Ysgol Cybi

Polisi E-Ddiogelwch Ysgolion / *Schools E-Safety Policy*

(Fersiwn 1, Rhagfyr 2022 / *Version 1, December 2022*)

Ynglŷn â'r polisi hwn

Mae'r polisi hwn yn amlinellu beth y mae angen i'r ysgol ei wneud i sicrhau bod y prosesau perthnasol ar waith ynghylch e-ddiogelwch a'i bod yn sicrhau cydymffurfiad â pholisïau a deddfwriaeth berthnasol.

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

About this policy

This policy outlines what the school needs to do to ensure that the relevant processes are in place regarding e-safety and that it ensures compliance with relevant policies and legislation.

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*	Rhagfyr 2022 / *December 2022*	Fersiwn cyntaf o'r polisi / *First version of policy*	

Dyddiad yr adolygiad nesaf / *Date of next review*	
Bydd y polisi hwn yn cael ei adolygu yn: / *This policy will be reviewed in:*	Rhagfyr 2024 / *December 2024*

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.llyw.cymru

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.llyw.cymru

Telephone: 01248 751833

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

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

Dogfen: Polisi templed ar brosesau a gofynion e-ddiogelwch.

Document: *Policy template on e-safety processes and requirements.*

Cyfrifoldeb: Cyfrifoldeb y Pennaeth yw sicrhau bod gweithdrefnau ar waith i sicrhau fod yr ysgol yn cydymffurfio â gofynion e-ddiogelwch a'r corff llywodraethu i fonitro cydymffurfiad â'r polisi hwn. Cyfrifoldeb y Pennaeth yw sicrhau gweithrediad a chydymffurfiaeth gan holl staff yr ysgol.

Responsibility: *It is the responsibility of the Headteacher to ensure procedures are in place to ensure that the school complies with the requirements of e-safety and for the school governing body to monitor compliance with this policy. It is the responsibility of the Headteacher to ensure implementation and compliance by all school staff.*

Cynnwys **Tudalen**

1. Datganiad Polisi 5
2. Sgôp 5
3. Ddeddfwriaeth, Canllawiau a Pholisïau 5
4. Diffiniadau 6
5. Cyfrifoldebau 9
5.1. Corff Llywodraethu Ysgol 9
5.2. Pennaeth 9
5.3. Holl Staff yr Ysgol 10
5.4. Swyddog Diogelu Data Ysgolion 10
6. Beth yw e-ddiogelwch? 10
7. Beth mae cyfathrebu electronig yn ei gynnwys? 11
8. Defnydd o dechnoleg newydd mewn addysg 11
9. Dysgu ac addysgu 12
9.1. Pam bod defnyddio'r rhyngrwyd yn bwysig 12
9.2. Sut mae defnyddio'r rhyngrwyd yn fuddiol i addysg? 12
9.3. Sut all y rhyngrwyd wella dysgu? 13
10. Llwybrau i e-ddiogelwch 13
10.1. Egwyddorion cyffredinol 13
10.2. Cyfathrebu electronig rhwng staff a disgyblion 14
11. Rheoli Systemau Gwybodaeth 14
11.1. Sut cynhelir diogelwch systemau gwybodaeth? 14
11.2. Sut rheoleiddir e-bost? 15
11.3. Sut rheoleiddir cynnwys cyhoeddedig? 16
11.4. A ellir cyhoeddi gwaith neu luniau o ddisgyblion? 16
11.5. Sut rheoleiddir rhwydweithio cymdeithasol a chyhoeddi personol? 16
11.6. Sut rheoleiddir ffiltro? 17
11.7. Sut caiff fideo-gynadledda ei fonitro? 18
11.7.1. Defnyddwyr 18
11.7.2. Cynnwys 18
11.8. Sut caiff dysgu ar-lein ei fonitro? 19
11.8.1. Athrawon yn cytuno i 19
11.8.2. Rhieni/gofalwyr yn cytuno i 20
11.9. Sut mae disgyblion yn dysgu sut i werthuso cynnwys ar y rhyngrwyd? 20
11.10. Sut ellir rheoleiddio'r dechnoleg ddiweddaraf? 21
12. Sut y diogelir data personol? 21
13. Penderfyniadau Polisi 21
13.1. Sut awdurdodir mynediad i'r rhyngrwyd? 21
13.2. Sut asesir risg? 21
13.3. Sut ymdrinnir â chwynion am e-ddiogelwch? 22
13.4. Sut defnyddir y rhyngrwyd ar draws y gymuned? 22
14. Polisi Cyfathrebu 23
14.1. Sut cyflwynir y polisi i'r disgyblion? 23
14.2. Sut trafodir y polisi â staff? 23
14.3. Sut rhennir y polisi â rhieni/gofalwyr? 23
15. Ymateb i ddigwyddiad sy'n peri pryder 23
15.1. Beth yw'r peryglon? 24
15.2. Sut ddylai'r ysgol ymateb? 24

16. Y Fframwaith Cyfreithiol 24
16.1 Cod Plant 25
16.2 Deddfwriaeth Perthnasol 26
17. Enwau a Chyfeiriadau Cyswllt E-ddiogelwch 29
18. Hyfforddiant 30
19. Mynd yn Erbyn y Polisi 30
20. Adolygu'r Polisi a Threfniadau Arolygiaeth 30
ATODIAD A- Ymateb i ddigwyddiad sy'n peri pryder 32
ATODIAD B- Polisi E-Ddiogelwch Ysgolion- Rhestr Wirio'r Pennaeth 33

English Version **39**

1. Datganiad Polisi

Mae'r ysgol yn cydnabod bod y rhyngrwyd a thechnolegau cyfathrebu gwybodaeth yn rhan bwysig o fywyd bob dydd. Mae defnydd diogel ac effeithiol o'r rhyngrwyd, dysgu ar-lein, cyfryngau cymdeithasol a thechnoleg gwybodaeth bellach yn sgil bywyd hanfodol i ddisgyblion a staff.

E-ddiogelwch yw addysgu am fuddion a risgiau defnyddio technolegau newydd, a darparu camau diogelu ac ymwybyddiaeth sy'n galluogi unigolion i reoli eu profiadau ar-lein.

Mae'r ysgol yn adnabod bod y defnydd o dechnoleg yn cyflwyno heriau a risgiau tu mewn a thu allan i'r ysgol. Mae diogelwch ar-lein yn rhan hanfodol o ddiogelu a bydd yr ysgol yn sicrhau fod bob disgybl ac aelod o staff yn cael eu hamddiffyn rhag niwed posib ar-lein. Rhaid cefnogi disgyblion i allu rheoli ac ymateb i risgiau ar-lein gan y gall mynediad heb ei reoleiddio i'r rhyngrwyd a thechnolegau cyfathrebu gwybodaeth roi disgyblion mewn sefyllfa anodd, amhriodol a pheryglus hyd yn oed.

Mae'n rhaid i'r ysgol fod â phrosesau ar waith i sicrhau y defnyddir TGCh yn gyfrifol, gan sicrhau diogelwch disgyblion. Hefyd, bydd prosesau'n grymuso, yn amddiffyn ac yn addysgu staff ysgol yn eu defnydd o dechnoleg ac yn sefydlu mecanweithiau i nodi, ymyrryd a dwysáu digwyddiad lle y bo'n briodol.

2. Sgôp

Mae'r polisi hwn yn berthnasol i'r holl weithwyr, gwirfoddolwyr, llywodraethwyr, contractwyr, asiantaethau, cynrychiolwyr a staff dros dro sy'n gweithio i'r ysgol, ac sydd yn ddefnyddwyr o, systemau technoleg gwybodaeth a chyfathrebu'r ysgol.

Mae'r polisi hwn yn berthnasol i bob mynediad i'r rhyngrwyd a chyfathrebiadau electronig eraill, yn ogystal â rhwydweithio cymdeithasol; cyhoeddi personol a dysgu ar-lein a defnydd o technoleg megis cyfrifiadur, gliniadur, tabled neu ffôn symudol mewn perthynas â busnes yr ysgol.

3. Ddeddfwriaeth, Canllawiau a Pholisïau

Dylid darllen y polisi hwn hefyd ar y cyd â pholisïau perthnasol eraill yr ysgol gan gynnwys (ond heb fod yn gyfyngedig i) y *Polisi Recordio Sesiynau Ffrydio'n Fyw; Polisi Cadw Recordiadau; Polisi Diogelu Data Ysgolion; Polisi Diogelwch Gwybodaeth Ysgolion; Polisi E-bost Staff Ysgolion, Polisi Cyfryngau Cymdeithasol Staff Ysgolion; Polisi Ysgolion yn Tynnu Lluniau at Ddibenion Cyhoeddusrwydd; Polisi Digwyddiadau Diogelwch Data Ysgolion; Polisi Cais gan Wrthrych y Data Ysgolion; Polisi Diogelu; Polisi Amddiffyn Plant; Polisi Ymddygiad Bygythiol; Polisi Disgyblu; Polisi Gwrth-fwlio; Polisi Defnydd Derbyniol* a *Chyfnodau Cadw Ysgolion.*

Mae'r rhain i gyd ar gael ar y dudalen diogelu data ar Feicrowefan y Gwasanaeth Dysgu.

Dylai staff gydymffurfio â *Chod Ymddygiad ac Ymarfer Proffesiynol* y CGA (Cyngor y Gweithlu Addysg) - http://www.ewc.wales/site/index.php/cy/priodoldeb-i-ymarfer/cod-ymddygiad-ac-ymarfer-proffesiynol-cga.html

Mae'r ddeddfwriaeth ganlynol yn ymwneud ag e-ddiogelwch (gweler adran 17 am ragor o fanylion am y fframwaith cyfreithiol):

- *Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR);*
- *Deddf Diogelu Data 2018;*
- *Cod Plant;*
- *Deddf Troseddau Rhywiol 2003;*
- *Deddf Casineb Hiliol a Chrefyddol 2006;*
- *Deddf yr Heddlu a Chyfiawnder 2006;*
- *Deddf Camddefnyddio Cyfrifiaduron 1990;*
- *Deddf Cyfathrebu Maleisus 1988;*
- *Deddf Hawlfraint, Dyluniadau a Patentau 1988;*
- *Deddf Trefn Gyhoeddus 1986;*
- *Deddf Plant 1989;*
- *Deddf Gwasanaethau Cymdeithasol a Llesiant (Cymru) 2014;*
- *Deddf Cyhoeddiadau Anllad 1959;*
- *Deddf Amddiffyn rhag Aflonyddu 1997;*
- *Deddf Rheoleiddio Pwerau Ymchwilio 2000;*
- *Rheoliadau Telegyfathrebu (Arferion Busnes Cyfreithlon) (Dehongli Cyfathrebu) 2000;*
- *Deddf Cyfathrebu 2003:*
- *Deddf Crwneriaid a Chyfiawnder 2009;*
- *Y Gyfraith Cwcis*

4. Diffiniadau

Dysgu Cyfunol	Mae dysgu cyfunol yn ddull cyfarwyddiadol sy'n cynnwys cyfuniad o weithgareddau dysgu ar-lein ac wyneb yn wyneb. Er enghraifft, gall myfyrwyr gwblhau aseiniadau hunan-gyflymder ar-lein erbyn dyddiad penodol ac yna cyfarfod ar y safle neu ar-lein ar gyfer gweithgareddau dysgu ychwanegol.
Dysgu cydamserol (dysgu ar y pryd)	Pan fydd dysgwyr yn cymryd rhan mewn cwrs dysgu ar-lein ar yr un pryd ond mewn gwahanol leoliadau, fe'i gelwir yn ddysgu cydamserol. Mae dysgu cydamserol yn caniatáu i ddysgwyr ryngweithio â'r hyfforddwr a chyfranogwyr eraill. Gwneir hyn drwy feddalwedd sy'n creu ystafell ddosbarth rithiol.
Dysgu anghydamserol	Mae dysgu anghydamserol yn ddull o addysg lle mae disgyblion yn dysgu'r un cynnwys o wahanol leoedd

(dysgu nad yw'n ddysgu ar y pryd)	(daearyddol) ac ar wahanol adegau. Gall disgyblion gael gafael ar ddeunyddiau, gofyn cwestiynau, ac ymarfer eu medrau ar unrhyw adeg sy'n gweithio iddyn nhw.
Ystafell ddosbarth rithiol	Mae'r ystafell ddosbarth rithiol yn cyfeirio at amgylchedd dysgu ystafell ddosbarth ddigidol sy'n digwydd dros y rhyngrwyd yn hytrach nag mewn ystafell ddosbarth ffisegol. Fe'i gweithredir drwy feddalwedd sy'n caniatáu i athro a myfyrwyr ryngweithio.
Cyfryngau ffrydio	Mae cyfryngau ffrydio yn cyfeirio at fideo a sain sy'n cael ei lawrlwytho i gyfrifiadur o'r rhyngrwyd fel llif parhaus o ddata ac sy'n cael ei chwarae wrth iddo gyrraedd y cyfrifiadur cyrchfan.
Cyfryngau cymdeithasol	Unrhyw blatfform ar-lein sy'n cynnig rhyngweithio amser real rhwng y defnyddiwr ac unigolion neu grwpiau eraill. Mae enghreifftiau'n cynnwys, ond heb fod yn gyfyngedig i lwyfannau cyfathrebu, fforymau trafod ar-lein, blogiau, mannau cydweithredol, gwasanaethau rhannu cyfryngau, apiau micro-flogio a defnyddio gwe-gamerâu.
Gofod cymdeithasol ar-lein	Gofodau ar y rhyngrwyd (safleoedd/tudalennau) lle gallwch gwrdd â phobl eraill a sgwrsio, naill ai mewn amser real (ystafelloedd sgwrsio a sgwrsio byw) neu drwy negeseuon a byrddau negeseuon.
Gwe Fyd-eang (www.)	System wybodaeth ar y rhyngrwyd yw'r We Fyd-eang sy'n caniatáu i ddogfennau gael eu cysylltu â dogfennau eraill drwy ddolenni hyperdestun, gan alluogi'r defnyddiwr i chwilio am wybodaeth drwy symud o un ddogfen i'r llall.
Podledu	Podlediad yw'r arfer o ddefnyddio'r rhyngrwyd i sicrhau bod recordiadau digidol o ddarllediadau ar gael i'w lawrlwytho i gyfrifiadur neu ddyfais symudol.
Ystafell sgwrsio	Tudalen we sy'n cynnwys ffenestr lle gallwch deipio testun i alluogi sgwrs 'amser real' ar ffurf testun gydag unigolion neu grwpiau bach.
Blog / Flog	Gwefan lle mae cofnodion rheolaidd yn cael eu gwneud ar ffurf cyfnodolyn neu ddyddiadur ar-lein. Mae Blog neu 'log gwe' yn aml yn cynnig sylwebaeth neu newyddion ar bwnc penodol tra bod Flog yn defnyddio fideo i ddogfennu eu bywydau bob dydd fel dyddiadur fideo parhaus. Trefnir blogiau yn gronolegol fel arfer a chyda llai o ffurfioldeb na gwefan. Mae llawer o flogiau'n derbyn ac yn ymateb i sylwadau.
Wici	Gwefan neu adnodd tebyg sy'n caniatáu i ddefnyddwyr ychwanegu a golygu cynnwys gyda'i gilydd.
Porwr	Pecyn meddalwedd neu ap symudol am ddim yw porwr sy'n dangos tudalennau gwe, graffeg a'r rhan fwyaf o gynnwys ar-lein. Mae meddalwedd porwr wedi'i gynllunio'n benodol i drosi cod cyfrifiadurol HTML ac XML yn ddogfennau y gellir eu darllen gan bobl. Mae porwyr yn dangos tudalennau gwe.
Tudalen We	Tudalen we yw'r hyn sydd i'w weld mewn porwr gwe pan fydd ar y rhyngrwyd. Gall tudalennau gynnwys testun,

