CYNGOR SIR YNYS MÔN
ISLE OF ANGLESEY COUNTY COUNCIL

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.*	

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*

Manylion Cyswllt:

Swyddog Diogelu Data Ysgolion

E-bost:
dpoysgolionmon@ynysmon.gov.uk

Rhif ffôn: 01248 751833

Cyfeiriad:
Gwasanaeth Dysgu
Cyngor Sir Ynys Môn
Swyddfeydd y Cyngor
Llangefni
Ynys Môn
LL77 7TW

Contact Details:

Schools Data Protection Officer

E-mail:
dpoysgolionmon@ynysmon.gov.uk

Telephone: 01248 751833

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

Rydym yn hapus i ddarparu'r polisi hwn ar ffurfiau eraill ar gais. Defnyddiwch y manylion cyswllt uchod. / *We are happy to provide this policy in alternative formats on request. Please use the above contact details.*

Dogfen:	Templed polisi sy'n 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.
Document:	*Policy template outlining what the school needs to do to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at the school.*
Cyfrifoldeb:	Cyfrifoldeb corff llywodraethu a Phennaeth yr ysgol yw sicrhau bod gweithdrefnau ar waith i sicrhau bod yr ysgol yn rheoleiddio'r gwaith o reoli, gweithredu a defnyddio'r system CCTV yn yr ysgol. Cyfrifoldeb y Pennaeth yw sicrhau bod holl staff perthnasol yr ysgol yn gweithredu ac yn cydymffurfio.
Responsibility:	*It is the responsibility of the school governing body and the Headteacher to ensure procedures are in place to ensure that the school regulates the management, operation and use of the CCTV system at the school. It is the responsibility of the Headteacher to ensure implementation and compliance by all relevant school staff.*

Cynnwys **Page**

1. Datganiad Polisi 4
2. Sgôp 4
3. Deddfwriaeth, Canllawiau a Pholisïau 5
4. Diffiniadau 6
5. Cyfrifoldebau 7
   5.1. Corff Llywodraethu'r Ysgol 7
   5.2. Y Pennaeth (ac/neu'r Person sy'n Gyfrifol am Ddiogelu Data yn yr Ysgol) 7
   5.3. Swyddog Diogelu Data Ysgolion 8
6. Pam bod gan yr ysgol CCTV 9
7. Sail Gyfreithiol dros Brosesu 9
8. Rheoli System 10
   8.1. Asesiad Effaith Diogelu Data (DPIA) 11
   8.2. Mynediad 11
9. Darllediadau CCTV 12
   9.1. Hysbysiadau 12
   9.2. Lleoliad y Camerâu 13
   9.3. Ymwelwyr 14
10. Gwyliadwriaeth Gudd 14
11. Storio a Chadw Offer a Data 15
12. Asesu'r System CCTV 15
13. Lawrlwytho Gweithdrefnau Ffilm 16
14. Ceisiadau gan Wrthrych y Data 17
    14.1. Delweddau o Unigolion Eraill / Trydydd Partïon 18
15. Mynediad at Ddelweddau a Datgelu Delweddau i Drydydd Partïon 18
16. Rhannu Delweddau CCTV â'r Heddlu 20
17. Prosesu Trydydd Parti 20
18. Technoleg Adnabod Wynebau Byw (LFR) 21
19. Hyfforddiant 21
20. Cwynion 21
21. Torri'r Polisi 22
22. Adolygu Trefniadau Polisi ac Arolygiaeth 22

ATODIAD A- Log System CCTV Ysgolion 45
ATODIAD B- Log Lleoliadau CCTV Ysgolion 51
ATODIAD C- Gweithdrefn CCTV yr Ysgol 52
ATODIAD D- Polisi CCTV Ysgolion- Rhestr Wirio'r Pennaeth 53

English Version **24**

1. Datganiad Polisi

Nod deddfwriaeth diogelu data yw diogelu preifatrwydd personol a hawliau unigolion y mae data yn cael ei gasglu, ei storio, ei brosesu neu ei gyflenwi yn eu cylch. Mae *Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR)* yn ei gwneud yn ofynnol i sefydliadau gael mesurau diogelwch technegol priodol ar waith i sicrhau bod data personol yn cael ei gadw'n ddiogel a'i ddiogelu rhag prosesu anawdurdodedig neu anghyfreithlon, ac yn erbyn colled, dinistr neu ddifrod damweiniol.

Mae casglu a/neu recordio delweddau o unigolion adnabyddadwy yn gyfystyr â phrosesu gwybodaeth bersonol ac felly mae angen cydymffurfio â'r egwyddorion diogelu data o dan *UK GDPR* a *Deddf Diogelu Data 2018.*

Mae'r ysgol yn defnyddio camerâu CCTV i fonitro gweithgareddau o fewn yr ysgol ac ar dir yr ysgol i nodi gweithgarwch troseddol sy'n digwydd, a ragwelir iddo ddigwydd neu a ganfuwyd ei fod wedi digwydd. Fe'i defnyddir hefyd er mwyn sicrhau diogelwch a lles y disgyblion a'r staff yn yr ysgol ynghyd â'i hymwelwyr a'r cyhoedd.

Mae'r polisi hwn yn manylu ar ddiben ac yn rheoleiddio'r gwaith o reoli, gweithredu a defnyddio'r system CCTV yn yr ysgol. Mae hefyd yn rhoi manylion am y gweithdrefnau i'w dilyn.

Diben y polisi hwn yw sicrhau:

- bod yr ysgol yn cydymffurfio â deddfwriaeth diogelu data, gan gynnwys *Deddf Diogelu Data 2018*; *Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR)* ac egwyddorion *Cod Ymarfer y Surveillance Camera Commissioner*;
- bod y delweddau sy'n cael eu tynnu yn cael eu defnyddio at y dibenion y mae'r ysgol yn gofyn amdanynt;
- y gall yr ysgol gysuro'r personau hynny y mae eu delweddau'n cael eu tynnu bod y delweddau'n cael eu trin yn unol â deddfwriaeth diogelu data.

Mae'r system yn cynnwys nifer o gamerâu gosodedig a dôm wedi'u lleoli o amgylch safle'r ysgol. Mae'r holl gamerâu gosodedig mewn golwg amlwg ar safle'r ysgol. Nid yw'r ysgol yn defnyddio CCTV fel mater o drefn i fonitro'n gudd neu i fonitro eiddo preifat y tu allan i dir yr ysgol, oni bai bod amgylchiadau eithriadol neu eithafol i wneud hynny.

Bydd yr ysgol yn trin y system, yr holl wybodaeth, dogfennau a recordiadau (y rhai a gafwyd a'r rhai a ddefnyddiwyd wedyn) fel data a ddiogelir o dan *UK GDPR* a *Deddf Diogelu Data 2018.*

Ni fydd deunyddiau na gwybodaeth a gafwyd o ganlyniad i CCTV yn cael eu defnyddio at unrhyw ddiben masnachol. Ni fydd delweddau byth yn cael eu rhyddhau i'r cyfryngau at ddibenion adloniant.

2. Sgôp

Mae'r polisi hwn yn berthnasol i bob aelod o staff yn yr ysgol sydd wedi'u hawdurdodi i gael mynediad i system CCTV yr ysgol.

Mae'r polisi hwn hefyd yn cyflwyno hysbysiad a chanllaw i wrthrychau data (gan gynnwys disgyblion, rhieni, staff, gwirfoddolwyr, ymwelwyr â'r ysgol ac aelodau o'r cyhoedd ac unrhyw bersonau eraill y gellir tynnu eu delweddau ar y system CCTV) ynghylch eu hawliau mewn perthynas â data personol a gofnodir drwy system CCTV yr ysgol.

Mae'r polisi hwn yn ymdrin â'r defnydd o systemau gwyliadwriaeth a CCTV sy'n dangos delweddau symudol a delweddau llonydd o bobl y gellid eu hadnabod, yn ogystal â gwybodaeth sy'n ymwneud ag unigolion at unrhyw un o'r dibenion canlynol:

- arsylwi beth mae unigolyn yn ei wneud;
- cymryd camau gweithredu i atal trosedd;
- defnyddio delweddau o unigolion y gall effeithio ar eu preifatrwydd.

Mae'r polisi hwn a'r gweithdrefnau sydd ynddo yn berthnasol i holl systemau CCTV yr ysgol gan gynnwys gwe-gamerâu, gosodiadau cudd ac unrhyw system arall sy'n tynnu delweddau o unigolion adnabyddadwy er mwyn gwylio a recordio gweithgareddau unigolion o'r fath.

Caiff delweddau CCTV eu monitro a'u cofnodi yn unol â'r polisi hwn.

