnogir y polisi hwn gan adnoddau ar y dudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

About this policy

This policy outlines what the school needs to do to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at the school.

This policy is supported by resources on the Data Protection page on the Learning Service Microsite.

Fersiwn / *Version*	**Dyddiad / *Date***	**Crynodeb o newidiadau / *Summary of changes***	**Dyddiad a Dderbyniwyd gan Fwrdd o Lywodraethwyr / *Date Accepted by Board of Governors***
F1 / *V1*	Ebrill 2022 / *April 2022*	Polisi newydd- cymryd lle y fersiwn cyfredol / *New policy- replacing the current version.*	30/09/26

Dyddiad yr adolygiad nesaf / *Date of next review*	
Bydd y polisi hwn yn cael ei adolygu yn: / *This policy will be reviewed in:*	Ebrill 2025 / *April 2025*
Yr unigolyn a fydd yn ymgymryd â'r adolygiad fydd: / *The review will be undertaken by:*	Swyddog Diogelu Data Ysgolion / *Schools Data Protection Officer*

Content **Page**

1. Policy Statement 25
2. Scope 25
3. Legislation, Guidance and Policies 26
4. Definitions 27
5. Responsibilities 28
5.1. School Governing Body 28
5.2. Headteacher (and/or Person Responsible for Data Protection within the School) 28
5.3. Schools Data Protection Officer 29
6. Why does the School have CCTV 30
7. Lawful Basis for Processing 30
8. System Management 31
8.1. Data Protection Impact Assessment (DPIA) 32
8.2. Access 32
9. CCTV Coverage 33
9.1. Notifications 33
9.2. Location of Cameras 34
9.3. Visitors 35
10. Covert Surveillance 35
11. Storage and Retention of Equipment and Data 36
12. Assessment of the CCTV System 36
13. Download Footage Procedures 37
14. Subject Access Requests 38
14.1. Images of Other Individuals / Third Parties 39
15. Access to and Disclosure of Images to Third Parties 39
16. Sharing CCTV Images with the Police 41
17. Third Party Processing 41
18. Live Facial Recognition Technology (LFR) 42
19. Training 42
20. Complaints 42
21. Breach of the Policy 43
22. Review of Policy and Oversight Arrangements 43
APPENDIX A- Schools CCTV System Log 48
APPENDIX B- Schools CCTV Locations Log 51
APPENDIX C- Schools CCTV Procedure 52
APPENDIX D- Schools CCTV Policy- Headteacher's Checklist 56

1. Policy Statement

Data protection legislation aims to protect personal privacy and the rights of individuals about whom data is obtained, stored, processed or supplied. The *UK General Data Protection Regulation (UK GDPR)* requires that organisations have appropriate technical security measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Capturing and/or recording images of identifiable individuals constitutes processing personal information and therefore needs to comply with the data protection principles under *UK GDPR* and the *Data Protection Act 2018*.

The school uses CCTV cameras to monitor activities within the school and its grounds to identify criminal activity actually occurring, anticipated, or perceived. It is also used for the purpose of securing the safety and well-being of the pupils and staff at the school together with its visitors and the general public.

This policy details the purpose and regulates the management, operation and use of the CCTV system at the school. It also provides details around the procedures to be followed.

The purpose of this policy is to ensure that:

- the school complies with data protection legislation, including the *Data Protection Act 2018;* the *UK General Data Protection Regulation (UK GDPR)* and with the Surveillance Camera Commissioner's *Code of Practice;*
- the images that are captured are useable for the purposes the school require them for;
- the school can reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

The system comprises a number of fixed and dome cameras located around the school site. All fixed cameras are in plain sight on the school premises. The school does not routinely use CCTV for covert monitoring or monitoring of private property outside the school grounds, unless there is an exceptional or extreme circumstance to do so.

The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under *UK GDPR* and the *Data Protection Act 2018.*

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Images will never be released to the media for purposes of entertainment.

2. Scope

This policy applies to all members of staff within the school who are authorised to access the school's CCTV system.

This policy also serves as a notice and a guide to data subjects (including pupils, parents, staff, volunteers, visitors to the school and members of the public and any other persons whose images may be captured on the CCTV system) regarding their rights in relation to personal data recorded via the school's CCTV system.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- observing what an individual is doing;
- taking action to prevent a crime;
- using images of individuals that could affect their privacy.

This policy and the procedures contained within, applies to all of the school's CCTV systems including webcams, covert installations and any other system capturing images of identifiable individuals for the purpose of viewing and or recording the activities of such individuals.

CCTV images are monitored and recorded in strict accordance with this policy.