	ffotograffau, delweddau, diagramau, dolenni, hysbysebion, a mwy ar unrhyw dudalen a welir.
URL	URLau yw cyfeiriadau tudalennau a ffeiliau gwe ar borwr.
Fideo-gynadledda	Mae fideo-gynadledda yn delegyfathrebu ar ffurf fideo-gynhadledd sef cynnal cynhadledd ymysg pobl mewn lleoliadau anghysbell drwy gyfrwng signalau sain a fideo a drosglwyddir.
Seiberfwlio	Unrhyw ddefnydd o gyfryngau cymdeithasol neu dechnoleg cyfathrebu i fwlio unigolyn neu grŵp.
E-bost	Negeseuon a ddosberthir drwy ddulliau electronig gan un defnyddiwr cyfrifiadur i un neu fwy o dderbynwyr drwy rwydwaith. Yn ogystal â chynnwys testunol, mae e-bost yn caniatáu i'r anfonwr anfon ffotograffau, fideo neu glipiau sain ar ffurf neu ffeiliau digidol.
Cymhorthion digidol personol (PDAau)	Mae PDA yn gyfrifiadur sy'n ffitio yng nghledr eich llaw i helpu i gasglu gwybodaeth fel cysylltiadau, apwyntiadau, ffeiliau a rhaglenni.
Lawrlwytho	Mae lawrlwytho yn derm eang sy'n disgrifio trosglwyddo rhywbeth ar y rhyngrwyd neu'r We Fyd-eang i gyfrifiadur neu ddyfais arall. Fel arfer, mae llwytho i lawr yn gysylltiedig â chaneuon, cerddoriaeth a ffeiliau meddalwedd.
Bluetooth	System dechnegol yw Bluetooth sy'n caniatáu i bobl gyfnewid gwybodaeth a data gan ddefnyddio gwahanol fathau o ddyfeisiau electronig fel cyfrifiaduron, ffonau symudol, argraffwyr, camerâu fideo ac ati heb ddefnyddio gwifrau.
Data personol	Unrhyw wybodaeth sy'n ymwneud â pherson naturiol sydd wedi ei adnabod neu y gellir ei adnabod naill ai'n uniongyrchol neu'n anuniongyrchol o'r wybodaeth honno. Gellir storio hyn yn electronig, ar gyfrifiadur, neu mewn systemau ffeilio ar bapur.
Prosesu gwybodaeth	Casglu, meddiannu, cofnodi, trefnu, strwythuro, storio, dargadw, diwygio, addasu, altro, adennill, ymgynghori, lledaenu, cyfyngu, datgelu, dinistrio, dileu gwybodaeth neu ei defnyddio neu wneud unrhyw beth â hi.
Ap	Mae'r gair "ap" yn dalfyriad ar gyfer *"application"* yn y Saesneg. Mae'n ddarn o feddalwedd sy'n gallu rhedeg drwy borwr gwe neu all-lein ar gyfrifiadur, ac ar ffôn clyfar, tabled neu ddyfeisiau electronig eraill.
Storio Cwmwl	Mae storio cwmwl yn fodel cyfrifiadura cwmwl lle caiff data ei storio ar weinyddion o bell a gyrchir o'r rhyngrwyd, neu "gwmwl". Mae'n cael ei gynnal, ei weithredu a'i reoli gan ddarparwr gwasanaeth storio cwmwl ar weinyddion storio sy'n cael eu hadeiladu ar dechnegau rhithiol.
Systemau Gwybodaeth	Cyfrifiaduron prosesu gwybodaeth neu systemau cyfathrebu data.
Digwyddiad Diogelwch Data	Toriad diogelwch sy'n arwain at ddinistrio, colli, addasu, datgelu neu fynediad anawdurdodedig at ddata personol a drosglwyddir, a storir neu a brosesir mewn unrhyw ddull arall, yn ddamweiniol neu'n anghyfreithlon.

5. Cyfrifoldebau

5.1. Corff Llywodraethu Ysgol
Corff llywodraethu'r ysgol sy'n gyfrifol am:

- fonitro cydymffurfiad ac atebolrwydd cyffredinol yr ysgol yn ymwneud â'r polisi hwn;
- sicrhau y gall yr ysgol dystiolaethu cydymffurfiad â deddfwriaeth diogelu data.
- ymgymryd ag unrhyw hyfforddiant e-ddiogelwch a gynhigir.

5.2. Y Pennaeth
Mae'r Pennaeth yn gyfrifol am:

- sicrhau bod y polisi hwn yn cael ei weithredu a hyrwyddo dealltwriaeth a chydymffurfiaeth â'r polisi hwn a'r holl bolisïau sy'n ymwneud ag e-ddiogelwch;
- rhannu'r polisi hwn gyda holl staff a gwirfoddolwyr yr ysgol;
- sicrhau bod data personol o fewn yr ysgol yn cael ei gadw ac ei brosesu yn unol â'r *UK GDPR* a *Deddf Diogelu Data 2018;*
- penodi aelod penodol o staff a fydd yn gyfrifol am e-ddiogelwch/TGCh a bod y person hwn yn cael cymorth digonol gan staff eraill yr ysgol ac yn rhoi cymorth iddynt, yn enwedig yr uwch berson dynodedig ar gyfer diogelu;
- sicrhau bod staff yn cael hyfforddiant priodol mewn e-ddiogelwch a bod hyn yn cael blaenoriaeth uchel ar draws yr ysgol;
- trafod ac adolygu manylion y trefniadau e-ddiogelwch gyda holl staff yr ysgol yn rheolaidd;
- sicrhau bod proses ar waith i ddiogelu'r holl wybodaeth bersonol a chategori arbennig yn yr ysgol;
- pennu lefel y mynediad sydd i'w roi i unigolion penodol;
- adolygu a chadw Cofrestr Asedau Gwybodaeth a Cofnod o Weithgareddau Prosesu (ROPA) yr ysgol yn gyfredol;
- cael arweiniad gan y Swyddog Diogelu Data Ysgolion ar gytundebau sy'n ymwneud ag apiau, meddalwedd a systemau technoleg gwybodaeth a chyfathrebu;
- sicrhau bod disgyblion yn cael eu haddysgu ar e-ddiogelwch fel rhan hanfodol o'r cwricwlwm;
- sicrhau bod cofnodion yn cael eu cadw o bob digwyddiad e-ddiogelwch a bod y rhain yn cael eu hadrodd i'r uwch dîm arweinyddol;
- rheoli a monitro risgiau ac asedau gwybodaeth o fewn yr ysgol;
- sicrhau bod y camau angenrheidiol wedi'u cymryd i ddiogelu'r seilwaith technegol a bodloni gofynion technegol systemau technoleg gwybodaeth a chyfathrebu'r ysgol;
- cynnal archwiliadau mewnol sydd yn monitro cydymffurfiad;
- sicrhau bod proses gadarn ar waith i ganfod a nodi achosion o dor-rheolau data; ymchwilio ac asesu achosion o dor-rheolau data gan gynnwys risgiau a

rhannu unrhyw ddigwyddiadau diogelwch data gyda'r Swyddog Diogelu Data Ysgolion;
- cysylltu â'r Swyddog Diogelu Data Ysgolion wrth weithredu neu newid proses neu system, er mwyn penderfynu a oes angen DPIA ai peidio;
- sefydlu diwylliant o adrodd a dysgu er mwyn galluogi'r ysgol sefydlu lle mae problemau yn bodoli ac i ddatblygu strategaethau gyda'r Swyddog Diogelu Data Ysgolion er mwyn atal problemau rhag godi yn y dyfodol.

5.3. Holl Staff yr Ysgol

Mae'r holl staff sy'n cael eu cyflogi neu'n gwirfoddoli yn yr ysgol, gan gynnwys athrawon, cymorthyddion dosbarth a staff cymorth busnes, yn gyfrifol am:

- ddefnyddio technoleg gwybodaeth a chyfathrebu yn unol â'r polisi hwn a'r hyfforddiant a ddarperir;
- sicrhau diogelwch a lles pobl eraill, ar-lein ac all-lein;
- bod yn ymwybodol o'r broses o gael gafael ar gymorth ac arweiniad sy'n ymwneud â chodi pryderon ac ymateb i bryderon diogelwch ar-lein a cheisio cymorth ac arweiniad sy'n ymwneud â hynny;
- gweithio'n ddiogel ac yn gyfrifol, i fodelu ymddygiad cadarnhaol ar-lein ac i reoli safonau ac arferion proffesiynol wrth ddefnyddio technoleg;
- ymgymryd ag unrhyw hyfforddiant e-ddiogelwch a gynhigir.

5.4. Swyddog Diogelu Data Ysgolion

Mae'r Swyddog Diogelu Data Ysgolion yn gyfrifol am:

- fonitro gweithrediad a chydymffurfiad yr ysgol âr polisi ac i fonitro trefniadau diogelwch o fewn yr ysgol;
- roi arweiniad i ysgolion ar gytundebau sy'n ymwneud ag apiau, meddalwedd a systemau technoleg gwybodaeth a chyfathrebu;
- sicrhau bod staff yr ysgol wedi'u hyfforddi'n ddigonol mewn perthynas ag e-ddiogelwch;
- cynorthwyo'r Pennaeth i benderfynu a oes angen DPIA ai peidio wrth weithredu neu newid proses neu system (gan ddefnyddio technolegau newydd);
- darparu cyngor a chymorth ac arwain ar adrodd am achosion o dor-rheolau data.

6. Beth yw e-ddiogelwch?

Nid yn unig y mae e-ddiogelwch yn cynnwys technoleg rhyngrwyd ond hefyd ffurfiau electronig o gyfathrebu megis ffonau symudol a thechnoleg ddiwifr. Mae e-ddiogelwch yn sefydlu mesurau diogelu ac yn annog ymwybyddiaeth, gan sicrhau bod defnyddwyr yn rheoli eu profiadau ar-lein mewn modd diogel a chadarnhaol.

Mae'r rhyngrwyd yn sianel gyfathrebu agored y mae unrhyw un yn rhydd i'w defnyddio. Gall y We Fyd-eang, e-bost, blogiau a rhwydweithio cymdeithasol

drosglwyddo gwybodaeth ledled y byd drwy'r rhyngrwyd am ychydig iawn o gost. Gall unrhyw un anfon negeseuon, trafod syniadau a chyhoeddi deunydd heb lawer o gyfyngiadau. Mae hyn yn gwneud y rhyngrwyd yn adnodd amhrisiadwy a ddefnyddir gan filiynau o bobl bob dydd.

Cyhoeddir llawer o'r deunydd a geir ar y rhyngrwyd ar gyfer oedolion, ac mae rhywfaint ohono'n amhriodol i blant. Gellir dod o hyd i wybodaeth hefyd am arfau, troseddau a hiliaeth, a dyma'r ffordd hawsaf o gael gafael ar wybodaeth o'r fath. Mae angen i ddisgyblion hefyd ddysgu y gall cyhoeddi deunydd personol beryglu eu diogelwch personol a diogelwch pobl eraill.

7. Beth mae cyfathrebu'n electronig yn ei gynnwys?

Gall cyfathrebu electronig gynnwys gwahanol ddulliau ac arddulliau cyfathrebu sy'n cynnwys, ond nid yn gyfyngedig i:

- ffyrdd o ryngweithio ar y rhyngrwyd: safleoedd rhwydweithio cymdeithasol a gwe-logiau (blogiau);
- dysgu ar-lein; dysgu drwy ystafell ddosbarth rithwir drwy'r rhyngrwyd (dysgu cydamserol a dysgu anghydamserol);
- ymchwil ar y rhyngrwyd: gwefannau, peiriannau chwilio a phorwyr gwe;
- ffonau symudol a chymhorthion digidol personol (PDAs);
- cyfathrebu drwy'r rhyngrwyd: e-bost a negeseuon gwib;
- gwe-gamerâu a fideo-gynadledda;
- consolau gemau di-wifr.

Mae technoleg ffonau symudol wedi datblygu'n sylweddol dros y blynyddoedd diwethaf - ac mae'n parhau i esblygu. Mae cysylltiadau di-wifr yn arbennig wedi ymestyn galluoedd ffonau symudol, gan alluogi mynediad i ystod eang o gynnwys a gwasanaethau newydd yn fyd-eang. Mae llawer o ffonau bellach yn cynnig mynediad i'r rhyngrwyd ac e-bost, ochr yn ochr â swyddogaethau safonol negeseuon, camera, fideo a recordio sain amlaf. Mae ffonau symudol, ochr yn ochr â mathau eraill o dechnoleg, yn newid y ffordd a'r cyflymder yr ydym yn cyfathrebu.

Dylai rhieni ac athrawon fod yn ymwybodol bod gan y rhyngrwyd fannau a rhwydweithiau cymdeithasol sy'n dod i'r amlwg ar-lein sy'n caniatáu i unigolion gyhoeddi cynnwys di-gyfyngol.

Mae ysgrifennu ar gyfer cynulleidfa yn bwysig i ddatblygiad iaith ac yn sgil bywyd hanfodol. Fodd bynnag, dylid annog myfyrwyr i fod yn ofalus ynghylch datgelu gormod o wybodaeth bersonol ac am yr anhawster o gael gwared ar destun amhriodol, delweddau neu gynnwys arall unwaith y caiff ei gyhoeddi.

8. Defnydd o dechnoleg newydd mewn addysg

Dylid ymchwilio i dechnolegau newydd er mwyn asesu eu budd addysgol, a rhaid gwneud **asesiad risg** cyn rhoi caniatâd i ddefnyddio'r dechnoleg yn yr ysgol.