3. Deddfwriaeth, Canllawiau a Pholisïau

Y brif ddeddfwriaeth diogelu data y mae'r polisi hwn yn cydymffurfio â hi yw *Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR)* a *Deddf Diogelu Data 2018.*

Mae deddfwriaeth berthnasol arall a gymerir i ystyriaeth o fewn y polisi hwn yn cynnwys:

- *Deddf Diogelu Rhyddidau 2012 (POFA);*
- *Deddf Hawliau Dynol 1998;*
- *Deddf Rheoleiddio Pwerau Ymchwilio 2000;*
- *Deddf Rhyddid Gwybodaeth 2000;*
- *Deddf Rheoleiddio Deddf Pwerau Ymchwilio 2000 (RIPA);*
- *Deddf Cyfiawnder Troseddol a Threfn Gyhoeddus 1994;*
- *Deddf Gweithdrefn ac Ymchwiliadau Troseddol 1996*

Mae'r polisi hwn hefyd yn seiliedig ar godau ymarfer perthnasol ac ar ganllawiau a gyhoeddwyd gan Swyddfa'r Comisiynydd Gwybodaeth (ICO)- *'Video Surveillance Guidance'* a *Chod Ymarfer y Surveillance Camera Commissioner,* yn enwedig y 12 egwyddor arweiniol. Bydd yr ysgol hefyd yn dilyn – *'In the picture: A data protection code of practice for surveillance cameras and personal information'* a'r *'Surveillance Camera Commissioner Buyers Toolkit'.*

Dylid darllen y polisi hwn hefyd ar y cyd â'r *Polisi Diogelu Data Ysgolion*; *Polisi Asesiad Effaith Diogelu Data Ysgolion; Polisi Diogelwch Gwybodaeth Ysgolion; Polisi*

Digwyddiadau Diogelwch Data Ysgolion; Polisi Cais gan Wrthrych y Data Ysgolion a *Gweithdrefn Rhannu Gwybodaeth gydag Awdurdodau Heddlu yn y Deyrnas Unedig Gwynedd a Môn*. Mae'r rhain i gyd ar gael ar y dudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

Dogfennau perthnasol sydd ar gael ar y dudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu:

- *Log Lleoliadau CCTV Ysgolion;*
- *Log System CCTV Ysgolion;*
- *Gweithdrefn CCTV yr Ysgol;*
- *Ffurflen Cais gan Wrthrych y Data Ysgolion;*
- *Ffurflen SA3 - Cais i sefydliad allanol am ddatgelu data personol i'r Heddlu.*

4. Diffiniadau

Data personol	Unrhyw wybodaeth ynglŷn ag unigolyn naturiol yr adnabyddir neu y gellir ei adnabod yn uniongyrchol neu'n anuniongyrchol drwy'r wybodaeth honno. Gellir ei storio'n ddigidol, ar gyfrifiadur, neu mewn systemau ffeilio ar bapur.
Data categori arbennig	Gwybodaeth ynglŷn â hil, tarddiad ethnig, barn wleidyddol, credoau crefyddol neu athronyddol, aelodaeth undeb llafur (neu ddiffyg aelodaeth), gwybodaeth enetig, gwybodaeth fiometreg (i adnabod unigolyn) unigolyn, a gwybodaeth ynglŷn ag iechyd, bywyd rhywiol neu ogwydd rhywiol unigolyn. Data categori arbennig yw data personol sydd angen amddiffyniad bellach oherwydd ei fod yn sensitif.
Prosesu Gwybodaeth	Casglu, derbyn, cofnodi, trefnu, strwythuro, storio, cadw, diwygio, addasu, newid, adennill, ymgynghori, lledaenu, cyfyngu, datgelu, dinistrio, cael gwared â gwybodaeth, ei defnyddio neu wneud unrhyw beth â hi.
Gwyliadwriaeth	Monitro symudiadau ac ymddygiad unigolion; gall hyn gynnwys fideo, sain neu ffilm fyw. At ddibenion y polisi hwn, dim ond fideos fydd yn berthnasol.
Gwyliadwriaeth Agored	Unrhyw ddefnydd o wyliadwriaeth nad yw ei hawdurdod yn dod o dan Ddeddf Rheoleiddio Pwerau Ymchwilio 2000.
Gwyliadwriaeth Gudd	Unrhyw ddefnydd o wyliadwriaeth nad yw'n cael ei rannu'n fwriadol â'r gwrthrychau y mae'n eu recordio. Ni fydd gwrthrychau'n cael gwybod am wyliadwriaeth o'r fath.
Technoleg Adnabod Wynebau Byw (LFR)	Mae technoleg adnabod wynebau byw (LFR), a elwir hefyd yn gydnabyddiaeth wyneb awtomatig, yn adnabod pobl mewn fideo mewn amser real, gan ddefnyddio set o ffotograffau fel cyfeiriad. Mae camerâu gwyliadwriaeth adnabod wynebau yn sganio'r holl wynebau y gallant eu gweld mewn torf i wirio hunaniaeth pobl yn erbyn cronfa ddata mewn amser real.
Systemau Gwybodaeth	Cyfrifiaduron prosesu gwybodaeth neu systemau cyfathrebu data.

Risg	Effaith ansicrwydd ar amcanion. Risgiau i unigolion: y potensial am ddifrod neu drallod. Nodweddir risg yn aml gan gyfeirio at "ddigwyddiadau" a "chanlyniadau" posibl, neu gyfuniad o'r rhain.
Effaith	Beth fyddai canlyniadau'r risg pe bai'n digwydd. Effaith yn cael ei ystyried fel un sy'n cael effaith uniongyrchol neu effaith yn y dyfodol.
Anawdurdodedig	Heb hawl cyfreithlon.
Amgryptio	Mae amgryptio data yn ddull diogelwch lle mae gwybodaeth yn cael ei hamgodio a dim ond defnyddiwr sydd â'r allwedd amgryptio gywir y gellir cael gafael ar neu ddadgryptio data. Mae data wedi'i amgryptio yn ymddangos wedi'i sgramblo neu'n annarllenadwy i berson neu endid sy'n cael mynediad heb ganiatâd.

5. Cyfrifoldebau

5.1. <u>Corff Llywodraethu'r Ysgol</u>
Mae corff llywodraethu'r ysgol yn gyfrifol am:

- sicrhau bod y polisi hwn wedi'i fabwysiadu'n ffurfiol gan yr ysgol;
- monitro cydymffurfiaeth ac atebolrwydd cyffredinol yr ysgol mewn perthynas â'r polisi hwn;
- sicrhau y gall yr ysgol dystiolaethu cydymffurfiaeth â deddfwriaeth diogelu data.

5.2. <u>Y Pennaeth (ac/neu'r Unigolyn sy'n Gyfrifol am Ddiogelu Data yn yr Ysgol)</u>
Mae'r Pennaeth ac/neu'r unigolyn sy'n gyfrifol am ddiogelu data yn yr ysgol yn gyfrifol am:

- sicrhau bod proses ar waith i fonitro cydymffurfiaeth yr ysgol â'r polisi hwn yn barhaus;
- sicrhau bod y defnydd o systemau CCTV yn cael ei weithredu yn unol â'r polisi hwn a'i fod yn cael ei brosesu'n gyfreithlon ac yn deg;
- sicrhau bod holl weithwyr yr ysgol yn ymwybodol o'r cyfyngiadau mewn perthynas â mynediad at ddelweddau a recordiwyd a'u datgeliad;
- gweithredu ac atebolrwydd cyffredinol ar gyfer sut mae'r ysgol yn defnyddio'r system CCTV;
- rheoli a gweithredu'r system CCTV yn gyffredinol o ddydd i ddydd, gan gynnwys gweithgareddau sy'n ymwneud â gosodiadau, cofnodi, adolygu, monitro a sicrhau cydymffurfiaeth â'r polisi hwn;
- ymgynghori â'r Swyddog Diogelu Data Ysgolion o ran prosesu gwyliadwriaeth a delweddau CCTV yn gyfreithlon;
- sicrhau bod y gwaith monitro CCTV yn gyson â'r safonau a'r amddiffyniadau uchaf;
- cynnal gwaith monitro perfformiad rheolaidd, gan gynnwys hapwiriadau gweithredu ar y system CCTV;
- sicrhau bod arwyddion digonol yn cael eu codi o amgylch yr ysgol yn unol â *Chod Ymarfer y Surveillance Camera Commissioner;*

- sicrhau bod y *Log Lleoliadau CCTV Ysgolion* wedi'i gwblhau a'i fod yn cael ei ddiweddaru;
- sicrhau bod y ddogfen *Gweithdrefn CCTV yr Ysgol* wedi'i gwblhau a'i fod yn cael ei ddiweddaru;
- cadw cofnod o fynediad (e.e. cofnod systemau) i neu ryddhad o unrhyw ddeunydd a gofnodir neu a gedwir yn y system;
- sicrhau y glynir wrth gyfnodau cadw penodol ac ystyried pwy sy'n cael mynediad i ddelweddau CCTV a pham;
- sicrhau bod delweddau a recordir yn cael eu storio am gyfnod heb fod yn hwy na 30 diwrnod ac yna'n cael eu dileu oni bai bod hynny'n ofynnol fel rhan o ymchwiliad troseddol neu achos llys (troseddol neu sifil);
- sicrhau bod gwyliadwriaeth a delweddau CCTV yn cael eu dinistrio yn unol â gofynion cyfreithiol pan fyddant y tu allan i'w cyfnodau cadw;
- sicrhau bod y perimedr golwg o gamerâu lleoliad sefydlog yn cydymffurfio â'r polisi hwn yn fewnol ac yn allanol;
- sicrhau nad yw camerâu allanol yn ymwthiol o ran eu safleoedd a'u golwg o dai preswyl cyfagos ac yn cydymffurfio â'r egwyddor o "ddisgwyliad rhesymol o breifatrwydd";
- sicrhau bod ffilm monitro yn cael ei storio mewn man diogel gyda mynediad gan staff awdurdodedig yn unig;
- sicrhau bod mesurau seiberddiogelwch cadarn ar waith i ddiogelu data a gedwir ar y system;
- sicrhau bod rheoli camerâu yn monitro ymddygiad amheus, difrod troseddol ac ati yn unig ac nad yw'n monitro nodweddion unigol;
- cadw cofnodion cynhwysfawr a chywir o'r holl weithgareddau prosesu data, gan gynnwys gwyliadwriaeth a delweddau CCTV a manylu ar ddiben y gweithgaredd o fewn ROPA yr ysgol;
- sicrhau bod staff sydd â mynediad i system CCTV yr ysgol yn cael hyfforddiant digonol i sicrhau dealltwriaeth lawn o'r system ac i gadw cofnodion o fanylion yr hyfforddiant;
- rheoli unrhyw gwynion ynglŷn â'r system CCTV gan gynnwys ystyried adborth/cwynion disgyblion a staff ynghylch ymosodiad posibl ar breifatrwydd neu gyfrinachedd oherwydd lleoliad camera CCTV penodol neu offer cysylltiedig.