3. Legislation, Guidance and Policies

The main data protection legislation that this policy complies with is that of the *UK General Data Protection Regulation (UK GDPR)* and the *Data Protection Act 2018.*

Other applicable legislation that is taken in to account within this policy, includes:

- *Protection of Freedoms Act 2012 (POFA);*
- *Human Rights Act 1998 (HRA);*
- *Regulation of Investigatory Powers Act 2000;*
- *Freedom of Information Act 2000 (FOIA);*
- *The Regulation of Investigatory Powers Act 2000 (RIPA);*
- *Criminal Justice and Public Order Act 1994;*
- *Criminal Procedure and Investigations Act 1996*

This policy is also based on relevant codes of practice and on guidance published by the Information Commissioner's Office (ICO)- *'Video Surveillance Guidance'* and on the principles of the Surveillance Camera Commissioner's *Code of Practice,* in particular the 12 guiding principles. The school will also follow-*'In the picture: A data protection code of practice for surveillance cameras and personal information'* and the *'Surveillance Camera Commissioner Buyers Toolkit'.*

This policy should also be read in conjunction with the *Schools Data Protection Policy; Schools Data Protection Impact Assessment (DPIA) Policy; Schools Information Security Policy; Schools Data Breach Policy*; *Schools Data Subject Access Request Policy* and the *Gwynedd and Anglesey Procedure for Sharing Information with Police Authorities in the*

United Kingdom. These are all available on the Data Protection page on the Learning Service Microsite.

Relevant documents that are available on the Data Protection page on the Learning Service Microsite:

- *Schools CCTV Locations Log;*
- *Schools CCTV System Log*;
- *Schools CCTV Procedure* document*;*
- *Schools Data Subject Access Request Form;*
- *SA3 Form- Request to external organisation for the disclosure of personal data to the Police.*

4. Definitions

Personal data	Any information relating to an identified or identifiable natural person that can be identified either directly or indirectly from that information. This can be stored electronically, on a computer, or in paper-based filing systems.
Special category data	Information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation. Special category data is personal data that needs more protection because it is sensitive.
Processing information	Collecting, obtaining, recording, organising, structuring, storing, retaining, amending, adapting, altering, retrieving, consulting, disseminating, restricting, disclosing, destroying, erasing information or using or doing anything with it.
Surveillance	Monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy, only video footage will be applicable.
Overt surveillance	Any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.
Covert surveillance	Any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.
Live Facial Recognition (LFR)	Live facial recognition (LFR) technology, also known as automatic facial recognition, identifies people in a video in real time, using a set of photographs as a reference. Facial recognition surveillance cameras scan all the faces they can see in a crowd to check people's identity against a database in real-time.
Information Systems	Information processing computers or data communication systems.
Risk	Effect of uncertainty on objectives. Risks to individuals: the potential for damage or distress. Risk is often characterised by

	reference to potential "events" and "consequences", or a combination of these.
Impact	What are the consequences of the risk were it to occur. Impact is considered as having either an immediate effect or a future effect.
Unauthorised	Without a legitimate right.
Encryption	Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data appears scrambled or unreadable to a person or entity accessing without permission.

5. Responsibilities

5.1. School Governing Body

The school governing body has the responsibility for:

- ensuring that this policy has been formally adopted by the school;
- monitoring the school's overall compliance and accountability relating to this policy;
- ensuring that the school can evidence compliance with data protection legislation.

5.2. Headteacher (and/or Person Responsible for Data Protection within the School)

The Headteacher and/or the person who is responsible for data protection within the school is responsible for:

- ensuring that there is a process in place to continually monitor the school's compliance with this policy;
- ensuring that the use of CCTV systems is implemented in accordance with this policy and is processed legally and fairly;
- ensuring that all school employees are aware of the restrictions in relation to access to, and disclosure of, recorded images;
- the overall operation and accountability for how the school uses the CCTV system;
- the overall day-to-day management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy;
- conferring with the Schools Data Protection Officer with regard to the lawful processing of the surveillance and CCTV footage;
- ensuring that the CCTV monitoring is consistent with the highest standards and protections;
- undertaking regular performance monitoring, including random operating checks on the CCTV system;
- ensuring that adequate signage is erected around the school in compliance with the Surveillance Camera Commissioner's *Code of Practice;*
- ensuring that the *Schools CCTV Locations Log* has been completed and is kept up-to-date;

- ensuring that the *Schools CCTV Procedure* document has been completed and is kept up-to-date:
- maintaining a record of access (e.g. a systems log) to or the release of any material recorded or stored in the system;
- ensuring that set retention periods are adhered to and consider who is allowed access to CCTV footage and why;
- ensuring that images recorded are stored for a period no longer than 30 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil);
- ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period;
- ensuring that the perimeter of view from fixed location cameras conforms to this policy both internally and externally;
- ensuring that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "reasonable expectation of privacy";
- ensuring that monitoring footage is stored in a secure place with access by authorised staff only;
- ensuring that there are robust cyber security measures in place to protect data held on the system;
- ensuring that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics;
- keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage and detailing the purpose of the activity within the school's ROPA;
- ensuring that staff that have access to the school's CCTV system receive adequate training to ensure full understanding of the system and to keep records of training details;
- managing any complaints regarding the CCTV system including giving consideration to both pupils and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.