Mae ysgolion yn defnyddio amrywiaeth eang o dechnolegau a chyfleoedd dysgu newydd, gan gynnwys:

- ffonau symudol sy'n cael eu pweru gan gyfrifiadur y gellir eu cysylltu â'r rhyngrwyd, Bluetooth a chamera isgoch;
- dysgu ar-lein drwy dechnolegau fel Microsoft Teams a Google Classroom y tu allan i'r ysgol;
- amgylcheddau dysgu newydd fel Moodle a llwyfannau dysgu eraill;
- sgiliau meddwl sy'n cael eu herio gan gemau ac efelychiadau;
- negeseuon llais ar y rhyngrwyd fel Skype a linc IWB;
- adrodd straeon digidol sy'n cynnwys meddwl annibynnol a hunan-gymhelliant;
- podledu, darlledu a recordio gwersi;
- fideo digidol.

Gall rhai o'r technolegau hyn ddiflannu. Bydd eraill yn esblygu. Yr hyn sy'n bwysig yw cyfuno gallu pobl ifanc i arbrofi gyda doethineb athrawon er mwyn datblygu'r defnydd priodol, effeithiol a diogel o dechnoleg mewn dysgu ac addysgu.

9. Dysgu ac addysgu

9.1. <u>Pam bod defnyddio'r rhyngrwyd yn bwysig?</u>

- diben defnyddio'r rhyngrwyd yn yr ysgol yw codi safonau addysgol, hwyluso cyrhaeddiad disgyblion, cefnogi gwaith proffesiynol staff a gwella swyddogaethau rheoli'r ysgol;
- mae defnyddio'r rhyngrwyd yn rhan o'r cwricwlwm statudol ac yn offeryn hanfodol ar gyfer dysgu;
- gall y rhyngrwyd ddarparu dysgu y tu allan i'r ysgol megis dysgu ar-lein gartref yn ystod cyfnodau y mae'n rhaid cau ysgolion neu na all disgyblion fynychu'r ysgol;
- mae mynediad i'r rhyngrwyd yn un o hawliau disgyblion sy'n dangos agwedd gyfrifol ac aeddfed tuag at ddefnyddio'r cyfryngau;
- mae'r rhyngrwyd yn elfen hanfodol o fywyd yn yr unfed ganrif ar hugain mewn perthynas ag addysg, busnes a chysylltiadau cymdeithasol. Mae'n ddyletswydd ar yr ysgol i roi mynediad hawdd i ddisgyblion i'r rhyngrwyd fel rhan o'u profiad dysgu;
- mae disgyblion yn gwneud defnydd helaeth o'r rhyngrwyd y tu allan i'r ysgol, ac mae angen iddynt ddysgu sut i werthuso'r wybodaeth ar y we a bod yn gyfrifol am eu diogelwch eu hunain.

9.2. <u>Sut mae defnyddio'r rhyngrwyd yn fuddiol i addysg?</u>

Mae'r canlynol yn rai o'r buddion o ddefnyddio'r rhyngrwyd mewn addysg:

- mynediad at ddysgu lle bynnag a phryd bynnag y mae'n gyfleus, gan gynnwys dysgu ar-lein gartref ac fel rhan o drefniadau dysgu cyfunol;
- mynediad at adnoddau byd-eang gan gynnwys amgueddfeydd ac orielau celf;
- bod yn rhan o Hwb (Llwyfan Dysgu Digidol Cenedlaethol) sy'n cysylltu pob ysgol yng Nghymru;
- cyfnewid addysgol a diwylliannol rhwng disgyblion ledled y byd;
- adnoddau galwedigaethol, cymdeithasol a hamdden mewn llyfrgelloedd, clybiau ac yn y cartref;
- mynediad i ddisgyblion a staff at arbenigedd mewn sawl maes;
- datblygiad proffesiynol i staff sy'n gallu manteisio ar ddatblygiadau cenedlaethol, adnoddau addysgol ac arfer effeithiol ar gyfer addysgu'r cwricwlwm;
- cydweithredu ar draws y gwasanaethau cymorth a sefydliadau proffesiynol;
- gwell mynediad at gymorth technegol, gan gynnwys rheoli rhwydweithiau o bell a diweddariadau awtomatig ar gyfer systemau;
- cyfnewid data cwricwlwm a gweinyddol gyda'r Awdurdod a Llywodraeth Cymru.

9.3. <u>Sut gall defnyddio'r rhyngrwyd wella dysgu?</u>

- bydd y rhyngrwyd yn darparu mynediad i ddysgu ar-lein pan nad yw'r ysgol ar agor neu pan na all disgyblion fynychu'r ysgol i sicrhau bod y dysgu'n parhau;
- bydd mynediad i'r rhyngrwyd yn cael ei gynllunio'n benodol at ddefnydd disgyblion, a bydd yn cynnwys system hidlo sy'n briodol ar gyfer oedran y disgyblion;
- dylai staff roi arweiniad i ddisgyblion am weithgareddau ar-lein a fydd yn cefnogi deilliannau dysgu a gynllunnir yn ôl oedran ac aeddfedrwydd y disgyblion;
- mae disgyblion yn derbyn arweiniad ar ddefnydd derbyniol ac annerbyniol o'r rhyngrwyd, a rhoddir amcanion clir iddynt wrth ddefnyddio'r rhyngrwyd;
- mae mynediad i'r rhyngrwyd wedi'i gynllunio gyda'r nod o wella ac ymestyn gweithgareddau dysgu. Bydd lefelau mynediad yn cael eu diwygio yn ôl gofyniad y cwricwlwm ac oedran y disgyblion;
- bydd disgyblion yn cael eu haddysgu i ddefnyddio'r rhyngrwyd yn effeithiol mewn gwaith ymchwil, gan gynnwys sgiliau sy'n eu galluogi i ddod o hyd i wybodaeth, ei hadalw a'i gwerthuso.

10. Llwybrau i e-ddiogelwch

Rhaid i staff a disgyblion ddeall bod defnyddio rhwydwaith yr ysgol yn fraint y gellir ei dileu ar unrhyw adeg os oes digon o reswm dros wneud hynny. Mae'r ysgol yn gallu monitro'r holl ddefnydd o'r rhwydwaith a'r rhyngrwyd er mwyn sicrhau diogelwch disgyblion.

10.1. <u>Egwyddorion cyffredinol</u>

Dylai defnydd o dechnoleg gwybodaeth a chyfathrebu ddilyn yr egwyddorion cyffredinol canlynol:

- mae systemau technoleg gwybodaeth a chyfathrebu'r ysgol wedi'u bwriadu'n bennaf at ddefnydd addysgol a rheoli a gweinyddu'r ysgol;
- rhaid dilyn deddfwriaeth diogelu data bob amser;
- rhaid i ddefnyddwyr beidio â cheisio defnyddio systemau at unrhyw ddibenion neu ddeunyddiau anghyfreithlon;
- dylai defnyddwyr gyfathrebu ag eraill mewn modd proffesiynol;
- ni ddylai defnyddwyr ddatgelu eu cyfrinair ac ni ddylent ei ysgrifennu na'i storio lle mae'n bosibl y gallai person arall ei ddwyn;
- ni ddylai defnyddwyr geisio defnyddio enw defnyddiwr neu gyfrinair person arall;
- rhaid i ddefnyddwyr adrodd cyn gynted â phosibl ar unrhyw ddeunydd neu ddigwyddiad sy'n ymddangos yn anghyfreithlon, yn amhriodol neu'n niweidiol i'r person a ddynodir gan yr ysgol;
- ni ddylai staff ddefnyddio safleoedd rhwydweithio cymdeithasol personol drwy systemau technoleg gwybodaeth a chyfathrebu'r ysgol.

10.2. Cyfathrebu electronig rhwng staff a disgyblion

Disgwylir i bob defnyddiwr ddilyn y rheolau etiquette (gwe-etiquette) wrth ddefnyddio'r rhwydwaith. Mae'r rhain yn cynnwys:

- bod yn gwrtais;
- defnyddio iaith briodol;
- peidio â defnyddio iaith sarhaus wrth gyfathrebu ag eraill;
- peidio â datgelu eich cyfeiriad, eich rhif ffôn nac unrhyw fanylion eraill amdanoch chi eich hun nac eraill;
- peidio â defnyddio'r rhyngrwyd mewn ffordd sy'n ymyrryd â'r ffordd y mae eraill yn defnyddio'r rhwydwaith;
- mae gweithgareddau anghyfreithlon yn cael eu gwahardd;
- ni ellir gwarantu y bydd e-bost yn breifat;
- mae rheolwyr y system yn monitro ac yn gallu cael gafael ar bob e-bost;
- bydd negeseuon sy'n ymwneud â gweithgareddau anghyfreithlon neu sy'n cefnogi gweithgareddau o'r fath yn cael eu dwyn i sylw'r awdurdodau.

11. Rheoli Systemau Gwybodaeth

Mae gan yr ysgol fesurau a phrosesau ar waith i sicrhau bod systemau gwybodaeth yn cael eu cynnal a bod ganddynt y mesurau diogelwch gofynnol ar waith a hefyd bod ganddi fesurau priodol ar waith i sicrhau bod gwybodaeth bersonol a gwybodaeth gyhoeddedig yn cael eu diogelu a'u bod yn cael eu rhannu'n briodol.

11.1. Sut cynhelir diogelwch systemau gwybodaeth?

Mae gan yr ysgol y mesurau canlynol mewn lle er mwyn cynnal systemau gwybodaeth:

- bydd yr ysgol yn ceisio sicrhau bod y systemau technoleg gwybodaeth a chyfathrebu y mae'n eu defnyddio mor ddiogel ag sy'n rhesymol bosibl drwy

gymryd cyngor ac arweiniad cyfrifol ar y gofynion technegol ar gyfer y systemau hynny;
- ni ddylai dyfeisiau heb eu rheoli cael eu cysylltu i rwydwaith yr ysgol heb gytundeb Uned TGCh Cyngor Sir Ynys Môn;
- bydd yr ysgol yn cynnal adolygiadau rheolaidd o ddiogelwch ei systemau technoleg gwybodaeth a chyfathrebu drwy contractwyr/darparwyr cefnogaeth sydd efo'r sgiliau addas;
- bod diogelu rhag firysau yn cael ei ddiweddaru'n rheolaidd;
- mae rhwydwaith yr ysgol wedi ei wahanu i fewn i is-rwydweithiau rhesymegol ac efo wal dân sydd yn unol âg anghenion y defnyddwyr a lefel diogelwch y defnyddwyr ar y rhwydwaith;
- bydd systemau yr ysgol yn darparu mynediad wedi'i hidlo i'r rhyngrwyd ar gyfer pob defnyddiwr fydd yn atal cynnwys anghyfreithlon, gyda hidlo ychwanegol ar gyfer grwpiau gwahanol o ddefnyddwyr, ar gyfer cynnwys amhriodol yn unol â canllawiau wedi eu creu gan Llywodraeth Cymru- https://hwb.gov.wales/api/storage/b6c34ed3-8499-4ba9-971f-b4299232096e/education-digital-standards_web-filtering_20211012_ll-500551-w-2.pdf
- bydd strategaethau wrth gefn (gan gynnwys gofynion all-lein ac all-safle) yn cael eu hystyried a byddant yn cyfateb i ofynion yr ysgol o ran adalw os bydd trychineb;
- bydd strategaethau diogelwch yn cael eu trafod gyda Gwasanaeth TGCh Cyngor Sir Ynys Môn lle bo hynny'n briodol;
- bydd data personol a anfonir dros y rhyngrwyd yn cael ei amgryptio neu ei wneud yn ddiogel drwy ddulliau eraill;
- rhoddir sylw arbennig i ddiogelu cyfrinair ac amgryptio ar gyfer dyfeisiau sydd wedi'u lleoli yn yr ysgol a dyfeisiau symudol;
- ni ellir defnyddio dyfais gludadwy heb ganiatâd penodol a chael archwiliad ar gyfer firysau;
- ni roddir caniatâd ar gyfer cyfleusterau system nad ydynt wedi'u cymeradwyo na ffeiliau y gellir eu hactifadu yng ngwaith y disgyblion neu a anfonir drwy e-bost;
- ffeiliau a gedwir ar rwydwaith yr ysgol yn cael eu harchwilio'n rheolaidd;
- bydd y cydgysylltydd TGCh/rheolwr rhwydwaith yn adolygu capasiti'r system yn rheolaidd;
- gall monitro ychwanegol ddigwydd fel rhan o ymchwiliad yn dilyn tystiolaeth o gamddefnydd ymddangosiadol;
- bydd staff yr ysgol yn cydymffurfio â'r *Polisi Diogelwch Gwybodaeth Ysgolion*.

11.2. Sut rheoleiddir e-bost?

Mae gan yr ysgol y mesurau canlynol ar waith i reoleiddio defnydd o e-byst:

- dim ond cyfrifon e-bost a gymeradwyir gan yr ysgol y gall disgyblion eu defnyddio;
- dim ond cyfrifon e-bost swyddogol, ysgol y gall staff eu defnyddio i gyfathrebu â disgyblion;
- rhaid i ddisgyblion hysbysu athro ar unwaith os ydynt yn derbyn e-bost sarhaus;

- rhaid i ddisgyblion beidio â datgelu manylion personol amdanynt eu hunain nac eraill mewn neges e-bost, na threfnu i gwrdd ag unrhyw un heb ganiatâd penodol;
- gall gorddefnyddio negeseuon e-bost cymdeithasol lesteirio dysgu, ac felly mae cyfyngiadau ar waith;
- dylid cymryd gofal wrth e-bostio sefydliadau allanol a dylid ceisio caniatâd cyn anfon e-bost, fel gyda llythyrau wedi'u hysgrifennu ar bapur pennawd;
- ni roddir caniatâd i anfon llythyrau cadwyn i gyfeiriadau eraill:
- bydd staff yr ysgol yn cydymffurfio â *Pholisi E-bost Staff Ysgolion.*

11.3. Sut rheoleiddir cynnwys cyhoeddedig?
Mae gan yr ysgol y mesurau canlynol ar waith i reoleiddio cynnwys cyhoeddedig:

- dylid cynnwys cyfeiriad, cyfeiriad e-bost a rhif ffôn yr ysgol fel manylion cyswllt ar y wefan. Ni ddylid cyhoeddi gwybodaeth bersonol am staff neu ddisgyblion;
- bydd yr UDA a'r tîm gweinyddol yn gyfrifol yn gyffredinol am olygu'r deunydd a sicrhau ei fod yn gywir ac yn briodol;
- dylid bod yn ofalus wrth gyhoeddi cyfeiriadau e-bost er mwyn osgoi derbyn e-byst sothach;
- dylai gwefan/cyfrifon rhwydwaith cymdeithasol yr ysgol gyfateb i ganllawiau'r ysgol ar gyfer cyhoeddiadau, gan gynnwys parch at eiddo deallusol a hawlfraint;
- bydd staff yr ysgol yn cydymffurfio â *Pholisi Cyfryngau Cymdeithasol Staff Ysgolion* a *Pholisi Tynnu Lluniau at Pwrpas Cyhoeddusrwydd Ysgolion.*