5.3. <u>Swyddog Diogelu Data Ysgolion</u>

Mae'r Swyddog Diogelu Data Ysgolion yn gyfrifol am:

- ddarparu trosolwg annibynnol o faterion cydymffurfiaeth;
- sicrhau bod yr ysgol yn prosesu ac yn delio â gwyliadwriaeth a ffilm CCTV yn unol â deddfwriaeth diogelu data;
- monitro deddfwriaeth i sicrhau bod yr ysgol yn defnyddio gwyliadwriaeth yn deg ac yn gyfreithlon;
- monitro bod gwyliadwriaeth a ffilm CCTV yn cael eu dinistrio gan yr ysgol yn unol â gofynion cyfreithiol pan maent yn disgyn y tu allan i'w cyfnodau cadw;
- cydlynu ceisiadau mynediad am ddata a ddelir ar systemau CCTV;

- darparu cyngor a chymorth pan ofynnir amdanynt a chynghori a chynorthwyo gyda chwynion a gweithrediad offer;
- darparu arweiniad a chefnogaeth gyda chwblhau Asesiad Effaith Diogelu Data (DPIA) lle bo angen a monitro perfformiad DPIA yr ysgol;
- monitro effaith defnyddio offer CCTV ar breifatrwydd;
- darparu cymorth gyda chreu unrhyw gytundebau prosesu data ar gyfer proseswyr data.

6. Pam bod gan yr ysgol CCTV

Mae defnydd o'r system CCTV yn yr ysgol ar gyfer:

- amddiffyn a chynnal lles a llesiant disgyblion, staff, ymwelwyr a'r cyhoedd;
- hyrwyddo iechyd a diogelwch disgyblion, staff, ymwelwyr a'r cyhoedd;
- cynnal amgylchedd diogel;
- cynyddu diogelwch personol a lleihau ofn troseddu;
- atal a lleihau'r nifer o ddigwyddiadau bwlio ac ymddygiad gwrthgymdeithasol (gan gynnwys lladrad a fandaliaeth);
- atal gweithredoedd troseddol yn erbyn unigolion ac eiddo;
- diogelu adeiladau, asedau, eiddo ac offer yr ysgol yn ystod ac ar ôl oriau ysgol;
- diogelu eiddo personol disgyblion, staff ac ymwelwyr rhag colled neu ddifrod;
- cynorthwyo staff i adnabod a datrys digwyddiadau;
- monitro diogelwch a chyfanrwydd y safle ysgol a danfoniadau a chyraeddiadau, gan gynnwys parcio ceir;
- sicrhau bod y rheolau ysgol yn cael eu parchu fel y gellir rheoli'r ysgol yn briodol;
- cefnogi'r Heddlu a'r gymuned i rwystro, atal, lleihau, darganfod ac ymchwilio i droseddau;
- cynorthwyo i adnabod, dal a chosbi'r sawl sydd wedi cyflawni trosedd;
- ei ddefnyddio fel tystiolaeth yn ystod gweithdrefnau disgyblaeth a chwynion lle bo angen a lle mae'n briodol i wneud hynny.

7. Sail Gyfreithiol dros Brosesu

Defnyddir camerâu i fonitro gweithgareddau yn yr ysgol; ei meysydd parcio a mannau cyhoeddus eraill er mwyn adnabod gweithgarwch neu ymddygiad droseddol bosibl neu wirioneddol nad yw'n cydymffurfio â chodau ymddygiad yr ysgol ac er mwyn diogelu lles a diogelwch disgyblion, ymwelwyr a'r cyhoedd.

Ystyrir bod prosesu yn rhan o dasg gyhoeddus yr ysgol felly ystyrir mai'r sail gyfreithlon ar gyfer prosesu yw:

- *Erthygl 6(1)(e) mae prosesu yn angenrheidiol er mwyn cyflawni tasg a gyflawnir er budd y cyhoedd neu wrth arfer awdurdod swyddogol a freiniwyd yn y rheolydd.*

Bydd yr ysgol yn sicrhau ei bod:

- yn prosesu gwyliadwriaeth a ffilm CCTV yn gyfreithlon ac yn deg;

- yn casglu gwyliadwriaeth a ffilm CCTV am resymau cyfreithlon; ei fod ond yn cael ei ddefnyddio at y dibenion y bwriedir ei ddefnyddio a'i fod yn cael ei ddefnyddio'n unol â hynny;
- yn casglu gwyliadwriaeth a ffilm CCTV sy'n berthnasol ac yn ddigonol heb fod yn ormodol o ran y rheswm dros ei gasglu;
- yn dylunio'r system i ystyried ei heffaith ar unigolion a'u preifatrwydd a'u data personol;
- wedi rhoi polisïau a gweithdrefnau ar waith sy'n cael eu cyfathrebu drwy'r ysgol;
- yn ystyried yr holl safonau gweithredol, technegol a chymhwysedd sy'n berthnasol i'r gwyliadwriaeth a'r system CCTV a'i phwrpas, a gweithio i gwrdd â'r safonau hynny a'u cynnal yn unol â'r gyfraith;
- â gweithdrefnau cyfrifoldeb ac atebolrwydd clir ar gyfer delweddau a gwybodaeth sy'n cael eu casglu, eu cadw a'u defnyddio;
- yn cyfyngu ar fynediad at ddelweddau a gwybodaeth a gadwir gyda rheolau clir ar bwy sydd â hawl i gael mynediad atynt;
- yn sicrhau nad yw unrhyw wyliadwriaeth na delweddau CCTV sy'n adnabod unigolyn yn cael ei gadw yn hirach na bod angen;
- yn diogelu ffilm sy'n cynnwys data personol yn erbyn dinistriad, addasiad, datgeliad a mynediad anawdurdodedig yn ddamweiniol ac yn anghyfreithlon;
- yn dryloyw ac yn cynnwys pwynt cyswllt lle gall pobl gael mynediad at wybodaeth a cyflwyno cwynion;
- yn ymgymryd ag adolygiadau ac archwiliadau rheolaidd i sicrhau bod polisiau a safonau'n cael eu cynnal.

Gall camddefnydd o system CCTV fod yn drosedd.

Gall datgeliadau anawdurdodedig achosi niwed a gofid i unigolion, a gallant arwain at yr ICO yn cymryd camau gorfodi. Gall cyfreithiau eraill sy'n canolbwyntio ar enllib, aflonyddu, cyfathrebu maleisus neu ymddygiad bygythiol hefyd fod yn berthnasol mewn rhai amgylchiadau.

8. Rheoli System

Caiff y system CCTV ei pherchnogi, ei gweithredu, ei gweinyddu a'i rheoli gan yr ysgol. Yr ysgol yw'r rheolydd data ar gyfer y delweddau a gynhyrchir gan y system CCTV. Mae'r holl gamerau yn cael eu monitro o fewn yr ysgol neu gan gwmni monitro mae'r ysgol yn ei enwebu.

Mae'n bwysig bod datgeliad a mynediad at y delweddau a recordir gan wyliadwriaeth a ffilm CCTV yn cael eu cyfyngu a'u rheoli'n ofalus, nid yn unig i sicrhau bod hawliau unigolion yn cael eu cadw, ond hefyd i sicrhau bod y gadwyn dystiolaeth yn parhau'n gyfan, pe bai angen y delweddau at ddibenion tystiolaethol.

Dylai'r Pennaeth gwblhau'r ddogfen *Gweithdrefn CCTV yr Ysgol* (ATODIAD A) sydd yn rhoi manylion ar sut mae'r system yn cael ei reoli. Mae hwn ar gael ar y dudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu hefyd.

8.1. Asesiad Effaith Diogelu Data (DPIA)

Pan fydd systemau neu gamerâu CCTV newydd am eu gosod, bydd yr ysgol yn cynnal Asesiad Effaith Diogelu Data (DPIA) sy'n nodi risgiau sy'n gysylltiedig â gosod a sicrhau cydymffurfiaeth lawn â deddfwriaeth diogelu data mewn ymgynghoriad â'r Swyddog Diogelu Data Ysgolion. Gall hyn hefyd olygu bod angen ymgynghori â staff, rhieni a chyrff perthnasol eraill.

Bydd DPIA yn cael ei gynnal cyn gosod unrhyw system wyliadwriaeth a CCTV. Os bydd y DPIA yn datgelu unrhyw risgiau diogelwch posibl neu faterion diogelu data eraill, bydd yr ysgol yn sicrhau bod darpariaethau digonol ar waith i oresgyn y materion hyn.

Pan fydd yr ysgol yn nodi risg uchel i fuddiannau unigolyn na ellir ei goresgyn, bydd yr ysgol yn ymgynghori â'r ICO cyn defnyddio'r system CCTV, a bydd yr ysgol yn gweithredu ar gyngor yr ICO.

Bydd yr ysgol yn sicrhau y bydd gosod y systemau gwyliadwriaeth a CCTV bob amser yn cyfiawnhau ei dulliau. Os yw'r defnydd o system wyliadwriaeth a theledu cylch cyfyng yn rhy ymwthiol o ran preifatrwydd, bydd yr ysgol yn ceisio darpariaeth amgen.

Bydd y defnydd o'r system CCTV yn cael ei gynnal mewn modd proffesiynol, moesegol a chyfreithiol ac mae unrhyw wyriad o'r defnydd o dechnolegau diogelwch CCTV at ddibenion eraill yn cael ei wahardd gan y polisi hwn.

Os yw'r systemau gwyliadwriaeth a CCTV yn cyflawni eu diben ac nad oes eu hangen mwyach, bydd yr ysgol yn eu dadactifadu. Bydd unrhyw gamerâu sy'n dangos diffygion yn cael eu hatgyweirio ar unwaith er mwyn osgoi unrhyw risg o ddigwyddiad diogelwch data.