5.3. Schools Data Protection Officer

The Schools Data Protection Officer is responsible for:

- providing an independent overview of compliance issues;
- ensuring that the school handles and processes surveillance and CCTV footage in accordance with data protection legislation;
- monitoring legislation to ensure the school is using surveillance fairly and lawfully;
- monitoring that surveillance and CCTV footage is destroyed by the school in line with legal requirements when it falls outside of its retention period;
- coordinating access requests for data held on CCTV systems;
- providing advice and assistance when requested and advise and assist on complaints and the operation of the equipment;

- providing guidance and support with completing a Data Protection Impact Assessment (DPIA) where necessary and monitoring the performance of the school's DPIA;
- monitoring the privacy impact of the use of CCTV equipment;
- providing support with creating any data processing agreements for data processors.

6. Why does the School have CCTV

The use of the CCTV system at the school is:

- to protect and maintain the well-being and welfare of pupils, staff, visitors and the general public;
- to promote the health and safety of pupils, staff, visitors and the general public;
- to maintain a safe and secure environment;
- to increase personal safety and reduce the fear of crime;
- to prevent and reduce the incidence of bullying and anti-social behaviour (including theft and vandalism);
- to deter criminal acts against persons and property;
- to protect the school buildings, assets, property and equipment both during and after school hours;
- to protect the personal property of pupils, staff and visitors from loss or damage;
- to assist staff in identifying and resolving incidents;
- to monitor the security and integrity of the school site and deliveries and arrivals, including car parking;
- to ensure that the school rules are respected so that the school can be properly managed;
- to support the Police and the community in preventing, deterring, reducing, detecting and investigating crime;
- to assist in identifying, apprehending and prosecuting those who have committed an offence;
- to be used as evidence during disciplinary, grievance and complaint procedures where necessary and appropriate to do so.

7. Lawful Basis for Processing

Cameras will be used to monitor activities within the school; its car parks and other public areas to identify potential or actual criminal activity or behaviour which does not comply with school codes of conduct and for securing the safety and well-being of pupils, visitors and the general public.

Processing is considered to form part of the school's public task therefore the lawful basis for processing is considered to be:

- *Article 6(1)(e,) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*

The school will ensure that it:

- processes surveillance and CCTV footage legally and fairly;
- collects surveillance and CCTV footage for legitimate reasons; is only used for the purposes for which it is intended and ensuring that it is used accordingly;
- collects surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection;
- designs the system to take into account its effect on individuals and their privacy and personal data;
- has defined policies and procedures in place which are communicated throughout the school;
- considers all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law;
- has clear responsibility and accountability procedures for images and information collected, held and used;
- restricts access to retained images and information with clear rules on who can gain access;
- ensures that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary;
- protects footage containing personal data against accidental, unlawful destruction, alteration and disclosure and unauthorised access;
- is transparent and includes a contact point through which people can access information and submit complaints;
- regularly undertakes reviews and audits to ensure that policies and standards are maintained.

The misuse of CCTV system and images could constitute a criminal offence.

Unauthorised disclosures can cause damage and distress to individuals, and may lead to the ICO taking enforcement action. Other laws that focus on libel, harassment, malicious communications or threatening behaviour may also apply in some circumstances.

8. System Management

The CCTV system is owned, operated, administered and managed by the school. The school is the data controller for the images produced by the CCTV system. All cameras are monitored within the school or by the school's preferred monitoring company.

It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage 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.

The Headteacher should complete the *Schools CCTV Procedure* document (APPENDIX C) that details how the system is managed. This is also available on the Data Protection page on the Learning Service Microsite.

8.1. Data Protection Impact Assessment (DPIA)

Where new CCTV systems or cameras are to be installed, the school will carry out a Data Protection Impact Assessment (DPIA) identifying risks related to the installation and ensuring full compliance with data protection legislation in consultation with the Schools Data Protection Officer. This may also involve the need for consultation with staff, parents and other relevant bodies.

A DPIA will be carried out prior to the installation of any surveillance and CCTV system. If the DPIA reveals any potential security risks or other data protection issues, the school will ensure that there are adequate provisions in place to overcome these issues.

Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before the CCTV system is used, and the school will act on the ICO's advice.

The school will ensure that the installation of the surveillance and CCTV systems will always justify its means. If the use of a surveillance and CCTV system is too intrusive in terms of privacy, the school will seek alternative provision.