11.4. A ellir cyhoeddi gwaith neu luniau o ddisgyblion?
Mae gan yr ysgol fesurau ar waith i sicrhau bod ffotograffau, delweddau a gwybodaeth bersonol ond yn cael eu rhannu dan rai amgylchiadau a gyda'r camau canlynol ar waith:

- lluniau a delweddau sy'n cynnwys disgyblion yn cael eu dewis yn ofalus. Ni ddylai testun sy'n cyd-fynd â lluniau adnabod disgyblion unigol;
- ni ddefnyddir enwau disgyblion yn unman ar wefan yr ysgol na chyfrifon cyfryngau cymdeithasol mewn cysylltiad â ffotograffau a delweddau;
- ceisir cymeradwyaeth ysgrifenedig gan rieni/gofalwyr cyn i luniau o ddisgyblion gael eu cynnwys ar wefan yr ysgol/cyfrifon cyfryngau cymdeithasol drwy ffurflenni caniatâd. Ni fydd yr ysgol yn rhannu gwybodaeth bersonol am ddisgyblion heb i rieni/gofalwyr roi caniatâd i wneud hynny;
- dim ond gyda chydsyniad y disgybl a'i rieni/gofalwyr y gellir cyhoeddi gwaith.
- bydd yr ysgol yn cydymffurfio â'r *Polisi Tynnu Lluniau at Ddibenion Cyhoeddusrwydd Ysgolion.*

11.5. Sut rheoleiddir rhwydweithio cymdeithasol a chyhoeddi personol?
Bydd gan yr ysgol y mesurau canlynol ar waith i reoleiddio'r hyn sydd ar gael o ran gwefannau a chyfryngau cymdeithasol a'r hyn a gyhoeddir:

- bydd yr ysgol yn rhwystro/hidlo mynediad i safleoedd rhwydweithio cymdeithasol. Ar hyn o bryd mae gwasanaeth hidlo Cyngor Sir Ynys Môn yn

rhwystro mynediad i nifer o safleoedd rhwydweithio cymdeithasol. Fodd bynnag, mae ysgolion yn gyfrifol am roi gwybodaeth am unrhyw safleoedd eraill y gallai fod angen iddynt eu hidlo/blocio;

- bydd fforymau amhriodol yn cael eu rhwystro;
- cynghorir disgyblion i beidio byth â rhoi unrhyw fanylion personol sy'n rhoi gwybodaeth am eu hunaniaeth neu eu lleoliad. Mae enghreifftiau'n cynnwys enw go iawn, cyfeiriad, rhif ffôn symudol neu rif tŷ, yr ysgol a fynychwyd, cyfeiriadau IM ac e-bost, enwau llawn ffrindiau, diddordebau penodol a chlybiau ac ati;
- dylid dweud wrth ddisgyblion am beidio â chynnwys lluniau personol ar unrhyw ofod rhwydwaith cymdeithasol. Dylent ystyried pa mor gyhoeddus y gallai'r wybodaeth fod, ac ystyried defnyddio ardaloedd preifat. Dylid rhoi cyngor ar unrhyw fanylion cefndir yn y llun a allai adnabod y disgybl neu ei leoliad e.e. rhif tŷ, enw stryd neu ysgol;
- dylid defnyddio cyfrineiriau i ddiogelu blogiau neu wicis swyddogol a wneir gan athrawon, a dylid rhedeg y rhain ar wefan yr ysgol. Dylid cynghori athrawon i beidio â rhedeg mannau rhwydweithio cymdeithasol at ddefnydd personol disgyblion;
- dylid cynghori disgyblion am ddiogelwch a'u hannog i greu cyfrineiriau, gwrthod mynediad i unigolion nad ydynt yn eu hadnabod, a chael eu hyfforddi ar sut i atal negeseuon annymunol. Dylid annog disgyblion i wahodd ffrindiau yn unig, ac i wrthod mynediad i eraill;
- dylid cynghori disgyblion i ymatal rhag cyhoeddi meddyliau preifat penodol, manwl;
- dylai ysgolion fod yn ymwybodol y gall bwlio ddigwydd drwy rwydweithio cymdeithasol, yn enwedig lle sydd wedi'i greu nad yw wedi'i ddiogelu gan gyfrinair ac eraill wedi'u gwahodd i weld sylwadau'r bwli;
- bydd staff yr ysgol yn cydymffurfio â'r *Polisi Tynnu Lluniau at Bwrpas Cyhoeddusrwydd Ysgolion, Polisi Cyfryngau Cymdeithasol Staff Ysgolion* a *Pholisi Diogelwch Gwybodaeth Ysgolion.*

11.6. <u>Sut rheoleiddir ffiltro?</u>
Mae gan yr ysgol y mesurau canlynol ar waith i reoleiddio ffiltro:

- bydd yr ysgol yn gweithio gyda Gwasanaeth TGCh Cyngor Sir Ynys Môn, i sicrhau bod systemau sy'n amddiffyn disgyblion yn cael eu diwygio a'u gwella'n rheolaidd;
- os bydd staff neu ddisgyblion yn darganfod gwefannau amhriodol, rhaid rhoi'r URL i'r Cydgysylltydd TGCh a'r rheolwr systemau, i'w anfon ar unwaith i Ddesg Gymorth Gwasanaethau TG Cyngor Sir Ynys Môn a'i ddosbarthu i bob system ysgol;
- bydd yr holl fynediad i'r rhyngrwyd yn yr ysgol yn cael ei gofnodi;
- bydd defnydd o'r rhyngrwyd yn cael ei fonitro ar hap i sicrhau ei fod yn cydymffurfio â pholisi'r ysgol;
- mae'r holl fynediad i'r rhyngrwyd yn yr ysgol wedi'i hidlo. O dan amgylchiadau prin, bydd gwir angen osgoi cyfyngiadau technegol drwy ddefnyddio cysylltiad

heb ei hidlo. Dylai'r Pennaeth roi caniatâd personol bob tro y defnyddir y rhyngrwyd heb hidlydd, ac adolygu'r angen am fynediad rheolaidd;
- mae'r ysgol yn defnyddio cyfuniad o fynediad *Walled Garden* a mynediad wedi'i hidlo sy'n briodol ar gyfer oedran disgyblion, i gefnogi amcanion addysgeg;
- mae'r *Polisi E-Ddiogelwch Ysgolion* yn gydnaws â pholisi'r ysgol o ran disgyblaeth;
- bydd uwch aelodau o staff yn sicrhau bod dulliau hidlo yn cael eu hadolygu'n rheolaidd er mwyn sicrhau bod y dulliau hynny'n briodol, yn effeithiol ac yn rhesymol;
- rhaid rhoi gwybod i'r asiantaethau priodol am unrhyw ddeunydd y mae'r ysgol yn credu ei fod yn anghyfreithlon;
- bydd staff yr ysgol yn cydymffurfio â'r *Polisi Diogelwch Gwybodaeth Ysgolion.*

11.7. Sut caiff fideo-gynadledda ei fonitro?

Mae gan yr ysgol y mesurau canlynol ar waith ynglŷn â fideo-gynadledda:

- dylid diffodd yr holl offer fideo-gynadledda yn y dosbarth pan nad yw'n cael ei ddefnyddio;
- mae offer sy'n gysylltiedig â Rhwydwaith Dysgu Gydol Oes Cymru yn defnyddio'r system rolau E.164 genedlaethol;
- ni ddylai cyfeiriadau IP allanol fod ar gael i safleoedd eraill;
- ni ddylid cynnwys gwybodaeth gyswllt fideo-gynadledda ar wefan yr ysgol;
- rhaid cadw'r offer yn ddiogel a'i gloi os oes angen pan nad yw'n cael ei ddefnyddio;
- ni ddylid mynd ag offer fideo-gynadledda i ffwrdd o safle'r ysgol heb ganiatâd. Ni ellir monitro na rheoli'r ffordd y defnyddir rhwydwaith ar unrhyw rwydwaith ar wahân i'r rhwydwaith addysgol.

11.7.1. Defnyddwyr

- dylai disgyblion ofyn am ganiatâd yr athro neu'r athrawes sy'n goruchwylio cyn gwneud neu ateb galwad fideo-gynadledda;
- dylai fideo-gynadledda gael ei oruchwylio'n briodol yn ôl oedran y disgyblion;
- rhaid cymryd gofal mawr wrth ddirprwyo'r cyfrifoldeb am ddefnyddio offer fideo-gynadledda y tu allan i oriau ysgol;
- dim ond aelodau allweddol o staff ddylai gael mynediad i'r system fideo-gynadledda, y wefan neu'r dudalen reoli o bell arall sydd ar gael ar systemau mwy;
- dim ond aelodau o staff ddylai gael mynediad at unrhyw fanylion mewngofnodi a chyfrineiriau unigryw ar gyfer y gwasanaethau fideo-gynadledda addysgol, a dylid cadw'r manylion hyn mewn man diogel.

11.7.2. Cynnwys

- wrth recordio gwers fideo-gynadledda, rhaid rhoi'r rheswm dros y recordio ac ar ddechrau'r gynhadledd dylid ei gwneud yn glir i bawb sy'n cymryd rhan bod y gynhadledd yn cael ei recordio;

- rhaid i ddeunydd sy'n cael ei recordio gael ei storio'n ddiogel yn unol â'r *Cyfnodau Cadw Ysgolion*;
- os cynhwysir deunydd sy'n perthyn i drydydd parti, dylai staff sicrhau bod recordio yn dderbyniol er mwyn osgoi tramgwyddo hawliau eiddo deallusol y trydydd parti;
- mae fideo-gynadledda yn weithgaredd heriol sy'n rhoi amrywiaeth eang o fanteision dysgu i ddisgyblion. Mae paratoi a gwerthuso yn rhannau hanfodol o'r gweithgaredd cyfan;
- dylid cynnal deialog ag eraill sy'n ymwneud â'r gynhadledd cyn cymryd rhan yn y gynhadledd fideo. Os yw'r gynhadledd yn cael ei chynnal ar safle gwahanol, i ffwrdd o'r ysgol, mae'n bwysig ei bod yn darparu deunydd sy'n briodol i'r dosbarth.

11.8. <u>Sut gaiff dysgu ar-lein ei fonitro?</u>
Mae gan yr ysgol y mesurau canlynol ar waith ynglŷn â dysgu ar-lein:

- anogir disgyblion i weithio o leoliad cartref addas a rennir lle maent yn teimlo'n gyfforddus;
- argymhellir bod athrawon a disgyblion yn defnyddio'r cyfleuster sy'n gallu newid neu gymylu arddangosiad cefndir;
- nid oes rhaid i ddisgyblion roi eu camerâu ymlaen - mae troi'r camera ymlaen yn ddewisol;
- mae cytundeb wedi'i sefydlu rhwng yr ysgol (athro) a rhieni/gofalwyr ynghylch disgwyliadau ac ymddygiad disgyblion a rhieni/gofalwyr yn ystod gwersi ar-lein;
- gellir recordio rhai gwersi at ddibenion diogelu. Bydd cyfranogwyr yn cael gwybod pan fydd y wers yn cael ei recordio;
- mae gan yr ysgol *Bolisi Recordio Sesiynau Ffrydio'n Fyw* a *Pholisi Cadw Recordiadau.*
- mae gan yr ysgol ganllaw ar ddysgu ar-lein i'r staff a'r rhieni.

<u>11.8.1. Mae athrawon yn cytuno i:</u>

- fod yn brydlon ar ddechrau a diwedd pob gwers;
- trafod rolau a chyfrifoldebau gyda disgyblion ar ddechrau pob gwers;
- creu a chytuno ar reolau sylfaenol a safonau ymddygiad clir yn seiliedig ar bolisi rheoli ymddygiad cyfredol yr ysgol;
- cyfleu'n glir y disgwylir ymddygiad 'safon ystafell ddosbarth' gan bawb sy'n bresennol;
- sefydlu disgwyliadau o'r dechrau ac egluro'r rheolau drwy roi cyflwyniad i'r sesiwn (e.e. pwy sy'n cael siarad, sut i ofyn cwestiwn neu ofyn am help);
- hysbysu uwch dîm rheoli'r ysgol, disgyblion a rhieni/gofalwyr am unrhyw wersi a drefnwyd, gwersi a ganslwyd neu newidiadau mewn trefniadau;
- sicrhau eu bod yn diweddaru eu hunain ar yr holl bolisïau a gweithdrefnau perthnasol, gan gynnwys polisïau diogelwch ar-lein, diogelu a diogelu data;

- atal sefyllfa un-i-un ar ddiwedd dosbarth ar-lein drwy ddatgysylltu'r holl gyfranogwyr ar ddiwedd y wers.

11.8.2. Mae rhieni/gofalwyr yn cytuno i:
Mae rhieni/gofalwyr yn cytuno y bydd eu plentyn yn dilyn y rheolau a'r disgwyliadau defnydd:

- caniateir i'r disgybl ymuno â gwersi ar-lein yr ysgol ar yr amod bod y disgybl fel dysgwr a'r rhiant/gofalwr yn ymrwymo i'r cod ymddygiad;
- rhiant/gofalwr i ymrwymo i ddarllen a thrafod y cod ymddygiad gyda'r disgybl;
- bydd y disgybl yn brydlon i bob gwers;
- mae gan ddisgyblion fynediad i'r ffeiliau perthnasol ar gyfer pob gwers ymlaen llaw ac mae'r deunyddiau wrth law;
- mae dyfais y disgybl (gliniadur/Chromebook/PC ac ati) yn barod cyn i'r wers ddechrau gyda'r disgybl eisoes wedi mewngofnodi i'w gyfrif;
- rhiant/gofalwr i wneud ei orau i sicrhau bod y disgybl wedi'i wisgo'n iawn. Mae rhiant/gofalwr yn deall nad yw gwisgo dillad nos yn cael ei ystyried yn ddillad priodol;
- rhiant/gofalwr i geisio sicrhau bod y disgybl mewn ystafell addas e.e. ystafell fyw neu ystafell fwyta ac ystyried cefndir, ongl camera, preifatrwydd ac ati;
- rhiant/gofalwr i geisio sicrhau nad oes dim byd arall yn digwydd yn yr ystafell e.e. yn ceisio sicrhau nad yw'r brodyr a chwiorydd yn yr ystafell yn chwarae, bod y teledu wedi'i ddiffodd ac nad oes dim yn tynnu sylw nac yn torri ar draws y wers/cyfarfod. Os nad yw hyn yn bosibl, bydd yn gwneud ei orau i sicrhau bod awyrgylch yr ystafell yn addas i'r disgybl gael gwers gyda grŵp o ddisgyblion eraill. Os nad yw hyn yn bosibl, bydd y meicroffon yn cael ei fudo er mwyn atal y sŵn yn yr ystafell rhag tarfu ar y wers;
- mae rhiant/gofalwr yn deall y disgwylir yr un safonau ymddygiad â phe bai'r disgybl yn yr ysgol. Mae rhiant/gofalwr yn deall y bydd yr athro/athrawes yn torri cyswllt os yw'r disgybl yn arddangos unrhyw ymddygiad amhriodol;
- rhiant/gofalwr i geisio sicrhau bod y disgybl yn dangos parch at bawb yn yr ystafell ddosbarth ar-lein ac yn ceisio cyfrannu at y dosbarth mewn modd cadarnhaol a heb fod yn aflonyddgar ar unrhyw adeg;
- nad oes unrhyw ran o'r wers/cyfarfod yn cael ei recordio ar unrhyw ddyfais nac unrhyw luniau'n cael eu tynnu gan unrhyw un yn y cartref;
- ni fydd rhiant/gofalwr yn ymuno â'r wers/cyfarfod nac yn tarfu arni;
- os oes gan riant/gofalwr bryder, maent yn deall na ddylid mynegi hyn yn ystod y wers/cyfarfod. Gall rhiant/gofalwr drafod y pryder drwy gysylltu â'r ysgol ar ôl y wers.