Bydd y defnydd o CCTV a'r Asesiad Effaith Diogelu Data (DPIA) sy'n ymwneud ag ef yn cael eu hadolygu'n rheolaidd er mwyn sicrhau bod eu gweithrediad yn parhau i fod yn angenrheidiol ac yn gymesur wrth gyflawni'r dibenion a nodwyd.

Bydd yr ysgol yn cydymffurfio â’r *Polisi Asesiad Effaith Diogelu Data Ysgolion (DPIA).*

8.2. Mynediad

Bydd y Pennaeth yn gyfrifol am reoli'r system CCTV o ddydd i ddydd. Cyfrifoldeb y Pennaeth yw goruchwylio mynediad a chynnal a chadw'r system CCTV.

Gall y Pennaeth ddirprwyo'r gwaith o weinyddu'r system CCTV i aelod arall o staff. Dim ond y Pennaeth fel Rheolwr y System neu weithwyr awdurdodedig eraill yr ysgol sydd angen mynediad at y data fydd yn cael mynediad at y system CCTV a’r data a gesglir. Bydd y Pennaeth yn ystyried pwy sy'n cael mynediad i'r ffilm hon a pham. Bydd mynediad i ddelweddau wedi'u recordio yn cael ei gyfyngu i'r staff hynny sydd wedi'u hawdurdodi i'w gweld, ac ni fydd ar gael yn ehangach.

Dim ond i bersonau awdurdodedig, o dan oruchwyliaeth y Pennaeth, y rhoddir mynediad i systemau cofnodi a delweddau CCTV a gedwir, yn unol â'r amcanion a bennwyd gan yr ysgol neu os oes rhyw reswm arall a chyfreithlon dros roi mynediad o'r fath. Bydd

systemau cofnodi yn cael eu diogelu gan fesurau diogelwch priodol megis diogelu cyfrinair fel mesur diogelwch ychwanegol.

Bydd log systemau yn cael ei gadw gan yr ysgol, gan nodi pwy a ddefnyddiodd y recordiadau/delweddau, ar ba ddyddiadau ac amseroedd, ac at ba ddibenion. Dylid defnyddio templed *Log System CCTV Ysgolion* (ATODIAD A). Mae hwn hefyd ar gael ar y dudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

Bydd delweddau'n cael eu gweld a/neu eu monitro mewn ardal ddiogel, gyfyngedig a phreifat addas er mwyn lleihau'r tebygolrwydd o bersonau anawdurdodedig yn cael mynediad atynt neu'n cael cyfle i gael mynediad atynt. Mae monitorau arddangos gweledol wedi'u lleoli mewn ardal ddynodedig ac ni ddylai unrhyw un nad yw'n berson awdurdodedig eu gweld neu allu eu gweld. Ni ddylid caniatáu i weithwyr eraill yr ysgol a disgyblion gael mynediad i'r ardal honno pan fydd gwylio'n digwydd.

Mae'r holl weithredwyr awdurdodedig a staff ysgol sydd â mynediad i ddelweddau CCTV yn ymwybodol o'r gweithdrefnau y mae angen eu dilyn wrth gael gafael ar y delweddau a recordiwyd. Mae holl staff yr ysgol yn ymwybodol o'r cyfyngiadau mewn perthynas â mynediad i ddelweddau wedi'u recordio a'u datgelu, a dim ond mewn ffordd sy'n gyson â'r dibenion a'r gweithdrefnau y bydd yn cael eu hawdurdodi i ddefnyddio'r system CCTV.

Dan rhai amgylchiadau, gall unigolion eraill hefyd weld y recordiadau er mwyn cyflawni'r amcanion yr amlinellir uchod. Pan fydd recordiadau CCTV yn cael eu gweld, bydd mynediad yn cael ei gyfyngu i unigolion awdurdodedig ar sail pwy sydd angen gwybod.

Gellir datgelu delweddau a recordir i lywodraethwyr ysgol fel rhan o broses disgyblaethu, gweithdrefn gwyno neu gwyn mewnol os yw'n briodol.

Bydd ceisiadau a dderbynnir gan gyrff allanol (e.e. cyfreithwyr, Heddlu) i weld neu ryddhau delweddau yn cael eu cyfeirio i'r Swyddog Diogelu Data Ysgolion yn y lle cyntaf.

Bydd angen i'r ysgol hefyd sicrhau bod mesurau diogelwch seiber cadarn ar waith i ddiogelu'r data a gadwir yn y system.

9. Darllediadau CCTV

9.1. <u>Hysbysiadau</u>

Mae'n rhaid i'r ysgol hysbysu staff, disgyblion, ymwelwyr ac aelodau o'r cyhoedd eu bod yn mynd i mewn i ardal sydd â gwyliadwriaeth CCTV a nodi pam ei bod yn casglu gwybodaeth bersonol ar ffurf delweddau CCTV. Cynhwysir hyn yn *Hysbysiadau Preifatrwydd* yr ysgol.

Dylid arddangos hysbysiadau sy'n hysbysu pobl bod CCTV ar waith mewn lleoliad clir ym mhob ardal sy'n cael ei ffilmio fel sy'n ofynnol dan *God Ymarfer y Surveillance Camera Commissioner.*

Bydd defnyddio arwyddion sydd wedi eu harddangos yn glir ym mhrif fynedfeydd allanol yr ysgol ac yna arwyddion pellach yn yr ardaloedd ac mewn mannau rheoledig yn hysbysu pobl eu bod mewn ardal lle mae system wyliadwriaeth ar waith.

Bydd lleoliadau priodol ar gyfer arwyddion yn cynnwys mynedfeydd i safleoedd ar gyfer cerddwyr a cherbydau h.y. drysau allanol, gatiau ysgol; derbynfa ac yn agos at bob camera mewnol. Dylai'r arwyddion fod yn glir ac yn ddarllenadwy.

Dylai'r arwyddion gynnwys yr wybodaeth ganlynol:

- hunaniaeth yr unigolyn neu’r sefydliad sy’n gyfrifol am y system CCTV;
- pwrpas y system CCTV;
- manylion ynglŷn â gyda phwy i gysylltu ynglŷn â’r system CCTV;
- unrhyw wybodaeth arall y gall ddod yn ofyniad statudol.

9.2. <u>Lleoliad y Camerâu</u>
Bydd lleoliad y camerâu CCTV yn cael ei ddewis gyda gofal mawr ac ni fyddant yn cael eu gosod mewn mannau lle byddai gan unigolion ddisgwyliad rhesymol o breifatrwydd (fel ystafelloedd newid a thoiledau). Cymerir gofal i sicrhau nad yw disgwyliadau preifatrwydd rhesymol yn cael eu torri. Bydd yr ysgol yn sicrhau bod lleoliad yr offer yn cael ei ystyried yn ofalus i sicrhau ei fod ond yn cipio delweddau sy'n berthnasol i'r dibenion y caiff ei osod ar ei gyfer ac yn cydymffurfio â deddfwriaeth diogelu data.

Oni bai bod angen ymateb ar unwaith i ddigwyddiadau, bydd camerâu CCTV ar safle'r ysgol yn cael eu gosod mewn man sefydlog ac ni fyddant yn cael eu cyfeirio, eu cylchdroi na'u pwyntio ar unigolion penodol, eu heiddo neu grŵp penodol o unigolion neu ddigwyddiadau. Dim ond yn y fath fodd fel ei fod ond yn monitro'r mannau hynny y bwriedir i'r offer eu gorchuddio y bydd yr holl offer CCTV o'r fath a osodir yn yr ysgol yn cael ei leoli. Bydd y system CCTV yn cael ei defnyddio i arsylwi eiddo'r ysgol er mwyn adnabod digwyddiadau sydd angen ymateb.

Bydd yr ysgol yn sicrhau hyd eithaf ei gallu nad oes unrhyw recordiadau (neu ddim ond ychydig iawn) o bobl sy’n mynd heibio neu eiddo preifat person arall. Ni fydd y system wyliadwriaeth yn cael ei phwyntio ar gerbydau preifat nac eiddo y tu allan i berimedr yr ysgol.

O fewn adeiladau'r ysgol, mae'r ddarpariaeth CCTV mewn coridorau, mannau grisiau, mannau mynediad, ardaloedd cyhoeddus, cymunedol a chymdeithasol. Nid yw’r system yn gallu recordio sain.

Ni fydd y system yn recordio unrhyw sain a bydd yr ysgol yn diffodd yn ddiofyn unrhyw allu i recordio sain.

Ni fydd CCTV yn cael ei ddefnyddio mewn ystafelloedd dosbarth oni bai bod gwyliadwriaeth gudd yn **gwbl angenrheidiol.**

Bydd yr ysgol yn cadw cofnod sy'n rhoi manylion am leoliad gwahanol gamerâu a'r hyn a gaiff ei gipio gan y camera o fewn yr ardal honno yn yr ysgol drwy'r *Log Lleoliadau CCTV*

Ysgolion (ATODIAD B). Mae hwn hefyd ar gael ar y dudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

Bydd y system CCTV yn cael ei gweithredu 24 awr y dydd, bob dydd o'r flwyddyn. Yn ystod cyfnodau o gau'r ysgol, efallai y bydd gan y Pennaeth neu aelodau eraill o staff enwebedig fynediad o bell diogel i ddelweddau byw a delweddau wedi'u recordio.

Mae'r system wyliadwriaeth wedi'i chynllunio a'i gosod ar gyfer yr effeithiolrwydd a'r effeithlonrwydd mwyaf posibl, fodd bynnag, ni all yr ysgol warantu y bydd y system yn cwmpasu neu'n canfod pob un digwyddiad sy'n digwydd yn y meysydd dan wyliadwriaeth a gall 'mannau dall' fodoli.