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy.

If the surveillance and CCTV systems fulfil their purpose and are no longer required, the school will deactivate them. Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

The use of CCTV and the Data Protection Impact Assessment (DPIA) relating to it shall be regularly reviewed to ensure its operation remains necessary and proportionate in meeting its stated purposes.

The school will comply with the *Schools Data Protection Impact Assessment (DPIA) Policy.*

8.2. Access

The Headteacher will be responsible for the day-to-day management of the CCTV system. Supervising the access and maintenance of the CCTV system is the responsibility of the Headteacher.

The Headteacher may delegate the administration of the CCTV system to another staff member. The CCTV system and the data collected will only be accessible by the Headteacher as the System Manager or other authorised school employees who need to have access to the data. The Headteacher will consider who is allowed access to this

footage and why. Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

Access to recording systems and retained CCTV images will only be given to authorised persons, under the supervision of the Headteacher, in pursuance of the objectives set by the school or if there is some other overriding and lawful reason to grant such access. Recording systems will be protected by appropriate security measures such as password protection as an additional security measure.

A systems log will be maintained by the school, stating who accessed the recordings/images, on what dates and times, and for what purposes. The *Schools CCTV System Log* (APPENDIX A) template should be used. This is also available on the Data Protection page on the Learning Service Microsite.

Images will be viewed and/or monitored in a suitably secure, restricted and private area to minimise the likelihood of, or opportunity for access, to unauthorised persons. Visual display monitors are located in a designated area and should not be viewed or be capable of being viewed by anyone other than authorised persons. Other school employees and pupils should not be allowed to have access to that area when a viewing is taking place.

All authorised operators and school staff with access to CCTV images are aware of the procedures that need to be followed when accessing the recorded images. All school staff are aware of the restrictions in relation to access to, and disclosure of, recorded images and will only be authorised to use the CCTV system in a way that is consistent with the purposes and procedures.

In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

Recorded images may be disclosed to school governors as part of an internal disciplinary proceeding, grievance procedure or complaint if appropriate.

Applications received from outside bodies (e.g. solicitors, Police) to view or release images will be referred to the Schools Data Protection Officer in the first instance.

The school will also need to ensure that there are robust cyber security measures in place to protect the data held within the system.

9. CCTV Coverage

9.1. Notifications

The school must notify staff, pupils, visitors and members of the public that they are entering a zone that is covered by CCTV surveillance and note why it is collecting personal information in the form of CCTV images. This is included in the school's *Privacy Notices.*

Notices informing people that CCTV is in operation should be displayed in a prominent position in all zones that are being filmed as required by the Surveillance Camera Commissioner's *Code of Practice*.

Using prominently placed signs at the main external entrances to the school and then using further signs inside the zones and controlled areas will let people know when they are in an area where a surveillance system is in operation.

Appropriate locations for signage will include entrances to premises both for pedestrians and vehicles i.e. external doors, school gates; reception area and in close proximity to each internal camera. The signs should be clear and legible.

The signs should contain the following information:

- identity of the person or organisation responsible for the CCTV system;
- the purposes of the CCTV system;
- details of whom to contact regarding the CCTV system;
- any other information that may become a statutory requirement.

9.2. Location of Cameras

The location of the CCTV cameras will be chosen with great care and will not be erected in places where individuals would have a reasonable expectation of privacy (such as changing rooms and toilets). Care will be taken to ensure that reasonable privacy expectations are not violated. The school will ensure that the location of equipment is carefully considered to ensure they only capture images relevant to the purposes for which they are installed and comply with data protection legislation.

Unless an immediate response to events is required, CCTV cameras on school premises will be erected in a fixed place and will not be directed, rotated or trained at certain individuals, their property or a specific group of individuals or events. All such CCTV equipment installed in the school will only be sited in such a way that it only monitors those spaces that are intended to be covered by the equipment. The CCTV system will be used to observe the school's property in order to identify incidents requiring a response.

The school will ensure to the greatest extent possible that there is no (or only minimal) recording of passers-by or another person's private property. The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

Within the school buildings, the CCTV coverage is in corridors, stairwells, access areas, public, communal and social areas.

The system will not record any sound and the school will switch off by default any capability to record audio.

CCTV will not be used in classrooms unless covert surveillance is **absolutely necessary**.

The school will keep a record that provides detail regarding the location of different cameras and what is captured by the camera within that area within the school via the

Schools CCTV Locations Log (APPENDIX B). This is also available on the Data Protection page on the Learning Service Microsite.

The CCTV system will be operated 24 hours a day, every day of the year. During periods of school closure, the Headteacher or other nominated staff members may have secure remote access to live and recorded images.