11.9. Sut mae disgyblion yn dysgu sut i werthuso cynnwys ar y rhyngrwyd?

- bydd yr ysgol yn sicrhau bod deunyddiau a geir o'r rhyngrwyd sy'n cael eu copïo neu eu defnyddio ar adegau eraill gan staff a disgyblion yn cydymffurfio â chyfraith hawlfraint;

- dylid addysgu disgyblion i fod yn ymwybodol iawn o'r deunyddiau y maent yn eu darllen, a dylid dangos iddynt sut i ddilysu gwybodaeth cyn ei derbyn yn gywir;
- bydd disgyblion yn cael eu haddysgu i gydnabod ffynhonnell yr wybodaeth y maent yn ei defnyddio ac i barchu hawlfraint wrth ddefnyddio deunyddiau rhyngrwyd yn eu gwaith.

11.10. Sut gellir rheoleiddio'r dechnoleg ddiweddaraf?
Bydd gan yr ysgol y mesurau canlynol ar waith i reoleiddio technoleg:

- bydd y technolegau diweddaraf yn cael eu harchwilio am eu gwerth addysgol, a bydd asesiad risg yn cael ei wneud cyn rhoi caniatâd i'w defnyddio yn yr ysgol;
- ni ddylid defnyddio ffonau symudol yn ystod gwersi nac yn ystod amser gwersi ffurfiol; gwaharddir negeseuon testun ymosodol neu amhriodol;
- bydd yr ysgol yn cydymffurfio â'r *Polisi Diogelwch Gwybodaeth Ysgolion.*

12. Sut y diogelir data personol?

Bydd yr ysgol yn sicrhau bod ei systemau technoleg gwybodaeth a chyfathrebu yn cydymffurfio â gofynion deddfwriaeth diogelu data. Caiff data personol ei gofnodi, ei brosesu, ei drosglwyddo a'i ddarparu ar-lein yn unol â'r *Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR)* a *Deddf Diogelu Data 2018*.

Bydd pob defnyddiwr yn cydymffurfio â *Pholisi Diogelu Data Ysgolion* a *Pholisi Diogelwch Gwybodaeth Ysgolion*, gan gynnwys y gofyniad i storio gwybodaeth yn ddiogel.

Os bydd digwyddiad diogelwch data o ganlyniad i ddefnyddio'r rhyngrwyd, gwefan, cyfrif cyfryngau cymdeithasol, dysgu ar-lein ac ati, bydd yr ysgol yn hysbysu'r Swyddog Diogelu Data Ysgolion ar unwaith a bydd yn cydymffurfio â'r *Polisi Digwyddiadau Diogelwch Data Ysgolion.*

13. Penderfyniadau Polisi

13.1. Sut awdurdodir mynediad i'r rhyngrwyd?
- bydd yr ysgol yn cadw cofnod parhaus o bob aelod o staff a disgybl sydd â chaniatâd i gael mynediad at ddolenni electronig yr ysgol;
- rhaid i ddisgyblion wneud cais unigol am fynediad i'r rhyngrwyd drwy gytuno i gydymffurfio â'r rheolau e-ddiogelwch;
- gofynnir i rieni lofnodi a dychwelyd ffurflen sy'n rhoi caniatâd i ddisgyblion gael mynediad i'r rhyngrwyd;
- hysbysir rhieni y bydd disgyblion yn cael mynediad i'r rhyngrwyd dan oruchwyliaeth.

13.2. Sut asesir risg?

Gall technoleg ddarparu diogelwch a sicrwydd; fodd bynnag, mae risgiau cysylltiedig hefyd. Mae angen i ddisgyblion ddeall y risgiau hyn er mwyn eu helpu i ddatblygu strategaethau priodol ar gyfer cadw eu hunain yn ddiogel.

Gellir categoreiddio risgiau i blant a phobl ifanc yn fras o dan y penawdau cynnwys, cyswllt ac ymddygiad a gellir eu rheoli drwy leihau argaeledd, cyfyngu ar fynediad a chynyddu gwydnwch.

Mae'r ysgol yn hyrwyddo arfer diogel a phriodol drwy sefydlu canllawiau defnydd derbyniol clir a chadarn. Cyflawnir hyn drwy gydbwyso diogelwch rhag camddefnydd posibl gan gydnabod bod technoleg yn arf cyfathrebu effeithiol.

Bydd yr ysgol yn cymryd pob cam rhesymol i sicrhau mai dim ond at ddeunydd priodol y caiff defnyddwyr fynediad ato. Er gwaethaf hyn, oherwydd natur fyd-eang y rhyngrwyd a'i gysylltiadau pwnc, mae'n amhosibl gwarantu na fydd deunydd amhriodol byth yn cael ei gyrchu ar gyfrifiadur ysgol. Ni all yr ysgol na Chyngor Sir Ynys Môn dderbyn cyfrifoldeb am y deunydd a gyrchir nac am unrhyw ganlyniadau a allai ddeillio o ddefnyddio'r rhyngrwyd.

Efallai y byddai'n briodol cynnal Asesiad Effaith Diogelu Data (DPIA) ar gyfer mathau o brosesu sy'n debygol o arwain at *risg uchel* i fuddiannau unigolion. Dylid ystyried a oes angen DPIA **cyn** defnyddio unrhyw dechnoleg newydd. Gall y Swyddog Diogelu Data Ysgolion roi cyngor ac arweiniad ynghylch DPIAau.

Gall defnyddio systemau cyfrifiadurol heb ganiatâd neu at ddibenion amhriodol fod yn drosedd o dan *Ddeddf Camddefnyddio Cyfrifiaduron 1990.*

Caiff y dulliau o gydnabod, asesu a lleihau'r risgiau eu hadolygu'n rheolaidd.

13.3. <u>Sut ymdrinnir â chwynion am e-ddiogelwch?</u>

- mae uwch aelod o staff yn delio â chwynion am gamddefnyddio'r rhyngrwyd;
- rhaid cyfeirio unrhyw gwynion am staff sy'n cam-ddefnyddio'r rhyngrwyd at y Pennaeth;
- disgyblion a rhieni'n cael gwybod am y weithdrefn gwyno;
- rhaid i rieni a disgyblion weithio mewn partneriaeth â staff i ddatrys materion;
- cynhelir trafodaethau gydag Uned Diogelu'r Cyhoedd Leol yr Heddlu i sefydlu gweithdrefnau ar gyfer ymdrin â throseddau posibl;
- mae'r cosbau a nodir ym mholisi'r ysgol yn cynnwys y canlynol:

    - cyfweliad/cwnsela gan y pennaeth blwyddyn;
    - hysbysu rhieni a gwarcheidwaid;
    - gwahardd mynediad i'r rhyngrwyd neu gyfrifiadur am gyfnod penodol o amser.

13.4. <u>Sut defnyddir y rhyngrwyd ar draws y gymuned?</u>

- bydd yr ysgol yn cysylltu â sefydliadau lleol i sicrhau bod dull cyffredin o ymdrin ag e-ddiogelwch;
- bydd yr ysgol yn dangos sensitifrwydd wrth ddelio â materion sy'n ymwneud â'r rhyngrwyd y mae disgyblion yn eu darganfod y tu allan i'r ysgol, e.e. safleoedd rhwydweithio cymdeithasol, ac yn cynnig cyngor priodol.

14. Polisi Cyfathrebu

14.1. Sut cyflwynir y polisi i'r disgyblion?

- bydd rheolau e-ddiogelwch yn cael eu harddangos mewn ystafelloedd sydd â mynediad i'r rhyngrwyd;
- disgyblion yn ymwybodol bod yr holl ddefnydd o'r rhyngrwyd yn cael ei fonitro;
- cyflwynir rhaglen e-ddiogelwch i godi ymwybyddiaeth o bwysigrwydd defnyddio'r rhyngrwyd yn ddiogel ac yn gyfrifol;
- dylid rhoi canllawiau ar sut i ddefnyddio'r rhyngrwyd yn gyfrifol ac yn ddiogel cyn caniatáu mynediad i'r rhyngrwyd;
- bydd modiwl ar e-ddiogelwch yn cael ei gynnwys yn y rhaglenni ABCh/TGCh sy'n cwmpasu'r defnydd o'r rhyngrwyd yn yr ysgol ac yn y cartref.

14.2. Sut trafodir y polisi â staff?

- mae pob aelod o staff yn derbyn copi o *Bolisi E-ddiogelwch* yr ysgol ac esboniad o sut i weithredu'r polisi a phwysigrwydd y polisi;
- dylai staff fod yn ymwybodol y gellir monitro ac olrhain traffig ar y rhyngrwyd; Mae gweithredu'n ddoeth ac ymddwyn mewn modd proffesiynol o'r pwys mwyaf;
- mae staff sy'n rheoli'r systemau hidlo neu'n monitro'r defnydd o TGCh yn cael eu goruchwylio gan uwch reolwyr, ac mae ganddynt weithdrefnau clir ar gyfer rhoi gwybod am unrhyw faterion sy'n peri pryder;
- darperir hyfforddiant ar sut i ddefnyddio'r rhyngrwyd yn ddiogel ac yn gyfrifol ac ar *Bolisi E-ddiogelwch* yr ysgol pryd bynnag y bo angen.

14.3. Sut rhennir y polisi â rhieni/gofalwyr?

- Mae rhieni/gofalwyr yn cael gwybod am bolisi'r ysgol drwy gylchlythyrau; llawlyfr yr ysgol a gwefan yr ysgol;
- mae materion sy'n ymwneud â'r rhyngrwyd yn cael eu trin yn sensitif, a rhoddir gwybod i rieni/gofalwyr am unrhyw gamau sydd wedi'u cymryd;
- anogir gweithio mewn partneriaeth â rhieni/gofalwyr. Gall hyn gynnwys nosweithiau rhieni sy'n cynnwys arddangosfeydd ac awgrymiadau ar sut i ddefnyddio'r rhyngrwyd yn ddiogel gartref;
- rhoddir cyngor i rieni/gofalwyr am systemau hidlo a gweithgareddau addysgol a hamdden sy'n cynnwys defnyddio'r rhyngrwyd;
- mae rhieni/gofalwyr sydd â diddordeb yn cael eu cyfeirio at y sefydliadau a restrir yn adran 18.

15. Ymateb i ddigwyddiad sy'n peri pryder

Mae technoleg rhyngrwyd a chyfathrebu electronig yn rhoi cyfle i blant a phobl ifanc ehangu eu profiadau a datblygu eu gallu creadigol yn yr ysgol a thu hwnt. Fodd bynnag, mae'n bwysig bod yn ymwybodol o beryglon defnyddio'r technolegau hyn.

Mae'r risgiau i e-ddiogelwch yn digwydd oherwydd pobl sy'n ymddwyn yn amhriodol neu hyd yn oed yn anghyfreithlon. Rhaid ymdrin ag unrhyw fater personol sy'n codi. Athrawon sydd ar y rheng flaen o amddiffyn; nhw sy'n arsylwi'r disgyblion, ac mae hyn yn hollbwysig o ran dod yn ymwybodol o risgiau i ddisgyblion ac ennill ymddiriedaeth disgyblion fel y gellir ymdrin â materion. Gall digwyddiadau amrywio o weithred ddifeddwl neu ddarn o ddrygioni i gamau anghyfreithlon sydd wedi'u cynllunio'n ofalus.

15.1. Beth yw'r peryglon?
Mae rhai peryglon posib o dechnolegau o'r fath yn cynnwys:

- derbyn cynnwys amhriodol;
- meithrin a thyfu perthynas amhriodol;
- ceisiadau am wybodaeth bersonol;
- safleoedd gwylio sy'n 'annog';
- bwlio a bygythiadau;
- dwyn hunaniaeth;
- cyhoeddi cynnwys amhriodol;
- hapchwarae ar-lein;
- camddefnyddio systemau cyfrifiadurol;
- cyhoeddi gwybodaeth bersonol;
- hacio a thorri rheolau diogelwch;
- llygru neu gamddefnyddio data;
- darparwyr nad ydynt yn cyflenwi unrhyw berchnogaeth gadarn na gwybodaeth gyswllt ar gyfer eu safleoedd;
- y peryglon sy'n gynhenid pan ellir sefydlu safleoedd gan ddefnyddio enw ffug a chyfeiriad e-bost heb wirio hunaniaeth;
- postio sylwadau dienw a allai fod yn faleisus;
- safleoedd sy'n rhoi blaenoriaeth isel i ddiogelwch defnyddwyr;
- safleoedd sy'n dathlu ymddygiad amhriodol ac annerbyniol.

15.2. Sut ddylai'r ysgol ymateb?
Gall y Swyddog Amddiffyn Plant roi arweiniad pan fydd aelod o staff yn pryderu am y defnydd a wneir o'r rhyngrwyd gan blentyn, person ifanc neu aelod o staff.

Cyfeirir at ATODIAD A. Mae'r siart llif yn dangos y camau y mae'n rhaid eu cymryd wrth ymdrin â mater sy'n peri pryder. Dim ond man cychwyn ddylai'r diagram hwn fod, gan fod y Gwasanaeth Dysgu a'r Gwasanaeth Plant a Theuluoedd yn darparu dogfennau ychwanegol i helpu ysgolion i ymateb i ddigwyddiadau sy'n ymwneud â diogelwch plant.

16. Y Fframwaith Cyfreithiol

Mae llawer o bobl ifanc a hyd yn oed aelodau o staff yn defnyddio'r rhyngrwyd yn rheolaidd heb sylweddoli bod rhai o'r gweithgareddau y maent yn eu gwneud o bosibl yn anghyfreithlon. Mae'r gyfraith yn datblygu'n gyflym ac mae newidiadau diweddar wedi'u gorfodi drwy gyfrwng y canlynol:

- Mae *Deddf Troseddau Rhywiol 2003* yn ymdrin â throseddau newydd fel meithrin perthynas amhriodol ar-lein, a gwneud/dosbarthu delweddau anweddus o blant, wedi codi oedran plentyn i 18 oed;
- *Deddf Casineb Hiliol a Chrefyddol 2006*, sy'n creu troseddau newydd sy'n ymwneud ag anogaeth casineb yn seiliedig ar gred grefyddol; a
- Mae *Deddf yr Heddlu a Chyfiawnder 2006* yn ymestyn terfynau *Deddf Camddefnyddio Cyfrifiaduron (1990*) drwy droseddoli methiant i atal ymosodiad ar y system.