Bydd gan aelodau o staff yr ysgol fynediad i fanylion ynglŷn â lle mae camerâu CCTV wedi'u lleoli, ac eithrio camerâu a osodir at ddiben monitro cudd.

9.3. Ymwelwyr

Bydd manylion POB ymweliad ac ymwelydd â'r ysgol yn cael eu cofnodi yn llyfr ymwelwyr yr ysgol neu drwy system arwyddo electronig, gan gynnwys yr amser mynediad. Bydd hyn yn cefnogi'r ysgol i adnabod unigolion.

10. Gwyliadwriaeth Gudd

Gwyliadwriaeth gudd yw'r defnydd o wyliadwriaeth nad yw'n cael ei rhannu'n fwriadol â'r gwrthrychau y mae'n eu recordio. Mae gwrthrychau'n cael eu recordio heb eu gwybodaeth. Mae enghreifftiau o wyliadwriaeth gudd yn cynnwys ffilmio rhywun yr amheuir ei fod yn cyflawni gweithgareddau anghyfreithlon neu dwyllodrus fel dwyn neu ffilmio rhywun lle mae amheuaeth o gam-drin, trais neu niwed fel y gellir casglu gwybodaeth a/neu dystiolaeth ar gyfer ymchwiliad.

Nid yw'r ysgol yn cydoddef y defnydd o wyliadwriaeth gudd wrth fonitro staff, disgyblion a/neu wirfoddolwyr yr ysgol. Bydd gwyliadwriaeth gudd yn cael ei chyfyngu i achlysuron prin a dim ond mewn **amgylchiadau eithriadol neu eithafol** y bydd yn weithredol, er enghraifft:

- lle mae achos da dros amau bod camau anghyfreithlon neu anawdurdodedig yn digwydd, neu lle mae sail i amau camymddygiad difrifol;
- lle byddai hysbysu'r unigolion am y monitro yn amharu'n ddifrifol ar y rheswm dros wneud y recordiad.

Bydd cais am ddefnyddio camerâu cudd yn nodi'n glir y diben a'r rhesymau dros eu defnyddio. Rhaid gofyn a chael awdurdodiad gan yr Uwch Dîm Rheoli'r Gwasanaeth Dysgu a Swyddog Awdurdodi yng Nghyngor Sir Ynys Môn yn unol â *Deddf Rheoleiddio Pwerau Ymchwilio 2000* cyn cychwyn.

Gall gwyliadwriaeth gudd a gynhelir gan staff yr ysgol heb fath o awdurdod gan Uwch Dîm Rheoli'r Gwasanaeth Dysgu fod yn destun camau disgyblu.

Dylai Uwch Dîm Rheoli'r Gwasanaeth Dysgu fod yn fodlon bod yr holl ddulliau atal corfforol eraill wedi'u disbyddu cyn defnyddio recordio cudd.

Bydd yr holl waith monitro o'r fath yn cael ei ddogfennu'n llawn a dim ond am gyfnod cyfyngedig a rhesymol y bydd yn digwydd.

Rhaid i fonitro cudd ddod i ben ar ôl cwblhau ymchwiliad. Ni fydd camerâu sydd wedi'u gosod at ddibenion monitro cudd yn cael eu defnyddio mewn ardaloedd y disgwylir yn rhesymol iddynt fod yn breifat, er enghraifft ciwbiclau toiled, ardaloedd newid ac ati.

11. Storio a Chadw Offer a Data

Bydd ffilm wedi’i recordio a'r offer monitro yn cael eu storio'n ddiogel mewn ardal gyfyngedig. Ni chaniateir mynediad heb awdurdod i'r ardal honno ar unrhyw adeg. Bydd mynediad i'r system CCTV a delweddau wedi'u storio yn cael ei gyfyngu i ddefnyddwyr awdurdodedig yn unig a bydd yr ardal dan glo pan nad yw'r defnyddwyr awdurdodedig yn ei meddiannu. Bydd mynediad i'r system wyliadwriaeth, meddalwedd a data yn cael ei gyfyngu'n llym i ddefnyddwyr awdurdodedig a byddant yn cael eu diogelu gan gyfrinair.

Ni fydd data a recordir yn cael ei gadw am fwy o amser nag sy'n angenrheidiol. Er eu bod yn cael eu cadw, bydd cyfanrwydd y recordiadau'n cael ei gynnal i sicrhau eu gwerth tystiolaethol ac i ddiogelu hawliau'r bobl y mae eu delweddau wedi'u recordio.

Pan gedwir data o'r fath, caiff ei gadw yn unol â deddfwriaeth diogelu data. Bydd gwybodaeth gan gynnwys dyddiad, amser a hyd y recordiad, yn ogystal â'r lleoliadau a gwmpesir a grwpiau neu unigolion a recordir, yn cael eu cofnodi yn y log systemau. Unwaith y bydd y cyfnod cadw wedi dod i ben, dylid tynnu neu ddileu'r delweddau.

Fel arfer, bydd data a recordir yn cael ei gadw am o leiaf bythefnos ond am uchafswm o 30 diwrnod, ac eithrio pan fo'r ddelwedd yn nodi mater sy'n golygu bod angen echdynnu a chadw'r darn hwnnw o dystiolaeth neu ei fod yn cael ei gadw'n benodol yng nghyd-destun ymchwiliad/erlyniad i'r mater hwnnw. Gall delweddau/recordiadau CCTV ddal materion fel ymddygiad troseddol neu risg i iechyd a diogelwch ac efallai y bydd angen cadw'r delweddau/recordiadau CCTV i ymchwilio i'r mater hwnnw. Gall y ffilm fod yn ofynnol yn gyfreithlon gan drydydd parti priodol fel yr Heddlu neu'r Awdurdod Lleol.

Oni bai bod angen data at y dibenion uchod gan yr ysgol neu gyrff ymchwilio, bydd data'n cael ei drosysgrifo'n awtomatig neu â llaw neu’n cael ei ddileu'n ddiogel. Bydd unrhyw luniau diangen a gaiff eu cipio’n cael eu dileu'n ddiogel o'r system ysgolion. Os bydd angen at ddibenion ymchwilio, bydd data'n cael ei ddinistrio cyn gynted ag nad oes ei angen mwyach.

12. Asesu’r System CCTV

Bydd y Pennaeth yn gwirio ac yn cadarnhau effeithlonrwydd y system bob dydd ac yn benodol bod yr offer yn recordio’n iawn; bod camerâu'n weithredol ac yn gweithredu'n effeithiol. Dylai'r camerâu a osodwyd ddarparu delweddau sydd o ansawdd addas at y dibenion penodedig y maent wedi'u gosod ar eu cyfer.

Gwneir gwiriadau i sicrhau cywirdeb unrhyw nodweddion megis lleoliad y camera a/neu gyfeiriad dyddiad ac amser. Os canfyddir nad yw'r amser/dyddiad ac ati yn gyson â'r amser/dyddiad presennol, bydd y Pennaeth yn cymryd camau i gywiro'r gwall. Bydd nodyn o newidiadau o'r fath yn cael ei gofnodi yn y log systemau.

Bydd camerâu'n cael eu cynnal a'u gwasanaethu'n briodol er mwyn sicrhau bod delweddau clir yn cael eu recordio. Bydd y system yn cael ei gwirio a bydd gwasanaethu'n cael ei gynnal o leiaf bob blwyddyn.

Mae unrhyw ddiweddariadau meddalwedd (yn enwedig diweddariadau diogelwch) y mae angen eu gwneud i'r system neu unrhyw ddyfeisiau eraill sy'n gysylltiedig â hi a gyhoeddir gan wneuthurwr yr offer, yn cael eu gwneud ar unwaith.

Dylid diogelu camerâu rhag fandaliaeth er mwyn sicrhau eu bod yn parhau i weithio.

Efallai yr hoffai'r corff llywodraethu dderbyn adroddiad blynyddol ar berfformiad a blaenoriaethau'r system gan gynnwys trosolwg byr o wiriadau a mesurau diogelwch, canmoliaeth a chwynion, ceisiadau am ddatgeliad ac ati.

13. Lawrlwytho Gweithdrefnau Ffilm

Er mwyn cynnal a chadw uniondeb y data (a sicrhau ei fod yn dderbyniol mewn unrhyw achos cyfreithiol), rhaid paratoi unrhyw ffilm lawrlwytho a ddefnyddiwyd i recordio digwyddiadau o'r gyriant caled yn unol â'r gweithdrefnau canlynol:

- rhaid i bob ffilm lawrlwytho gael ei adnabod gan farc unigryw;
- cyn ei ddefnyddio, rhaid glanhau pob ffilm lawrlwytho o unrhyw recordiad blaenorol;
- bydd y Pennaeth yn cofrestru dyddiad ac amser mewnosod ffilm lawrlwytho, gan gynnwys ei gyfeirnod;
- rhaid i'r ffilm sy'n ofynnol at ddibenion tystiolaethol gael ei selio, ei weld a'i lofnodi gan Gadeirydd y Llywodraethwyr a'r Pennaeth, ac yna ei ddyddio a'i storio mewn storfa dystiolaeth ddiogel ar wahân. Os na chaiff ffilm lawrlwytho ei gopïo ar gyfer yr Heddlu cyn iddo gael ei selio, gellir gwneud copi yn ddiweddarach ar yr amod ei fod wedyn yn cael ei ail-selio, ei dystio a'i lofnodi gan Gadeirydd y Llywodraethwyr a'r Pennaeth, yna ei ddyddio a'i ddychwelyd i'r storfa dystiolaeth.

Os caiff lluniau lawrlwytho eu harchifo, rhaid nodi'r cyfeirnod. Bydd ffilm lawrlwytho'n cael ei fynegeio, ei storio a'i ddinistrio'n briodol ar ôl ei ddefnyddio'n briodol, yn unol â'r ddeddfwriaeth diogelu data a'r cyfnodau cadw.