The surveillance system has been designed and installed for maximum effectiveness and efficiency, however, the school cannot guarantee that the system will cover or detect every single incident taking place in the areas of coverage and 'blind spots' may exist.

Members of school staff will have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

9.3. Visitors

Details of ALL visits and visitors to the school will be recorded in the school visitor book or via electronic signing in system, including the time of access. This will support the school with identifying individuals.

10. Covert Surveillance

Covert surveillance is the use of surveillance which is intentionally not shared with the subjects it is recording. Subjects are being recorded without their knowledge. Examples of covert surveillance includes filming someone who is suspected of performing illegal or fraudulent activities such as stealing or filming someone where there is suspicion of abuse, violence or harm so that information and/or evidence can be gathered for an investigation.

The school does not condone the use of covert surveillance when monitoring the school's staff, pupils and/or volunteers. Covert surveillance will be restricted to rare occasions and only be operable in **exceptional or extreme circumstances**, for example:

- where there is good cause to suspect that an illegal or unauthorised action is taking place, or where there are grounds to suspect serious misconduct;
- where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

A request for the use of covert cameras will clearly state the purpose and reasons for use. Authorisation must be sought and granted by the Learning Service Senior Management Team and an Authorising Officer of the Isle of Anglesey County Council in accordance with the *Regulation of Investigatory Powers Act 2000* prior to commencement.

Covert surveillance carried out by school staff without a form of authority from the Learning Service Senior Management Team may be subject to disciplinary action.

The Learning Service Senior Management Team should be satisfied that all other physical methods of prevention have been exhausted prior to the use of covert recording.

All such monitoring will be fully documented and will only take place for a limited and reasonable period.

Covert monitoring must cease following completion of an investigation. 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.

11. Storage and Retention of Equipment and Data

Recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. Access to the CCTV system and stored images will be restricted to authorised users only and the area will be locked when not occupied by the authorised users. Access to the surveillance system, software and data will be strictly limited to authorised users and will be password protected.

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.

Where such data is retained, it will be retained in accordance with data protection legislation. Information including the date, time and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the systems log. Once the retention period has expired, the images should be removed or erased.

Recorded data will normally be retained for a minimum of two weeks but for a maximum of 30 days, except where the image identifies an issue which necessitates extraction and retention of said piece of evidence or is retained specifically in the context of an investigation/prosecution of that issue. CCTV images/recordings may capture issues such as criminal behaviour or a risk to health and safety and the CCTV images/recordings may need to be retained to investigate that issue. The footage may be lawfully required by an appropriate third party such as the Police or the local authority.

Unless data is required for the above purposes by the school or investigatory bodies, data will be automatically or manually over-written or securely deleted. Any unnecessary footage captured will be securely deleted from the school system. If required for investigatory purposes, data will be destroyed as soon as it is no longer required.

12. Assessment of the CCTV System

The Headteacher will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording; that cameras are functional and are operating effectively. The cameras installed should provide images that are of suitable quality for the specified purposes for which they are installed.

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 Headteacher will take action to correct the error. A note of such changes will be recorded in the systems log.

Cameras are to be properly maintained and serviced to ensure that clear images are recorded. The system will be checked and servicing will be carried out at least annually.

Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied to the system or any other devices connected to it, are applied immediately.

Cameras should be protected from vandalism in order to ensure that they remain in working order.

The governing body may wish to receive an annual report of the system's performance and priorities including a brief overview of security checks and measures, compliments and complaints, disclosure requests etc.

13. Download Footage Procedures

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

- each download footage must be identified by a unique mark;
- before use, each download footage must be cleaned of any previous recording;
- the Headteacher will register the date and time of download footage insertion, including its reference;
- download footage required for evidential purposes must be sealed, witnessed and signed by the Chair of Governors and Headteacher, then dated and stored in a separate secure evidence store. If download footage is not copied for the Police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the Chair of Governors and Headteacher, then dated and returned to the evidence store.

If download footage is archived, the reference must be noted. Downloaded footage will be properly indexed, stored and destroyed after appropriate use, in accordance with the data protection legislation and retention periods.

When accessing and viewing images, two authorised members of staff must be present (one preferably being the Headteacher). A written record of access will be kept via a systems log. Records of access will be kept and will document the following:

- the date and time of removal;
- the name of the person removing the images;
- the name(s) of the person(s) and the organisation that they represent viewing the images;
- the reason for the viewing;

- how the request was dealt with;
- the outcome, if any, of the viewing;
- the date and time the images were returned to the system; or
- secure place, if they have been retained for evidential purposes.

Data will be provided in a permanent format where possible. If this is not possible, the individual will be offered the opportunity to view the footage.

Encryption should be used for exported recordings to protect the footage.