16.1 Cod Plant

Ers 2 Medi 2021, mae gwasanaethau ar-lein angen dilyn cyfres o reolau pan yn defnyddio data plant. Mae'r cyfres o reolau yma yn cael eu hadnabod fel y Cod Plant.

Mae'r Cod Plant yn gyfres o reolau sydd yn bwriadu i wneud y rhyngrwyd yn le mwy diogel i blant ddysgu, ymchwilio a chwarae. Mae'n ei gwneud yn ofynnol i sefydliadau roi buddiannau gorau'r plentyn yn gyntaf pan fyddant yn dylunio ac yn datblygu apiau, gemau, teganau cysylltiedig a gwefannau sy'n debygol o gael eu cyrchu gan bobl ifanc.

Mae'n rhaid i wefannau a cynnyrch ddarparu haenau ychwanegol o ddiogelwch ar gyfer data plant. Gallai hyn gynnwys cyfyngu neu ddileu rhai nodweddion i blant os mae nhw o dan 18 fydd efo'r canlyniad o:

- gosodiadau preifatrwydd yn cael eu gosod yn uchel iawn yn awtomatig;
- plant ac eu rhieni/gofalwyr yn cael mwy o reolaeth o'r gosodiadau preifatrwydd;
- olrhain lleoliad sydd ddim yn hanfodol yn cael eu diffodd;
- plant ddim yn cael eu 'pwnio' rhagor gan safleoedd drwy hysbysiadau i ostwng eu gosodiadau preifatrwydd; a
- offerynnau fwy eglur ac mwy hygyrch mewn lle er mwyn helpu plant i ymarfer eu hawliau diogelu data (gan gynnwys offerynnau caniatad rhieniol).

Mae'r ICO wedi cynhyrchu cyfres o adnoddau ar gyfer ysgolion er mwyn helpu plant i nodi ble gallan nhw fynd i gael cymorth, gan gynnwys yr hyn y dylen nhw ei wneud os ydyn nhw'n amau bod ap, gêm neu wefan yn camddefnyddio'u data neu nad yw'n cydymffurfio â'r Cod Plant.

Gwelir adnoddau ar wefan yr ICO:

Gwybodaeth ar gyfer ysgolion cynradd: https://ico.org.uk/for-organisations/posters-stickers-and-e-learning/school-resources/wales-primary/

Gwybodaeth ar gyfer ysgolion uwchradd: https://ico.org.uk/for-organisations/posters-stickers-and-e-learning/school-resources/wales-secondary/

16.2 Deddfwriaeth Perthnasol

Mae'r ddeddfwriaeth ganlynol hefyd yn ymdrin ag agweddau gwahanol o e-ddiogelwch:

Deddf Casineb Hiliol a Chrefyddol 2006	Mae'r Ddeddf hon yn troseddoli'r weithred o fygwth pobl oherwydd eu credoau crefyddol, neu annog casineb crefyddol drwy ddangos, cyhoeddi neu ddosbarthu deunydd ysgrifenedig sy'n fygythiol. Mae cyfreithiau eraill sydd eisoes yn amddiffyn pobl rhag bygythiadau yn seiliedig ar hil, rhyw neu gefndir ethnig.
Deddf Troseddau Rhywiol 2003	Mae'r drosedd newydd o feithrin perthynas amhriodol ar-lein wedi'i chyflawni os ydych yn 18 oed ac wedi cyfathrebu â phlentyn o dan 16 oed o leiaf ddwywaith (gan gynnwys dros y ffôn neu dros y rhyngrwyd). Mae'n drosedd i gwrdd â nhw neu deithio i gwrdd â nhw unrhyw le yn y byd gyda'r bwriad o gyflawni trosedd rywiol. Mae gorfodi plentyn o dan 16 oed i wylio gweithred rywiol, gan gynnwys edrych ar fideos, ffotograffau neu gamera gwe, er eich pleser eich hun yn anghyfreithlon. Mae hefyd yn drosedd i berson sydd mewn sefyllfa o ymddiriedaeth gyflawni gweithred rywiol gydag unrhyw berson o dan 18 oed y mae ganddo swydd o ymddiriedaeth drosto. (Mae athrawon, gweithwyr cymdeithasol, eich gweithwyr a gweithwyr iechyd proffesiynol i gyd wedi'u cynnwys yn y categori ymddiriedaeth hwn). Mae unrhyw un sy'n cael cyfathrach rywiol gyda phlentyn o dan 13 oed yn cyflawni trais rhywiol. Mae'r ddogfen ganlynol yn cynnwys gwybodaeth ddefnyddiol: "*Children & Families: Safer from Sexual Crime*": Mae anfon neges neu gynnwys arall sy'n ymosodol neu o natur anweddus, anllad neu fygythiol drwy'r rhyngrwyd; neu anfon negeseuon ffug drwy'r rhyngrwyd neu ddefnyddio'r rhyngrwyd yn gyson i wylltio, bod yn anghyfleustra neu boeni rhywun yn ddiangen, yn euog o drosedd a allai arwain at gyfnod yn y carchar.

	Mae'r geiriad hwn yn bwysig gan fod trosedd wedi'i chyflawni cyn gynted ag y bydd y neges wedi'i hanfon: nid oes angen profi unrhyw fwriad na phwrpas.
Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR) a Deddf Diogelu Data 2018	Mae'r rhain yn ei gwneud yn ofynnol i unrhyw un sy'n delio â gwybodaeth bersonol gydymffurfio ag egwyddorion pwysig diogelu data wrth ymdrin â data personol sy'n ymwneud â pherson byw. Mae'r rhain hefyd yn rhoi'r hawl i unigolion weld yr wybodaeth bersonol sy'n gysylltiedig â hwy sy'n cael ei chadw, derbyn iawndal ac atal prosesu'r wybodaeth.
Deddf Camddefnyddio Cyfrifiaduron (1990) (adrannau 1-3)	Beth bynnag fo cymhelliad yr unigolyn, mae'r Ddeddf yn mynnu ei bod yn drosedd: • cael mynediad i ffeiliau neu feddalwedd cyfrifiadurol heb ganiatâd (e.e. defnyddio cyfrinair rhywun arall i gael mynediad i ffeiliau); • mynediad heb ganiatâd, fel yr uchod, er mwyn cyflawni trosedd arall (fel twyll); neu • ymyrryd â gallu cyfrifiadur neu raglen i weithredu (er enghraifft a achosir gan firws neu drwy fethu ag atal ymosodiad ar y system). Gall dinasyddion neu drigolion y DU gael eu hestraddodi i wlad arall os amheuir eu bod wedi cyflawni un o'r troseddau uchod.
Deddf Cyfathrebu Maleisus 1988 (adran 1)	Mae'r ddeddfwriaeth hon yn mynnu ei bod yn drosedd anfon neges electronig (e-bost) sy'n cyfleu gwybodaeth anweddus, hynod sarhaus, bygythiol neu anwir; neu sydd o natur anweddus neu'n ddifrifol o sarhaus os mai'r bwriad oedd achosi pryder neu orbryder i'r derbynnydd.
Deddf Hawlfraint, Dyluniadau a Phatentau 1988	Hawl unigolyn yw hawlfraint i atal eraill rhag copïo neu ddefnyddio ei "waith" heb ganiatâd. Rhaid i'r deunydd o dan hawlfraint (a elwir yn "waith") fod yn waith a grëwyd gan yr awdur ei hun a chynnyrch sgil a barn. Mae hawlfraint yn codi pan fydd unigolyn yn mynegi syniad ar ffurf ddiriaethol. Mae gweithiau fel testun, cerddoriaeth, sain, ffilm a rhaglenni i gyd yn gymwys i'w hamddiffyn gan hawlfraint. Fel arfer, awdur y gwaith sy'n berchen ar yr hawlfraint, ond pe bai'r gwaith yn cael ei greu yn ystod cyflogaeth, yna'r cyflogwr sy'n berchen ar yr hawlfraint. Mae gwneud copi o'r cyfan neu ran sylweddol o waith unrhyw un heb ganiatâd yr awdur yn torri hawlfraint. Fel arfer bydd tystysgrif yn cyd-fynd â'r gwaith sy'n caniatáu i'r defnyddiwr ei gopïo neu ei ddefnyddio at ddibenion cyfyngedig. Mae bob amser yn ddoeth darllen telerau'r drwydded cyn gwneud copi neu ddefnyddio deunydd unrhyw un arall.

	Mae hefyd yn anghyfreithlon addasu neu ddefnyddio meddalwedd heb drwydded neu mewn unrhyw ffordd sy'n cael ei wahardd gan amodau'r drwydded feddalwedd.
Deddf Trefn Gyhoeddus 1986 (adrannau 17-29)	Mae'r Ddeddf yn pennu ei bod yn drosedd annog casineb hiliol drwy ddangos, cyhoeddi neu ddosbarthu deunydd ysgrifenedig sy'n fygythiol. Fel yn achos *Deddf Casineb Hiliol a Chrefyddol 2006*, mae hefyd yn drosedd meddu ar ddeunydd llidiol gyda'r bwriad o'i ryddhau.
Deddf Plant 1989	Mae'n drosedd cymryd, rhoi caniatâd i gymryd, gwneud, meddu, dangos, dosbarthu neu hysbysebu ffotograffau anweddus o blant ym Mhrydain Fawr. Yn yr achos hwn, mae plentyn yn golygu unrhyw un o dan 18 oed. Mae edrych ar ddelwedd o blentyn ar eich cyfrifiadur yn golygu eich bod wedi gwneud delwedd ddigidol. Mae delwedd o blentyn hefyd yn cynnwys gwneud delweddau ffug (wedi'u haddasu'n ddigidol neu fel arall). Gallai person sy'n cael ei ganfod yn euog o drosedd o'r fath wynebu cyfnod o 10 mlynedd yn y carchar.
Deddf Gwasanaethau Cymdeithasol a Llesiant (Cymru) 2014 (adran 130)	Mae dyletswydd i roi gwybod am blant sydd mewn perygl os oes achos rhesymol dros amau bod plentyn yn blentyn sydd mewn perygl ac ymddengys ei fod o fewn ardal yr awdurdod. Gallai hyn fod yn berthnasol o ran e-ddiogelwch os yw plentyn mewn perygl.
Deddf Cyhoeddiadau Anllad 1959	Mae cyhoeddi erthygl "anllad" yn drosedd. Mae cyhoeddi'n cynnwys trosglwyddo electronig.
Deddf Amddiffyn rhag Aflonyddu 1997	Rhaid i berson beidio ag ymddwyn mewn modd sy'n achosi aflonyddwch i berson arall, pan fydd yn gwybod, neu ddylai wybod, bod yr ymddygiad yn achosi aflonyddwch. Mae person sy'n ymddwyn mewn modd sy'n achosi i berson arall, ar o leiaf ddau achlysur, gredu y bydd trais yn cael ei achosi iddo, yn euog o drosedd os yw'n gwybod neu y dylai wybod bod ei ymddygiad yn achosi ofn i berson arall.
Deddf Rheoleiddio Pwerau Ymchwilio 2000	Mae *Deddf Rheoleiddio Pwerau Ymchwilio 2000* yn rheoleiddio'r broses o ymyrryd â chyfathrebu ac yn ei gwneud yn drosedd cyfnewid neu fonitro cyfathrebiadau heb ganiatâd y partïon sy'n ymwneud â'r cyfathrebu. Pasiwyd y Ddeddf hon i gydymffurfio â *Deddf Hawliau Dynol 1998*. Fodd bynnag, mae *Rheoliadau Telegyfathrebu (Arfer Busnes Cyfreithlon) (Dehongli Cyfathrebu) 2000* yn caniatáu rhywfaint o fonitro a chadw cofnodion, er enghraifft, i sicrhau bod y cyfathrebu'n berthnasol i weithgareddau ysgol neu er mwyn ymchwilio neu ddarganfod y defnydd a wneir o'r rhyngrwyd heb ganiatâd. Er gwaethaf hyn, cyn monitro, dylid cael caniatâd yn seiliedig ar wybodaeth, sy'n golygu bod yn rhaid cymryd camau i sicrhau bod pawb sy'n mynd i ddefnyddio'r system yn gwybod y bydd y cyfathrebu'n cael ei fonitro.

	Mae monitro'n gyfrinachol heb hysbysu'r defnyddwyr bod rhywun yn gwneud hynny mewn perygl o dorri deddfwriaeth diogelu data a deddfwriaeth preifatrwydd.
Deddf Cyfathrebu 2003 (adran 127)	Mae'n drosedd anfon neges neu fater arall sy'n sarhaus iawn neu o gymeriad anweddus, anllad neu fygythiol neu'n anwir at y diben o achosi annifyrrwch, anghyfleustra neu bryder diangen i un arall drwy gyfrwng rhwydwaith cyfathrebu electronig cyhoeddus.
Deddf Crwneriaid a Chyfiawnder 2009 (adran 62)	Yn ymwneud â meddu ar luniau gwaharddedig o blant.
Y Ddeddf Cwcis	Mae'r Ddeddf Cwcis yn ddarn o ddeddfwriaeth preifatrwydd sy'n ei gwneud yn ofynnol i wefannau gael caniatâd gan ymwelwyr i storio neu adalw unrhyw wybodaeth ar gyfrifiadur, ffôn clyfar neu dabled. http://www.cookielaw.org/the-cookie-law/

17. Enwau a Chyfeiriadau Cyswllt E-ddiogelwch

Child Exploitation & Online Protection Centre http://www.ceop.gov.uk	Gwefan Think U Know http://www.thinkuknow.co.uk/
Gwefan Wise Kids www.wisekids.org.uk	Internet Watch Foundation http://www.iwf.org.uk/
Childline http://www.childline.org.uk/	Internet Safety Zone http://www.internetsafetyzone.com/
Childnet International https://www.childnet.com/	NSPCC https://www.nspcc.org.uk/
Virtual Global Taskforce – Report Abuse http://www.virtualglobaltaskforce.com/	Internet Matters www.internetmatters.org
Internet Watch Foundation (IWF) www.iwf.org.uk	Lucy Faithfull Foundation www.lucyfaithfull.org
Net Aware www.net-aware.org.uk	The Marie Collins Foundation www.mariecollinsfoundation.org.uk
UK Safer Internet Centre www.saferinternet.org.uk	Professional Online Safety Helpline www.saferinternet.org.uk/about/helpline
360 Safe Self-Review tool for schools	Action Fraud

www.360safe.org.uk	www.actionfraud.police.uk
Get Safe Online www.getsafeonline.org	

18. Hyfforddiant

Bydd y Pennaeth a'r Swyddog Diogelu Data Ysgolion yn sicrhau bod staff, gan gynnwys llywodraethwyr ysgol, wedi'u hyfforddi'n ddigonol mewn perthynas ag e-ddiogelwch.