Wrth gyrchu a gwylio delweddau, rhaid i ddau aelod o staff awdurdodedig fod yn bresennol (un ohonynt yn ddelfrydol yw'r Pennaeth). Bydd cofnod ysgrifenedig o fynediad yn cael ei gadw drwy log systemau. Cedwir cofnodion mynediad a byddant yn dogfennu'r canlynol:

- dyddiad ac amser eu hechdynnu;
- enw'r person sy'n echdynnu'r delweddau;

- enw(au) y person(au) a'r sefydliad y maent yn ei gynrychioli yn edrych ar y delweddau;
- y rheswm dros y gwylio;
- sut yr ymdriniwyd â'r cais;
- canlyniad, os o gwbl, y gwylio;
- y dyddiad a'r amser y dychwelwyd y delweddau i'r system; neu
- lle diogel, os ydynt wedi'u cadw at ddibenion tystiolaethol.

Bydd data yn cael ei ddarparu mewn fformat parhaol lle bo’n bosibl. Os nad yw hyn yn bosibl, bydd yr unigolyn yn cael cyfle i weld y ffilm.

Dylid amgryptio recordiadau sydd wedi eu hechdynnu i ddiogelu’r ffilm.

14. Ceisiadau gan Wrthrych y Data

Mae gan unigolion yr hawl i ofyn am fynediad i'r data personol sydd gan yr ysgol arnynt mewn perthynas â hwy eu hunain ac i ddilysu cyfreithlondeb y prosesu o dan ddeddfwriaeth diogelu data. Mae hyn yn cynnwys gwybodaeth a gedwir ar y system CCTV, os yw wedi'i chadw. Bydd yn rhaid i'r ysgol sicrhau y gall roi copïau i unigolion o ddelweddau'r unigolyn hwnnw a gasglwyd gan y system CCTV cyn belled ag y bo'n rhesymol ymarferol. Mae'r hawl hon yn amodol ar rai eithriadau rhag mynediad, gan gynnwys mewn rhai amgylchiadau, lle gellir adnabod eraill.

Gofynnir i unigolion sy'n cyflwyno ceisiadau am fynediad gwblhau’r *Ffurflen Cais gan Wrthrych y Data Ysgolion* ac i ddarparu digon o wybodaeth a manylion penodol i alluogi adnabod y ffilm sy'n ymwneud â hwy, er enghraifft, dyddiad, amser a lleoliad y recordiad.

Gofynnir am dystiolaeth ffotograffig o hunaniaeth a/neu ddisgrifiad manwl i ganiatáu ar gyfer adnabod. Rhaid i'r ysgol fodloni ei hun o hunaniaeth unrhyw berson sy'n dymuno gweld delweddau neu gael mynediad i'r system a dilysrwydd y cais. Lle mae unrhyw amheuaeth, gwrthodir mynediad.

Wrth roi copi o'i ddata i'r person, gall yr ysgol ddarparu llun llonydd/cyfres o luniau llonydd, tâp neu ddisg gyda delweddau perthnasol. Os mai dim ond yr unigolyn sy'n gwneud y cais sydd i’w weld yn y ffilm, yna gellir caniatáu i'r unigolyn weld y ffilm.

Bydd copi o'r wybodaeth yn cael ei roi i'r unigolyn yn ddi-dâl; fodd bynnag, gall yr ysgol osod 'ffi resymol' i gydymffurfio â cheisiadau am gopïau pellach o'r un wybodaeth.

Mae gan yr ysgol hawl i wrthod mynediad i ffilm CCTV lle byddai hyn yn amharu ar hawliau cyfreithiol unigolion eraill neu'n peryglu ymchwiliad parhaus.

Os nad yw'r ysgol yn gallu cydymffurfio â chais gan wrthrych y data heb ddatgelu data personol unigolyn arall yr adnabyddir neu y gellir ei adnabod o'r wybodaeth honno, nid yw'n ofynnol iddi gydymffurfio â'r cais oni bai ei fod wedi'i fodloni bod yr unigolyn wedi rhoi ei gydsyniad datganedig i'r datgeliad, neu os yw'n rhesymol, gan roi sylw i'r amgylchiadau, i gydymffurfio heb gydsyniad yr unigolyn.

Bydd yr ysgol yn cydymffurfio â'r *Polisi Cais gan Wrthrych y Data Ysgolion* a bydd y Swyddog Diogelu Data Ysgolion yn rhoi cyngor ac arweiniad i'r ysgol a gall hwyluso a chefnogi'r gwaith o baratoi ymateb i'r cais.

Mae'r *Ffurflen Cais gan Wrthrych y Data Ysgolion* ar gael ar y dudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu a bydd yr ysgol yn sicrhau ei bod ar gael i unrhyw unigolion sy'n gofyn am y ffurflen hon. Bydd yr ysgol hefyd yn darparu dolenni i'r ffurflen ar eu gwefan neu gyfrifon cyfryngau cymdeithasol.

Dylai'r ysgol ofyn am gyngor y Swyddog Diogelu Data Ysgolion os nad yw'n siŵr sut i ddelio â chais.

14.1. <u>Delweddau o Unigolion Eraill / Trydydd Partïon</u>
Wrth ymdrin â chais gan wrthrych y data, rhaid i'r ysgol ystyried a oes delweddau o unigolion eraill ar wahân i'r unigolyn sy'n gwneud y cais sy'n ymddangos ar y ffilm.

Dylid cuddio delweddau o unigolion eraill cyn i'r data gael ei ryddhau i'r ymgeisydd. Pan fo lluniau'n cynnwys delweddau sy'n ymwneud â thrydydd partïon, bydd yr ysgol yn cymryd camau priodol i guddio a diogelu hunaniaeth yr unigolion hynny.

Efallai y bydd angen defnyddio meddalwedd arbenigol i olygu data gweledol trydydd partïon. Mae'r technegau sydd ar gael yn cynnwys gwneud rhywbeth yn aneglur (*blurring*), masgio, neu ddefnyddio llenwad solet i guddio rhannau o'r ffilm yn llwyr. Mae'r dechneg fwyaf perthnasol yn dibynnu ar yr amgylchiadau sut y crëwyd y ffilm ac ansawdd y ffilm.

Os oes angen i'r ysgol gontractio'r broses olygu (*redaction*) allan i sefydliad arbenigol, bydd angen i gontract ysgrifenedig fod ar waith gyda'r cwmni fel prosesydd data.

Dylid cysylltu â'r Swyddog Diogelu Data Ysgolion os nad yw'r ysgol yn siŵr a oes amgylchiadau eithriadol lle bo'n briodol rhannu delweddau o drydydd partïon. Bydd y Swyddog Diogelu Data Ysgolion yn ystyried y canlynol o dan yr amgylchiadau hyn:

- a yw'r cais yn *gofyn* am ddatgelu eraill neu a ellir ystumio'r delweddau er mwyn peidio â'u hadnabod;
- faint o amser y bydd yn ei gymryd i ddelio â'r cais ac os yw hyn yn fwy na throthwy'r hyn a ystyrir yn amser rhesymol i brosesu'r cais;
- a yw'r unigolion eraill wedi rhoi caniatad i ddatgelu'r delweddau;
- lle na cheisir neu y ceir caniatâd, a yw'n rhesymol fel arall o dan yr amgylchiadau i ddatgelu'r delweddau hynny i'r unigolyn sy'n gwneud y cais.

15. Mynediad at Ddelweddau a Datgelu Ddelweddau i Drydydd Partïon

Mewn amgylchiadau cyfyngedig a rhagnodedig, efallai y byddai'n briodol datgelu delweddau i drydydd parti, megis pan fo datgeliad yn ofynnol yn ôl y gyfraith mewn perthynas ag atal neu ganfod trosedd neu mewn amgylchiadau eraill pan fo eithriad yn gymwys o dan ddeddfwriaeth berthnasol.

Ni fydd unrhyw ddatgeliad o ddata wedi'i recordio i drydydd partïon ar wahân i bersonél awdurdodedig fel yr Heddlu a darparwyr gwasanaethau i'r ysgol lle byddai angen i'r rhain gael mynediad rhesymol at y data (e.e. ymchwilwyr).

Dylid gwneud ceisiadau'n ysgrifenedig i'r Pennaeth. Gwneir datgeliadau o'r fath yn ôl disgresiwn y Pennaeth, gan gyfeirio at ddeddfwriaeth berthnasol a, lle bo angen, yn dilyn cyngor gan y Swyddog Diogelu Data Ysgolion.

Mae'r canlynol yn enghreifftiau o sefyllfaoedd y gall y Pennaeth awdurdodi mynediad i ddelweddau CCTV i drydydd partïon awdurdodedig:

- pan fo'n ofynnol iddo wneud hynny, yr Heddlu neu ryw awdurdod statudol perthnasol pan fo'n ofynnol yn ôl y gyfraith i'r ysgol (neu ei hasiantau) wneud adroddiad ynghylch comisiynu trosedd a amheuir; neu
- yn dilyn cais gan yr Heddlu pan fo trosedd neu drosedd a amheuir wedi digwydd a/neu pan amheuir bod ymddygiad anghyfreithlon/gwrthgymdeithasol yn digwydd ar eiddo'r ysgol; neu
- llunio adroddiad ynghylch ymddygiad troseddol tybiedig; neu
- i asiantaethau erlyn – fel Gwasanaeth Erlyn y Goron (CPS); neu
- galluogi'r arweinydd diogelu dynodedig neu ei ddirprwy penodedig i archwilio ymddygiad a allai arwain at unrhyw bryder diogelu rhesymol neu i'r HSE a/neu unrhyw gorff statudol arall sy'n gyfrifol am ddiogelu plant; neu
- cynorthwyo'r ysgol i sefydlu ffeithiau mewn achosion o ymddygiad annerbyniol gan ddisgyblion, ac os felly, bydd y rhieni/gwarcheidwad yn cael gwybod fel rhan o reolaeth yr ysgol o ddigwyddiad penodol; neu
- i wrthrych y data (neu eu cynrychiolwyr cyfreithiol fel cyfreithwyr neu fargyfreithwyr) yn unol â chais am fynediad o dan ddeddfwriaeth diogelu data neu'n ddarostyngedig i orchymyn llys; neu
- i gwmni yswiriant yr ysgol lle bo angen er mwyn mynd ar drywydd hawliad am ddifrod a wnaed i eiddo sydd wedi'i yswirio; neu
- mewn unrhyw amgylchiadau eraill sy'n ofynnol o dan y gyfraith neu reoliad.