14. Subject Access Requests

Individuals have the right to request access to the personal data the school holds on them relating to themselves and to verify the lawfulness of the processing under data protection legislation. This includes information held on the CCTV system, if it has been kept. The school will have to ensure that it can provide individuals with copies of that individual's images captured by the CCTV system as far as reasonably practicable. This right is subject to certain exemptions from access, including in some circumstances, where others are identifiable.

Individuals submitting requests for access will be asked to complete the *Schools Data Subject Access Request Form* and to provide sufficient information and specific details to enable the footage relating to them to be identified, for example, date, time and location of the recording.

Photographic evidence of identity and/or detailed description to allow for identification will be requested. The school must satisfy themselves of the identity of any person wishing to view images or access the system and the legitimacy of the request. Where any doubt exists, access will be refused.

In giving the person a copy of their data, the school may provide a still/series of still pictures, a tape or disk with relevant images. If the footage contains only the individual making the request, then the individual may be permitted to view the footage.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

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.

Where the school is unable to comply with a subject access request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

The school will comply with the *Schools Data Subject Access Request Policy* and the Schools Data Protection Officer will provide advice and guidance to the school and may facilitate and support with preparing a response to the request.

The *Schools Data Subject Access Request Form* is available on the Data Protection page on the Learning Service Microsite and the school will make this available to any individuals who requests this form. The school will also provide links to the form on their website or social media accounts.

The school should seek the advice of the Schools Data Protection Officer if unsure of how to deal with a request.

14.1. Images of Other Individuals / Third Parties

When dealing with a subject access request the school must consider if there are images of other individuals other than the individual making the request that appears on the footage.

Images of other individuals should be obscured before the data is released to the applicant. Where footage contains images relating to third parties, the school will take appropriate steps to mask and protect the identities of those individuals.

Specialist software may need to be used to redact visual data of third parties. Available techniques include blurring, masking, or using a solid fill to completely obscure parts of the footage. The technique most applicable depends on the circumstances of how the footage was created and the quality of the footage.

If it is necessary for the school to contract out the redaction process to a specialist organisation, a written contract will need to be in place with the company as a data processor.

The Schools Data Protection Officer should be contacted if the school is unsure if there are exceptional circumstances where it is appropriate to share images of third parties. The Schools Data Protection Officer will consider the following in these circumstances:

- whether the request *requires* the disclosure of others or can the images be distorted so as not to identify them;
- how much time it will take to deal with the request and if this exceeds the threshold of what is considered as a reasonable time to process the request;
- whether the other individuals have consented to the disclosure of the images;
- where consent is not sought or obtained, whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

15. Access to and Disclosure of Images to Third Parties

In limited and prescribed circumstances, it may be appropriate to disclose images to a third party, such as when a disclosure is required by law in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.

ATODIAD C / *APPENDIX C*

Gweithdrefn CCTV yr Ysgol / *School's CCTV Procedure*

Ysgol /*School*	**Cybi**
Manylion pwy sydd yn gyfrifol am system CCTV yr ysgol / *Details of who is responsible for the school's CCTV system*	**Pennaeth – Rhian Grieves**
Manylion pa aelodau staff sydd gyda'r awdurdod i gael mynediad i system CCTV yr ysgol / *Details of which members of staff have been authorised to access the school's CCTV system*	**Rhian Grieves**
Manylion o beth yn union mae'r aelodau staff efo'r awdurdod i wneud efo system CCTV yr ysgol / *Details of exactly what the members of staff are authorised to do with the school's CCTV system*	**View**
Manylion o pa drefniadau sydd gan yr ysgol mewn lle ar gyfer rheoli a chynnal system CCTV yr ysgol / *Details of what arrangements the school has in place to manage and maintain the school's CCTV system*	**As per LA advice**

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 school where these would reasonably need access to the data (e.g. investigators).

Requests should be made in writing to the Headteacher. Such disclosures will be made at the discretion of the Headteacher, with reference to relevant legislation and where necessary, following advice from the Schools Data Protection Officer.

The following are examples when the Headteacher may authorise access to CCTV images to authorised third parties:

- where required to do so, the Police or some relevant statutory authority where the school (or its agents) are required by law to make a report regarding the commission of a suspected crime; or
- following a request by the Police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on school property; or
- to make a report regarding suspected criminal behaviour; or
- to prosecution agencies – such as the Crown Prosecution Service (CPS); or
- to enable the designated safeguarding lead or their appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern or to the HSE and/or any other statutory body charged with child safeguarding; or
- to assist the school in establishing facts in cases of unacceptable pupil behaviour, in which case, the parents/guardian will be informed as part of the school's management of a particular incident; or
- to data subjects (or their legal representatives such as lawyers or barristers) pursuant to an access request under data protection legislation or subject to a court order; or
- to the school insurance company where required in order to pursue a claim for damage done to insured property; or
- in any other circumstances required under law or regulation.