Bydd yr hyfforddiant yn gysylltiedig â hyfforddiant am amddiffyn plant a diogelu data. Bydd yn ymdrin â materion cysylltiedig fel y gyfraith ar hawlfraint deunyddiau electronig.

Bydd y Pennaeth yn cadw cofnod o bresenoldeb a chofrestr o bwy sydd wedi cwblhau hyfforddiant e-ddiogelwch a pha bryd y cafodd ei gwblhau.

Bydd yr ysgol yn cynnig addysg a gwybodaeth i rieni a gofalwyr am e-ddiogelwch.

19. Mynd yn Erbyn y 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 risg o gosbau sifil a throseddol sylweddol i'r unigolyn ac awdurdodau'r ysgol.

Felly, gellir ystyried peidio â chydymffurfio gan aelod o staff arwain i'r aelod staff fod yn ddarostyngedig i weithdrefn ddisgyblu'r ysgol. Os bydd aelod o staff yn torri'r polisi hwn, efallai y bydd ei gontract yn dod i ben ar unwaith.

20. Adolygu'r Polisi a Threfniadau Arolygiaeth

Bydd y polisi hwn yn cael ei adolygu gan y Swyddog Diogelu Data Ysgolion bob dwy flynedd, 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 gyda mewnbwn gan y Grŵp Gweithredol Diogelu Data Ysgolion a bydd yn cael ei fabwysiadu gan gorff llywodraethu'r ysgol. Caiff cydymffurfiaeth â'r polisi hwn a gweithdrefnau cysylltiedig eu monitro gan Dîm Arweinyddiaeth yr Ysgol a'r corff llywodraethu.

Bydd yr ysgol yn penodi aelod penodol o staff a fydd yn gyfrifol am e-ddiogelwch/ TGCh.

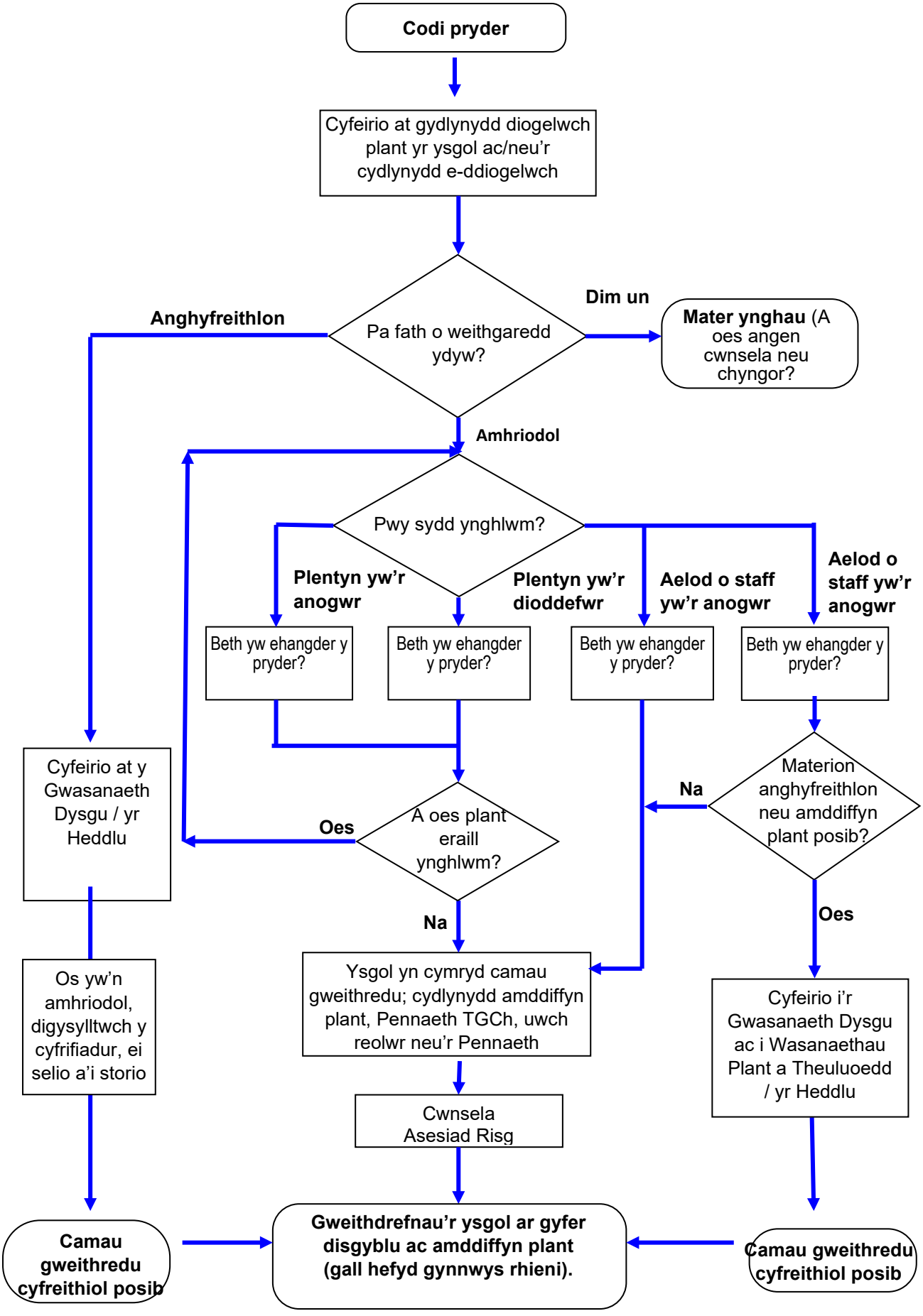
Os oes unrhyw ymholiadau neu bryderon am unrhyw beth a gynhwysir yn y polisi hwn, dylid cysylltu â'r Swyddog Diogelu Data Ysgolion heb betruso:

E-bost: dpoysgolionmon@ynysmon.llyw.cymru

Rhif ffon: 01248 751833

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

ATODIAD A- Ymateb i ddigwyddiad sy'n peri pryder



ATODIAD B

Polisi E-Ddiogelwch Ysgolion

Rhestr Wirio'r Pennaeth

Rhif	Camau gweithredu i'w cymryd	Oes gan yr ysgol hyn mewn lle (Oes/Nac Oes/Sylwadau/Dyddiadau ayyb)
1	Mae'r fersiwn cyfredol o'r *Polisi E-Ddiogelwch Ysgolion* wedi ei fabwysiadu'n ffurfiol gan Gorff Llywodraethu'r Ysgol.	
2	Mae proses ar waith i fonitro cydymffurfiad yr ysgol â'r polisi hwn yn barhaus.	
3	Mae'r polisi yma wedi ei rannu gyda staff a gwirfoddolwyr yr ysgol ac mae eglurhad wedi ei roi ar sut i weithredu y polisi ac ar bwysigrwydd y polisi.	
4	Mae staff wedi derbyn hyfforddiant e-ddiogelwch priodol ac mae hyn wedi derbyn blaenoriaeth uchel ar draws yr ysgol.	
5	Mae'r Pennaeth yn cadw cofnod o bresenoldeb a chofrestr o bwy sydd wedi cwblhau hyfforddiant e-ddiogelwch a pha bryd y cafodd ei gwblhau.	
6	Mae'r ysgol wedi penodi aelod penodol o staff a fydd yn gyfrifol am e-ddiogelwch/ TGCh ac mae'r person hwn yn cael cymorth digonol gan staff eraill yr ysgol ac yn rhoi cymorth iddynt, yn enwedig yr uwch berson dynodedig ar gyfer diogelu.	
7	Mae data personol yn yr ysgol yn cael ei gadw ac ei brosesu yn unol â'r *Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR)* a *Deddf Diogelu Data 2018*.	
8	Mae proses ar waith ar gyfer diogelu holl wybodaeth bersonol a chategori arbennig o fewn yr ysgol.	
9	Mae manylion y trefniadau e-ddiogelwch yn cael eu trafod a'u hadolygu gyda holl staff yr ysgol yn rheolaidd.	
10	Mae lefel mynediad sy'n cael ei warantu i unigolion penodol wedi cael ei bennu.	

11	Mae'r Cofrestr Asedau Gwybodaeth a Cofnod o Weithgareddau Prosesu (ROPA) yr ysgol yn cael eu hadolygu yn rheolaidd ac yn cael eu cadw yn gyfredol.	
12	Mae asesiad risg yn cael ei wneud ar unrhyw dechnoleg newydd cyn rhoi caniatâd i'w defnyddio yn yr ysgol. Mae'r ysgol bob amser yn cysylltu â'r Swyddog Diogelu Data Ysgolion wrth weithredu neu newid proses neu system, er mwyn penderfynu a oes angen DPIA ai peidio.	
13	Mae asedau a risgiau gwybodaeth o fewn yr ysgol cael eu rheoli.	
14	Yn gofyn am arweiniad gan y Swyddog Diogelu Data Ysgolion ar gytundebau sy'n ymwneud ag apiau, meddalwedd a systemau technoleg gwybodaeth a chyfathrebu.	
15	Yn sicrhau bod cofnodion yn cael eu cadw o bob digwyddiad e-ddiogelwch a bod y rhain yn cael eu hadrodd i'r uwch dîm arweinyddol.	
16	Yn cynnal archwiliadau mewnol sydd yn monitro cydymffurfiad o leiaf unwaith y tymor.	
17	Mae proses gadarn ar waith i ganfod a nodi achosion o dor-rheolau data; ymchwilio ac asesu achosion o dor-rheolau data gan gynnwys risgiau a rhannu unrhyw ddigwyddiadau diogelwch data gyda'r Swyddog Diogelu Data Ysgolion.	
18	Mae diwylliant o adrodd a dysgu wedi ei sefydlu er mwyn galluogi'r ysgol sefydlu lle mae problemau yn bodoli ac i ddatblygu strategaethau gyda'r Swyddog Diogelu Data Ysgolion er mwyn atal problemau rhag godi yn y dyfodol.	
19	Mae staff yn ymwybodol o'r broses o gael gafael ar gymorth ac arweiniad sy'n ymwneud â chodi pryderon ac ymateb i bryderon diogelwch ar-lein.	
20	Mae'r camau angenrheidiol wedi'u cymryd i ddiogelu'r seilwaith technegol a bodloni gofynion technegol systemau technoleg gwybodaeth a chyfathrebu'r ysgol.	
21	Mae'r ysgol yn gwirio yn rheolaidd bod y systemau technoleg gwybodaeth a chyfathrebu y mae'n eu defnyddio mor ddiogel ag sy'n rhesymol bosibl drwy gymryd cyngor ac arweiniad ar y gofynion technegol ar gyfer y systemau hynny.	
22	Mae'r ysgol yn cynnal adolygiadau rheolaidd o ddiogelwch ei systemau technoleg gwybodaeth a chyfathrebu drwy gontractwyr/darparwyr cefnogaeth sydd â'r sgiliau addas.	
23	Mae diogelu rhag firysau'n cael ei ddiweddaru'n rheolaidd.	

24	Nid yw dyfeisiau heb eu rheoli'n cael eu cysylltu i rwydwaith yr ysgol heb gytundeb Uned TGCh Cyngor Sir Ynys Môn.	
25	Mae rhwydwaith yr ysgol wedi ei wahanu i fewn i is-rwydweithiau rhesymegol ac â wal dân sydd yn unol âg anghenion y defnyddwyr a lefel diogelwch y defnyddwyr ar y rhwydwaith.	
26	Mae systemau'r ysgol yn darparu ar gyfer hidlo mynediad i'r rhyngrwyd i bob defnyddiwr, atal mynediad at gynnwys anghyfreithlon, a hidlo ychwanegol ar gyfer gwahanol grwpiau o ddefnyddwyr.	
27	Mae data personol a anfonir dros y rhyngrwyd yn cael ei amgryptio neu ei wneud yn ddiogel drwy ddulliau eraill.	
28	Mae gan yr ysgol strategaethau wrth gefn (gan gynnwys gofynion all-lein ac all-safle) sy'n cyfateb i ofynion yr ysgol o ran adalw os bydd trychineb.	
29	Mae strategaethau diogelwch yn cael eu trafod gyda Gwasanaeth TGCh Cyngor Sir Ynys Môn lle bo hynny'n briodol.	
30	Ni ddefnyddir dyfais gludadwy heb ganiatâd penodol a chael archwiliad ar gyfer firysau.	
31	Mae ffeiliau a gedwir ar rwydwaith yr ysgol yn cael eu harchwilio'n rheolaidd.	
32	Mae'r cydgysylltydd TGCh/rheolwr rhwydwaith yn adolygu capasiti'r system yn rheolaidd.	
33	Dim ond cyfrifon e-bost swyddogol, ysgol y mae staff yn eu defnyddio i gyfathrebu â disgyblion.	
34	Mae disgyblion yn ymwybodol bod rhaid hysbysu athro ar unwaith os ydynt yn derbyn e-bost sarhaus.	
35	Mae disgyblion yn ymwybodol rhaid iddynt beidio â datgelu manylion personol amdanynt eu hunain nac eraill mewn neges e-bost, na threfnu i gwrdd ag unrhyw un heb ganiatâd penodol.	
36	Mae cyfyngiadau ar waith er mwyn atal gorddefnyddio negeseuon e-bost cymdeithasol.	
37	Mae cyfeiriad, cyfeiriad e-bost a rhif ffôn yr ysgol wedi eu cynnwys fel manylion cyswllt ar y wefan (os yn berthnasol).	
38	Mae gwefan/cyfrifon rhwydwaith cymdeithasol yr ysgol yn cyfateb i ganllawiau'r ysgol ar gyfer cyhoeddiadau, gan gynnwys parch at eiddo deallusol a hawlfraint.	