Lle datgelir delweddau, bydd cofnod yn cael ei wneud yn y log systemau. Bydd y canlynol yn cael ei ddogfennu:

- y dyddiad a'r amser y caniatawyd mynediad neu'r dyddiad y gwnaed datgeliad;
- adnabod y trydydd parti a ganiatawyd mynediad neu y gwnaed datgeliad iddo;
- y person a awdurdododd y cais;
- y rheswm dros ganiatáu mynediad neu ddatgeliad;
- manylion y delweddau a welwyd;
- lleoliad y delweddau;
- unrhyw rif digwyddiad trosedd y gallai delweddau fod yn berthnasol iddo;
- llofnod y person sydd wedi'i awdurdodi i gasglu'r cyfrwng – lle bo'n briodol.

Gellir cynnal cyfarfodydd cyswllt gyda'r holl gyrff sy'n ymwneud â chefnogi'r system. Gellir cynnal cyfarfodydd cyswllt hefyd gyda'r Heddlu a chyrff eraill os oes angen.

Gellir defnyddio'r data o fewn gweithdrefnau disgyblu a chwyno'r ysgol yn ôl y gofyn, a byddant yn ddarostyngedig i ofynion cyfrinachedd arferol y gweithdrefnau hynny.

Dylid cofnodi pob cais am fynediad neu ddatgeliad. Os gwrthodir mynediad neu ddatgeliad, dylid cofnodi'r rheswm am hynny yn y log systemau.

16. Rhannu Delweddau CCTV a'r Heddlu

Gall yr Heddlu weld delweddau ar gyfer atal a chanfod troseddau. **Rhaid** i'r Heddlu lenwi'r ffurflen berthnasol (*Ffurflen SA3 - Cais i sefydliad allanol am ddatgelu data personol i'r Heddlu*). Ni ddylid rhannu delweddau CCTV os nad yw'r ffurflen berthnasol wedi'i chwblhau'n llawn gan yr Heddlu a'i derbyn gan yr ysgol cyn rhannu neu ddarparu mynediad i'r delweddau CCTV oni bai bod sefyllfa frys (e.e. plentyn sydd ar goll, plentyn sydd mewn perygl) sy'n gofyn am fynediad ar unwaith i'r ffilm. Yn yr achosion hyn, gellir cyflwyno'r ffurflen ar ôl y datgeliad.

Dim ond i'r cyfryngau i'w defnyddio wrth ymchwilio i drosedd benodol yn dilyn cais penodol gan yr Heddlu neu gan awdurdod ysgrifenedig yr Heddlu y caiff recordiadau a delweddau eu rhyddhau.

Bydd cofnod yn cael ei gadw o ryddhau unrhyw ffilm lawrlwytho i'r Heddlu neu ymgeiswyr awdurdodedig eraill. Rhaid cofnodi delweddau yn ysgrifenedig yn y log systemau pan mae'r Heddlu wedi eu gweld. Os bydd angen delweddau fel tystiolaeth, gellir rhyddhau copi i'r Heddlu o dan y gweithdrefnau a ddisgrifir yn y polisi hwn. Dim ond ar y ddealltwriaeth glir bod y ffilm lawrlwytho (ac unrhyw ddelweddau a gynhwysir arni) yn parhau i fod yn eiddo i'r ysgol y bydd delweddau'n cael eu rhyddhau, a'u bod i'w trin yn unol â deddfwriaeth diogelu data.

Mae gan yr ysgol hefyd yr hawl i wrthod caniatâd i'r Heddlu basio'r ffilm a lawrlwythwyd (ac unrhyw ddelweddau a gynhwysir arni) ymlaen i unrhyw berson arall. Ar adegau pan fydd llys yn gofyn am ryddhau ffilm wedi'i llwytho i lawr, bydd hyn yn cael ei gynhyrchu o'r storfa dystiolaeth ddiogel, yn gyfan mewn bag wedi'i selio.

Efallai y bydd yr Heddlu yn ei gwneud yn ofynnol i'r ysgol gadw'r ffilm a lawrlwythwyd i'w defnyddio fel tystiolaeth yn y dyfodol. Bydd ffilmiau o'r fath yn cael eu mynegeio'n briodol a'u storio'n ddiogel nes bod eu hangen ar yr Heddlu.

Bydd yr ysgol yn cydymffurfio â *Gweithdrefn Rhannu Gwybodaeth gydag Awdurdodau Heddlu yn y Deyrnas Unedig Gwynedd ac Ynys Môn.*

17. Prosesu Trydydd Parti

Pan fo'r CCTV yn cael ei weithredu neu ei reoli gan drydydd parti (fel cwmni diogelwch masnachol), rhaid i'r ysgol roi cytundeb prosesu data ysgrifenedig ar waith gyda'r cwmni hwnnw.

Dylai'r ysgol sicrhau bod y trydydd parti yn bodloni gofynion trwyddedu perthnasol y *Security Industry Authority (SIA).* Mae CCTV sy'n eiddo i'r ysgol, a weithredir gan ei staff ei hun ac y mae ei ddata'n cael ei reoli gan yr ysgol yn cael ei ystyried yn fewnol ac nid yw'n dod o dan ddeddfwriaeth SIA.

Bydd y Swyddog Diogelu Data Ysgolion yn rhoi cyngor ac arweiniad pellach a bydd yn paratoi unrhyw gytundeb gyda chwmni trydydd parti sy'n darparu CCTV ar gyfer yr ysgol.

Nid yw'r ysgol yn berchen ar nac yn rheoli systemau CCTV trydydd parti, ond gellir darparu delweddau o ddigwyddiadau gan drydydd partïon lle mae hyn yn unol ag amcanion Polisi CCTV yr ysgol ei hun a/neu reolau'r ysgol.

18. Technoleg Adnabod Wynebau Byw (LFR)

Mae technoleg adnabod wynebau byw (LFR), a elwir hefyd yn gydnabyddiaeth wyneb awtomatig, yn adnabod pobl mewn fideo mewn amser real, gan ddefnyddio set o ffotograffau fel cyfeiriad. Mae camerâu gwyliadwriaeth adnabod wynebau yn sganio'r holl wynebau y gallant eu gweld mewn torf i wirio hunaniaeth pobl yn erbyn cronfa ddata mewn amser real.

Os yw'r ysgol yn ystyried defnyddio technoleg adnabod wynebau byw (LFR), rhaid iddi drafod hyn gyda'r Swyddog Diogelu Data Ysgolion cyn prynu'r dechnoleg hon.

Bydd angen i'r ysgol ddangos safonau uchel o lywodraethu ac atebolrwydd o'r cychwyn cyntaf, gan gynnwys gallu cyfiawnhau bod y defnydd o LFR yn deg, yn angenrheidiol ac yn gymesur ym mhob cyd-destun penodol y caiff ei ddefnyddio ynddo.

Bydd angen ystyried pob risg hefyd wrth ddefnyddio'r math newydd hwn o dechnoleg a bydd angen cwblhau Asesiad Effaith Diogelu Data.

19. Hyfforddiant

Dylai staff sydd â mynediad i system CCTV yr ysgol gael hyfforddiant digonol i sicrhau dealltwriaeth o'r system.

Bydd y Pennaeth yn cadw cofnod o'r hyfforddiant a gynhelir gan staff sydd â mynediad i'r system CCTV.

20. Cwynion

Mae gan unigolion sydd wedi cael eu delwedd wedi ei ffilmio gan y system hawl i wrthwynebu a dylent ddilyn gweithdrefn gwyno'r ysgol.

Dylid cyfeirio unrhyw gwynion ac ymholiadau mewn perthynas â system CCTV yr ysgol at y Pennaeth i ddechrau.

Mae gan unigolion yr hawl i wneud cwyn i Swyddfa'r Comisiynydd Gwybodaeth (ICO) sef y rheoleiddiwr annibynnol ar gyfer diogelu data:

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

Rhif ffôn: 0303 123 1113

Cyfeiriad: Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

21. Torri’r Polisi

Gallai peidio â chydymffurfio â'r polisi hwn gan aelodau o staff yr ysgol arwain at ganlyniadau difrifol gan gynnwys torri'r gyfraith a pherygl o gosbau sifil a throseddol sylweddol i'r unigolyn ac awdurdodau'r ysgol.

Gall hyn arwain at roi'r unigolion y mae eu gwybodaeth bersonol yn cael ei phrosesu a'r ysgol mewn perygl.

Gellir ystyried peidio â chydymffurfio â pholisi neu gamddefnyddio gwybodaeth am y system wyliadwriaeth gan aelod o staff yr ysgol yn fater disgyblu. Os bydd gweithiwr nad yw'n gyflogai yn torri'r polisi hwn, efallai y bydd eu contract yn cael ei derfynu ar unwaith.

22. Adolygu’r Polisi a Threfniadau Arolygiaeth

Caiff y polisi hwn ei adolygu gan y Swyddog Diogelu Data Ysgolion, gan gynnwys ymgynghori fel y bo'n briodol gyda phartïon â buddiant, bob tair blynedd, oni bai bod newidiadau i ddeddfwriaeth, codau ymarfer neu ganllawiau yn ei gwneud yn ofynnol i'r polisi gael ei ddiweddaru'n gynt.