Where images are disclosed, a record will be made in the systems log. The following will be documented:

- the date and time at which access was allowed or the date on which disclosure was made;
- the identification of third party who was allowed access or to whom disclosure was made;
- the person who authorised the request;
- the reason for allowing access or disclosure;
- the details of images viewed;
- location of the images;
- any crime incident number to which images may be relevant;
- signature of person authorised to collect the medium – where appropriate.

Liaison meetings may be held with all bodies involved in the support of the system. Liaison meetings may also be held with the Police and other bodies if required.

The data 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.

All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented in the systems log.

16. Sharing CCTV Images with the Police

Images may be viewed by the Police for the prevention and detection of crime. The Police **must** complete the relevant form (*SA3 Form- Request to external organisation for the disclosure of personal data to the Police).* CCTV images should not be shared if the relevant form has not been fully completed by the Police and received by the school prior to sharing or providing access to the CCTV images unless there is an emergency situation (e.g. missing child, a child that is in danger) that requires immediate access to the footage. In these cases, the form can be submitted after the disclosure.

Recordings and images will only be released to the media for use in the investigation of a specific crime following a specific request by the Police or by the written authority of the Police.

A record will be maintained of the release of any download footage to the Police or other authorised applicants. Viewing of images by the Police must be recorded in writing in the systems log. 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 download footage (and any images contained thereon) remains the property of the school, and 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 footage (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded footage, this will be produced from the secure evidence store, complete in its sealed bag.

The Police may require the school to retain the downloaded footage for possible use as evidence in the future. Such downloaded footage will be properly indexed and securely stored until they are needed by the Police.

The school will comply with the *Gwynedd and Anglesey Procedure for Sharing Information with Police Authorities in the United Kingdom*.

17. Third Party Processing

Where the CCTV is operated or controlled by a third party (such as a commercial security company), the school must put a written data processing agreement in place with that company.

The school should ensure that the third party meet the relevant Security Industry Authority (SIA) licensing requirements. CCTV owned by the school, operated by its own staff and whose data is controlled by the school is classed as in-house and does not fall under SIA legislation.

The Schools Data Protection Officer will provide further advice and guidance and will prepare any agreement with a third party company providing CCTV for the school.

The school does not own or manage third party CCTV systems, but may be provided with images of incidents by third parties where this is in line with the objectives of the school's own CCTV Policy and/or its school rules.

18. Live Facial Recognition Technology (LFR)

Live facial recognition (LFR) technology, also known as automatic facial recognition, identifies people in a video in real time, using a set of photographs as a reference. Facial recognition surveillance cameras scan all the faces they can see in a crowd to check people's identity against a database in real-time.

If the school is considering using live facial recognition technology (LFR), it must discuss this with the Schools Data Protection Officer before purchasing this technology.

The school will need to demonstrate high standards of governance and accountability from the outset, including being able to justify that the use of LFR is fair, necessary and proportionate in each specific context in which it is deployed.

All risks will also need to be considered when using this new form of technology and completing a Data Protection Impact Assessment (DPIA) will be necessary.

19. Training

Staff that have access to the school's CCTV system should have adequate training to ensure understanding of the system.

The Headteacher will keep a record of training undertaken by staff with access to the CCTV system.

20. Complaints

Individuals who have had their image captured by the system have a right to object and should follow the school's complaints procedure.

Any complaints and enquiries in relation to the school's CCTV system should be addressed initially to the Headteacher.

Individuals have the right to make a complaint to the Information Commissioner's Office (ICO) who is the independent regulator for data protection:

E-mail: https://ico.org.uk/concerns/

Telephone: 0303 123 1113

Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

21. Breach of the Policy

Non-compliance with this policy by members of school staff could lead to serious consequences including a breach of the law and a risk of significant civil and criminal sanctions for the individual and the school authorities.

This can lead to putting both the individuals whose personal information is being processed and the school at risk.

Non-compliance with the policy or misuse of surveillance system information by a member of school staff may be considered a disciplinary matter. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

22. Review of Policy and Oversight Arrangements

This policy will be reviewed by the Schools Data Protection Officer, to include consultation as appropriate with interested parties, every three years, unless changes to legislation, codes of practice, or guidance requires the policy to be updated sooner.

The policy will be approved by the Learning Service Senior Management Team and will be adopted by the school governing body. Compliance with this policy and related procedures will be monitored by the School Leadership Team and the governing body.