Caiff y polisi ei gymeradwyo gan Uwch Dîm Rheoli'r Gwasanaeth Dysgu a chaiff ei fabwysiadu gan gorff llywodraethu'r ysgol. Bydd y Tîm Arweinyddiaeth Ysgolion a'r corff llywodraethu yn monitro cydymffurfiaeth â'r polisi hwn a gweithdrefnau cysylltiedig.

Os oes unrhyw ymholiadau neu bryderon am unrhyw beth a gynhwysir yn y polisi hwn, dylid cysylltu â'r Swyddog Diogelu Data Ysgolion heb betruso:

E-bost: dpoysgolionmon@ynysmon.gov.uk

Rhif ffôn: 01248 751833

Cyfeiriad:
Gwasanaeth Dysgu, Cyngor Sir Ynys Môn,
Swyddfeydd y Cyngor
Llangefni
Ynys Môn
LL77 7TW

Ceir rhagor o wybodaeth ynglŷn â diogelu data a CCTV o wefan yr ICO: https://ico.org.uk/ a gwefan y Surveillance Camera Commissioner: https://www.gov.uk/government/organisations/surveillance-camera-commissioner

Content | **Page**

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. <u>School Governing Body</u>
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. <u>Headteacher (and/or Person Responsible for Data Protection within the School)</u>
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. <u>Schools Data Protection Officer</u>
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.

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

ATODIAD A

Log Systemau CCTV Ysgolion

Mae'n rhaid cwblhau'r ffurflen hon wrth dynnu delweddau i lawr i'w gweld (*i'w argraffu neu gellir ychwanegu llinellau ychwanegol yn electronig fel bod angen).*

Tynnu Delweddau i Lawr i'w Gweld							
Dyddiad ac amser y tynnwyd y delweddau i lawr	**Enw (unigolyn sy'n tynnu'r delweddau i lawr)**	**Enw (yr unigolyn a'r sefydliad sy'n edrych ar y delweddau)**	**Y rheswm dros weld y delweddau**	**Sut yr ymdriniwyd â'r cais**	**Y deilliant o gael gweld y delweddau**	**Y dyddiad a'r amser y cawsant eu dychwelyd i'r system**	**Lle diogel a gadwir ar gyfer tystiolaeth**

Mae'n rhaid cwblhau'r ffurflen hon pan ganiateir mynediad neu ddatgeliad (*i'w hargraffu neu gellir ychwanegu llinellau ychwanegol yn electronig fel bod angen).*

Caniatáu Mynediad at Ddelweddau neu Ddatgelu Delweddau							
Dyddiad ac amser y caniatawyd mynediad / y gwnaethpwyd y datgeliad	**Dull adnabod y trydydd parti a ganiatawyd mynediad iddo neu y gwnaethpwyd y datgeliad iddo**	**Enw'r unigolyn yr awdurdododd y cais**	**Rheswm am ganiatáu mynediad neu ddatgeliad**	**Manylion o'r delweddau a welwyd**	**Lleoliad y delweddau**	**Rhif digwyddiad trosedd perthnasol**	**Llofnod yr unigolyn yr awdurdodir i gasglu delweddau**

Mae'n rhaid cwblhau'r ffurflen hon pan wrthodir mynediad neu ddatgeliad (*i'w hargraffu neu gellir ychwanegu llinellau ychwanegol fel bod angen).*

Gwrthod Mynediad at Ddelweddau neu Ddatgeliad Delweddau							
Dyddiad y cais	**Manylion yr unigolyn / sefydliad sy'n gofyn am fynediad neu ddatgeliad**	**Manylion y delweddau a ofynnwyd amdanynt**	**Lleoliad y delweddau y gofynnwyd amdanynt**	**Enw'r unigolyn a wrthododd y cais**	**Rheswm dros wrthod mynediad neu ddatgeliad**	**Manylion ynglŷn â pha bryd y gwrthodwyd a sut y cyfathrebwyd y gwrthodiad**	**Rhif digwyddiad trosedd perthnasol (os yn berthnasol)**

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**

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		

ATODIAD C / *APPENDIX C*

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

Ysgol /*School*	
Manylion pwy sydd yn gyfrifol am system CCTV yr ysgol / *Details of who is responsible for the school's CCTV system*	
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*	
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*	
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*	

ATODIAD D

Polisi CCTV Ysgolion

Rhestr Wirio'r Pennaeth

Rhif	Camau Gweithredu	A oes gan yr ysgol hyn ar waith (Oes/Nac Oes)/ Sylwadau/Dyddiadau etc.)
1	Bod y fersiwn cyfredol o'r Polisi CCTV Ysgolion wedi cael ei fabwysiadu'n ffurfiol gan Gorff Llywodraethu'r ysgol.	
2	Bod proses ar waith i fonitro cydymffurfiad yr ysgol â'r polisi hwn yn barhaus.	
3	Bod holl gyflogeion yr ysgol yn ymwybodol o'r cyfyngiadau mewn perthynas â mynediad at a datgeliad ffilm sydd wedi'i recordio.	
4	Bod amserlen ar waith i ymgymryd â monitro perfformiad rheolaidd, gan gynnwys gwiriadau gweithredu ar hap ar y system CCTV. Gwirio a chadarnhau effeithlonrwydd y system ac yn benodol bod yr offer yn recordio'n iawn; bod camerâu yn gweithio ac yn gweithredu'n effeithiol a bod y cyfeiriad dyddiad ac amser yn gywir.	
5	Bod arwyddion digonol wedi eu gosod o amgylch yr ysgol mewn cydymffurfiad â *Chod Ymarfer* y Surveillance Camera Commissioner: • bod hysbysiadau'n cael eu harddangos mewn safle clir ym mhob ardal sy'n cael ei ffilmio; • bod arwyddion sydd wedi eu gosod yn glir ym mhrif fynedfeydd allanol yr ysgol; • bod arwyddion yn cynnwys yr wybodaeth angenrheidiol sydd angen bod ar gael i unigolion.	
6	Bod y *Log Lleoliadau CCTV Ysgolion* wedi ei gwblhau ac yn cael ei ddiweddaru.	
7	Bod y ddogfen *Gweithdrefn CCTV yr Ysgol* wedi ei gwblhau ac yn cael ei ddiweddaru.	

8	Bod y *Log Systemau CCTV Ysgolion* yn cael ei ddefnyddio bob amser i gynnal cofnod o fynediad at, neu ryddhad unrhyw ddeunydd a gofnodir neu a storir yn y system.	
9	Monitro bod delweddau a recordir ond yn cael eu storio am gyfnod sydd ddim hirach na 30 diwrnod a'u bod yn cael eu chwalu oni bai bod angen eu cadw fel rhan o ymchwiliad droseddol neu achosion llys (troseddol neu sifil).	
10	Monitro bod mesurau diogelwch seibr ar waith i ddiogelu data a ddelir ar y system.	
11	Cofnodion o'r holl weithgareddau prosesu data mewn perthynas â gwyliadwriaeth a ffilm CCTV yn cael eu cynnwys yn ROPA'r ysgol.	
12	Staff sydd â mynediad i system CCTV yr ysgol wedi derbyn digon o hyfforddiant i sicrhau dealltwriaeth lawn o'r system a bod cofnodion o fanylion hyfforddiant yn cael eu cadw.	
13	Bod proses ar waith i reoli unrhyw gwynion ynglŷn â'r system CCTV.	
14	Bod Asesiad Effaith Diogelu Data (DPIA) wedi cael ei wneud ar gyfer y system CCTV a'i fod yn cael ei ddiweddaru.	
15	Bod monitorau arddangos digidol yn cael eu lleoli mewn ardal ddynodedig ddiogel sydd wedi ei chyfyngu ac sy'n breifat, lle na all unigolion awdurdodedig eu gweld.	
16	Nad yw camerâu wedi eu gosod mewn lleoedd lle byddai gan unigolion ddisgwyliad rhesymol o breifatrwydd (megis ystafelloedd newid a thoiledau).	
17	Nad yw camerâu wedi'u pwyntio ar gerbydau nac eiddo preifat y tu allan i berimedr yr ysgol ac nad oes (neu cyn lleied â phosibl) recordiadau o bobl sy'n mynd heibio neu eiddo preifat unigolyn arall.	
18	Bod holl ymwelwyr yr ysgol yn cael eu cofnodi yn y llyfr ymwelwyr ysgol neu drwy system arwyddo i mewn electronig.	
19	Bod y system CCTV yn cael gwaith cynnal blynyddol.	
20	Mae diweddariadau meddalwedd (yn enwedig diweddariadau diogelwch) yn cael eu gwneud ar unwaith.	
21	Bod gweithdrefn ffilm lawrlwytho cadarn, a'i bod yn cael ei dilyn.	
22	Bod proses Ceisiadau gan Wrthrych y Data ar waith i ddelio â cheisiadau am wybodaeth o ddelweddau CCTV.	

23	Bod proses ar waith i ddelio â cheisiadau am fynediad at a datgeliad delweddau i drydydd partïon.	
24	Na chaiff delweddau eu rhyddhau i'r Heddlu oni bai bod yr ysgol wedi derbyn *Ffurflen SA3 - Cais i sefydliad allanol am ddatgelu data personol i'r Heddlu* wedi'i llofnodi.	
25	Bod cytundeb prosesu data ysgrifenedig ar waith gyda'r cwmni sy'n gweithredu neu'n rheoli system CCTV yr ysgol (os yn berthnasol).	
26	Os ydych yn ystyried defnyddio technoleg adnabod wynebau byw (LFT), bod hyn wedi cael ei drafod gyda'r Swyddog Diogelu Data Ysgolion cyn prynu'r dechnoleg hon (os yn berthnasol).	

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).	