If there are any queries or concerns about anything contained in this policy, the Schools Data Protection Officer should be contacted without hesitation:

E-mail: dpoysgolionmon@ynysmon.gov.uk

Telephone: 01248 751833

Address:
Learning Service
Isle of Anglesey County Council
Council Offices
Llangefni
Anglesey
LL77 7TW

Further information regarding data protection and CCTV can be obtained from the ICO website: https://ico.org.uk/ and the Surveillance Camera Commissioner's website: https://www.gov.uk/government/organisations/surveillance-camera-commissioner

APPENDIX A

Schools CCTV System Log

This form must be completed when removing images to be viewed (*to be printed out or can add additional lines electronically as needed*).

Removing Images to be Viewed							
Date and time of removal	**Name (person removing the images)**	**Name (person and organisation viewing the images)**	**Reason for the viewing**	**How the request was dealt with**	**Outcome of the viewing**	**Date and time returned to system**	**Secure place retained for evidence**

APPENDIX D

Schools CCTV Policy

Headteacher's Checklist

No	Actions to be Taken	Has the school got this in place (Yes/No)/ Comments/Dates etc.)
1	The current version of the *Schools CCTV Policy* has been formally adopted by the School Governing Body.	
2	There is a process in place to continually monitor the school's compliance with this policy.	
3	All school employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.	
4	There is a schedule in place to undertake regular performance monitoring, including random operating checks, on the CCTV system. To check and confirm the efficiency of the system and in particular that the equipment is properly recording; that cameras are functional and are operating effectively and that the date and time reference is correct.	
5	There is adequate signage erected around the school in compliance with the Surveillance Camera Commissioner's *Code of Practice:* • notices are displayed in a prominent position in all zones that are being filmed; • there are prominently placed signs at the main external entrances to the school; • signs contain the required information that needs to be made available to individuals.	
6	The *Schools CCTV Locations Log* has been completed and is kept up-to-date.	
7	The *School's CCTV Procedure* document has been completed and is kept up-to-date.	
8	The *Schools CCTV System Log* is always used to maintain a record of access to or the release of any material recorded or stored in the system.	

9	Monitoring that images recorded are stored for a period of no longer than 30 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil).	
10	Monitoring that there are robust cyber security measures in place to protect data held on the system.	
11	Records of all data processing activities relating to surveillance and CCTV footage are included within the school's ROPA.	
12	Staff that have access to the school's CCTV system have received adequate training to ensure full understanding of the system and records of training details are kept.	
13	There is a process in place to manage any complaints regarding the CCTV system.	
14	A Data Protection Impact Assessment (DPIA) has been undertaken for the CCTV system and this is kept up-to-date.	
15	Visual display monitors are located in a secure designated area that is restricted and private where unauthorised persons cannot access it.	
16	Cameras have not been placed in places where individuals would have a reasonable expectation of privacy (such as changing rooms and toilets).	
17	Cameras are not trained on private vehicles or property outside the perimeter of the school and there is no (or only minimal) recording of passers-by or another person's private property.	
18	All visitors to the school are recorded in the school visitor book or via electronic signing in system.	
19	The CCTV system is serviced annually.	
20	Software updates (particularly security updates) are applied immediately.	
21	There is a robust download footage procedure and this is followed.	
22	There is a Subject Access Request process in place to deal with requests for information from CCTV images.	
23	There is a process in place to deal with requests for access to and disclosure of images to third parties.	
24	Images are not released to the Police unless the school has received a signed *SA3 Form- Request to external organisation for the disclosure of personal data to the Police.*	

25	There is a written data processing agreement in place with the company who operates or controls the school's CCTV System (if applicable).	
26	If considering using live facial recognition technology (LFR), this has been discussed with the Schools Data Protection Officer before purchasing this technology (if applicable).	

This form must be completed when access or disclosure is allowed (*to be printed out or can add additional lines electronically as needed*).

Allowing Access or Disclosure of Images							
Date and time access allowed / disclosure made	**Identification of third party allowed access or disclosure made to**	**Name of person who authorised request**	**Reason for allowing access or disclosure**	**Details of images viewed**	**Location of the images**	**Relevant crime incident number**	**Signature of person authorised to collect images**

This form must be completed when access or disclosure is refused (*to be printed out or can add additional lines electronically as needed*).

Refusal of Access or Disclosure of Images							
Date of request	**Details of person / organisation requesting access or disclosure**	**Details of images requested**	**Location of the images requested**	**Name of person who refused request**	**Reason for refusing access or disclosure**	**Details when refused and how refusal was communicated**	**Relevant crime incident number (if applicable)**

ATODIAD B / *APPENDIX B*

Log Lleoliadau CCTV Ysgolion / *Schools CCTV Locations Log*

Ysgol / *School:*	

Camera	**Ardal sydd yn cael ei fonitro / *Area that is being monitored***	**Nodiadau a Sylwadau / *Notes and Comments***
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		