39	Ni ddefnyddir enwau disgyblion yn unman ar wefan yr ysgol na chyfrifon cyfryngau cymdeithasol mewn cysylltiad â ffotograffau a delweddau.	
40	Ceisir cymeradwyaeth ysgrifenedig gan rieni/gofalwyr cyn i luniau o ddisgyblion gael eu cynnwys ar wefan yr ysgol/cyfrifon cyfryngau cymdeithasol drwy ffurflenni caniatâd.	
41	Dim ond gyda chaniatâd y disgybl a'i rieni/gofalwyr y gellir cyhoeddi gwaith.	
42	Mae'r UDA a'r tîm gweinyddol yn golygu'r deunydd ar gyfer gwefan a chyfrifon cyfryngau cymdeithasol yr ysgol ac yn sicrhau ei fod yn gywir ac yn briodol.	
43	Mae'r ysgol yn rhwystro/hidlo mynediad i safleoedd rhwydweithio cymdeithasol.	
44	Mae fforymau amhriodol yn cael eu rhwystro.	
45	Mae'r ysgol yn gweithio gyda Gwasanaeth TGCh Cyngor Sir Ynys Môn i sicrhau bod systemau sy'n amddiffyn disgyblion yn cael eu diwygio a'u gwella'n rheolaidd.	
46	Mae defnydd o'r rhyngrwyd yn cael ei fonitro ar hap i sicrhau ei fod yn cydymffurfio â pholisi'r ysgol.	
47	Mae'r Pennaeth yn roi caniatâd personol bob tro y defnyddir y rhyngrwyd heb hidlydd, ac adolygu'r angen am fynediad rheolaidd.	
48	Mae uwch aelodau o staff yn sicrhau bod dulliau hidlo yn cael eu hadolygu'n rheolaidd er mwyn sicrhau bod y dulliau hynny'n briodol, yn effeithiol ac yn rhesymol.	
49	Mae staff sy'n rheoli'r systemau hidlo neu'n monitro'r defnydd o TGCh yn cael eu goruchwylio gan uwch reolwyr, ac mae ganddynt weithdrefnau clir ar gyfer rhoi gwybod am unrhyw faterion sy'n peri pryder.	
49	Mae holl offer fideo-gynadledda yn y dosbarth yn cael ei roi i ffwrdd ac yn cael ei gloi os oes angen pan nad yw'n cael ei ddefnyddio.	
50	Nid yw gwybodaeth gyswllt fideo-gynadledda yn cael ei gynnwys ar wefan yr ysgol.	
51	Nid yw offer fideo-gynadledda yn cael ei gymryd i ffwrdd o safle'r ysgol heb ganiatâd.	
52	Mae fideo-gynadledda yn cael ei oruchwylio'n briodol yn ôl oedran y disgyblion.	

53	Dim ond aelodau allweddol o staff sydd gyda mynediad i'r system fideo-gynadledda, y wefan neu'r dudalen reoli o bell arall sydd ar gael ar systemau mwy.	
54	Dim ond aelodau o staff sydd â mynediad at unrhyw fanylion mewngofnodi a chyfrineiriau unigryw ar gyfer y gwasanaethau fideo-gynadledda addysgol, ac mae'r manylion hyn yn cael eu cadw mewn man diogel.	
55	Wrth recordio gwers fideo-gynadledda, mae'r rheswm dros y recordio bob amser yn cael ei roi ar ddechrau'r gynhadledd ac mae'n cael ei wneud yn glir i bawb sy'n cymryd rhan bod y gynhadledd yn cael ei recordio.	
56	Mae deunydd sy'n cael ei recordio yn cael ei storio'n ddiogel yn unol â'r *Cyfnodau Cadw Ysgolion*.	
57	Mae athrawon a disgyblion yn defnyddio'r cyfleuster sy'n gallu newid neu gymylu arddangosiad cefndir tra ar wers ar-lein.	
58	Mae cytundeb wedi'i sefydlu rhwng yr ysgol (athro) a rhieni/gofalwyr ynghylch disgwyliadau ac ymddygiad disgyblion a rhieni/gofalwyr yn ystod gwersi ar-lein.	
59	Mae gan yr ysgol *Bolisi Recordio Sesiynau Ffrydio'n Fyw* a *Pholisi Cadw Recordiadau.*	
60	Mae gan yr ysgol ganllaw ar ddysgu ar-lein i'r staff a'r rhieni.	
61	Mae'r ysgol yn sicrhau bod deunyddiau a geir o'r rhyngrwyd sy'n cael eu copïo neu eu defnyddio ar adegau eraill gan staff a disgyblion yn cydymffurfio â chyfraith hawlfraint.	
62	Mae'r ysgol yn cadw cofnod parhaus o bob aelod o staff a disgybl sydd â chaniatâd i gael mynediad at ddolenni electronig yr ysgol.	
63	Mae'n rhaid i ddisgyblion wneud cais unigol am fynediad i'r rhyngrwyd drwy gytuno i gydymffurfio â'r rheolau e-ddiogelwch.	
64	Gofynnir i rieni lofnodi a dychwelyd ffurflen sy'n rhoi caniatâd i ddisgyblion gael mynediad i'r rhyngrwyd a hysbysir rhieni y bydd disgyblion yn cael mynediad i'r rhyngrwyd dan oruchwyliaeth.	
65	Mae uwch aelod o staff wedi ei ddynodi i ddelio â chwynion am gamddefnyddio'r rhyngrwyd ac mae unrhyw gwynion am staff sy'n cam-ddefnyddio'r rhyngrwyd yn cael eu cyfeirio at y Pennaeth.	
66	Mae rheolau e-ddiogelwch yn cael eu harddangos mewn ystafelloedd sydd â mynediad i'r rhyngrwyd.	

67	Mae staff yn ymateb i ddigwyddiad sy'n peri pryder drwy ddilyn y camau sydd yn y siart llif sydd wedi ei gynnwys yn Atodiad A.	
68	Mae staff yr ysgol yn ymwybodol o'r cyfres o reolau o fewn y Cod Plant.	

Content **Page**

1. Policy Statement 41
2. Scope 41
3. Legislation, Guidance and Policies 41
4. Definitions 42
5. Responsibilities 44
5.1. School Governing Body 44
5.2. Headteacher 45
5.3. All Staff within the School 46
5.4. Schools Data Protection Officer 46
6. What is e-safety? 46
7. What does electronic communication include? 46
8. Use of new technology in education 47
9. Teaching and learning 48
9.1. Why is using the internet important? 48
9.2. How does using the internet benefit education? 48
9.3. How can using the internet enhance learning? 49
10. Routes to e-safety 49
10.1 General principles 49
10.2 Electronic communication between staff and pupils 49
11. Managing Information Systems 50
11.1. How is the safety of information systems maintained? 50
11.2. How is e-mail regulated? 51
11.3. How is published content regulated? 51
11.4. Can the work or photos of pupils be published? 51
11.5. How is social networking and personal publishing regulated? 52
11.6. How is filtering regulated? 53
11.7. How is videoconferencing monitored? 53
11.7.1. Users 54
11.7.2. Content 54
11.8. How is on-line learning monitored? 54
11.8.1. Teachers agree to 55
11.8.2. Parents/carers agree to 55
11.9. How do pupils learn how to evaluate internet content? 56
11.10. How can the latest technology be regulated? 56
12. How is personal data protected? 56
13. Policy Decisions 57
13.1. How is access to the internet authorised? 57
13.2. How is risk assessed? 57
13.3. How are complaints about e-safety dealt with? 58
13.4. How is the internet used across the community? 58
14. Communication Policy 58
14.1. How is the policy presented to the pupils? 58
14.2. How is the policy discussed with staff? 58
14.3. How is the policy shared with parents/carers? 59
15. Responding to an incident that causes concern 59
15.1. What are the dangers? 59

15.2. How the school should respond? 60
16. The Legal Framework 60
16.1 The Children's Code 60
16.2 Relevant Legislation 61
17. E-safety Contact Names and Addresses 64
18. Training 65
19. Breach of the Policy 65
20. Review of Policy and Oversight Arrangements 65
21. APPENDIX A- Responding to an incident that causes concern 67
22. APPENDIX B- Schools E-Safety Policy- Headteacher's Checklist 68

1. Policy Statement

The school recognises that the internet and information communication technologies are an important part of everyday life. Safe and effective use of the internet, on-line learning, social media and other information technology, is now an essential life skill for pupils and staff alike.

E-safety is the education about the benefits and risks of using new technologies, and to provide safeguards and awareness that enables individuals to control their on-line experiences.

The school recognises that the use of technology presents challenges and risks both inside and outside of school. Online safety is an essential part of safeguarding and the school will ensure that all pupils and staff are protected from potential harm online. Pupils must be supported to be able to manage and respond to online risks as unregulated access to the internet and information communication technologies can place pupils in an awkward, inappropriate and even dangerous situation.

The school must have processes in place to ensure that ICT is used responsibly, ensuring the safety of pupils. Also, processes will empower, protect and educate school staff in their use of technology and establish mechanisms to identify, intervene and escalate an incident where appropriate.

2. Scope

This policy applies to all employees, volunteers, governors, contractors, agencies, representatives and temporary staff working for the school, and are users of, the school's information and communication technology systems.

This policy applies to all access to the internet and other electronic communications, as well as social networking; personal publishing and on-line learning and the use of technology such as a computer, laptop, tablet or mobile phone relating to school business.

3. Legislation, Guidance and Policies

This policy should also be read in conjunction with other relevant school policies including (but not limited to) the *Recording Livestreaming Sessions Policy; Recording Retention Policy; Schools Data Protection Policy; Schools Information Security Policy; School Staff E-mail Policy, School Staff Social Media Policy; Schools taking Photographs for Publicity Purposes Policy; Schools Data Breach Policy; Schools Data Subject Access Request Policy*; *Safeguarding Policy; Child Protection Policy; Threatening Behaviour Policy; Disciplinary Policy; Anti Bullying Policy; Acceptable Use Policy* and *Schools Retention Schedule.*

These are all available on the data protection page on the Learning Service Microsite.

Staff should comply with the EWC's (Education Workforce Council) *Code of Professional Conduct and Practice*- http://www.ewc.wales/site/index.php/en/fitness-to-practise/code-of-professional-conduct-and-practice-pdf.html

The following legislation relates to e-safety (please see section 17 for more details regarding the legal framework):

- *UK General Data Protection Regulation (UK GDPR);*
- *Data Protection Act 2018;*
- *The Children's Code;*
- *Sexual Offences Act 2003;*
- *Racial and Religious Hatred Act 2006;*
- *Police and Justice Act 2006;*
- *Computer Misuse Act 1990;*
- *Malicious Communications Act 1988;*
- *Copyright, Designs and Patents Act 1988;*
- *Public Order Act 1986;*
- *Children Act 1989;*
- *Social Services and Well-being (Wales) Act 2014;*
- *Obscene Publications Act 1959;*
- *Protection from Harassment Act 1997;*
- *Regulation of Investigatory Powers Act 2000;*
- *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;*
- *Communications Act 2003:*
- *Coroners and Justice Act 2009;*
- *The Cookie Law*

4. Definitions

Blended learning	Blended learning is an instructional approach that includes a combination of online and in-person learning activities. For example, students can complete online self-paced assignments by a certain date and then meet on-site or online for additional learning activities.
Synchronous learning (simultaneous learning)	When learners participate in an online learning course at the same time but in different locations, it is known as synchronous learning. Synchronous learning allows learners to interact with the instructor and other participants. This is done through software that creates a virtual classroom.
Asynchronous learning (non-simultaneous learning)	Asynchronous learning is an approach to education where pupils learn the same content from different (geographic) places and at different times. Pupils can access materials, ask questions, and practice their skills at any time that works for them.

Virtual classroom	The virtual classroom refers to a digital classroom learning environment that takes place over the internet rather than in a physical classroom. It is implemented through software that allows a teacher and students to interact.
Streaming media	Streaming media refers to video and audio that is downloaded to a computer from the internet as a continuous stream of data and is played as it reaches the destination computer.
Social media	Any online platform that offers real-time interaction between the user and other individuals or groups. Examples include, but are not limited to communication platforms, online discussion forums, blogs, collaborative spaces, media sharing services, micro-blogging applications and the use of webcams.
Online social space	Internet areas (sites/pages) where you can meet other people and chat, either in real-time (chatrooms and live chat) or via messages and message boards.
World Wide Web (www.)	World Wide Web is an information system on the internet which allows documents to be connected to other documents by hypertext links, enabling the user to search for information by moving from one document to another.
Podcasting	Podcasting is the practice of using the internet to make digital recordings of broadcasts available for downloading to a computer or mobile device.
Chatroom	A web page that contains a window into which you can type text to enable a 'real-time' conversation in text form with individuals or small groups.
Blog / Vlog	A website where regular entries are made in the form of an on-line journal or diary. A Blog or 'web log' often offers commentary or news on a particular subject whilst Vlog uses video to document their daily lives as an ongoing video diary. Blogs are usually arranged chronologically and with less formality than a website. Many blogs accept and respond to comments.
Wiki	A website or similar resource that allows users to add and edit content collectively.
Browser	A browser is a free software package or mobile app that displays web pages, graphics, and most online content. Browser software is specifically designed to convert HTML and XML computer code into human-readable documents. Browsers display web pages.
Web Page	A web page is what can be seen in a web browser when on the internet. Pages may include text, photos, images, diagrams, links, advertisements, and more on any page that is viewed.
URL	URLs are the web browser addresses of internet pages and files.
Videoconferencing	Videoconferencing is telecommunication in the form of a videoconference which is the holding of a conference

	among people at remote locations by means of transmitted audio and video signals.
Cyber bullying	Any use of social media or communication technology to bully an individual or group.
E-mail	Messages distributed by electronic means from one computer user to one or more recipients via a network. In addition to textual content, e-mail allows the sender to send photographs, video or sound clips in digital form or files.
Personal digital aids (PDAs)	PDA is a computer that fits in the palm of your hand to help collect such information as contacts, appointments, files, and programs.
Downloading	Downloading is a broad term that describes transferring something on the internet or the World Wide Web to a computer or another device. Commonly, downloading is associated with songs, music, and software files.
Bluetooth	Bluetooth is a technical system that allows people to exchange information and data using different types of electronic devices such as computers, mobile phones, printers, video cameras, etc. without using wires.
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.
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.
App	The word "app" is an abbreviation for "application." It is a piece of software that can run through a web browser or offline on a computer, and on a smartphone phone, tablet or other electronic devices.
Cloud storage	Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the internet, or "cloud." It is maintained, operated and managed by a cloud storage service provider on storage servers that are built on virtualisation techniques.
Information systems	Information processing computers or data communication systems.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed information.

5. Responsibilities

5.1. School Governing Body
The school governing body has the responsibility for:

- monitoring the school's overall compliance and accountability relating to this policy;
- ensuring that the school can evidence compliance with data protection legislation;
- undertaking any e-safety training offered.

5.2. Headteacher

The Headteacher is responsible for:

- ensuring the implementation of this policy and promoting understanding and compliance with this policy and all policies relating to e-safety;
- sharing this policy with all school staff and volunteers;
- ensuring personal information within the school is kept and processed in line with *UK GDPR* and the *Data Protection Act 2018;*
- appointing a specific member of staff who will be responsible for e-safety/ICT and that this person has adequate support from, and provides support to, other school staff, particularly the designated senior person for safeguarding;
- ensuring staff have appropriate training in e-safety and that this is given high priority across the school;
- regularly discussing and reviewing details of the arrangements of e-safety with all school staff;
- ensuring there is a process in place to protect all personal and special category information within the school;
- determining the level of access to be granted to specific individuals;
- regularly reviewing and keeping the school's Information Asset Register and Records of Processing Activities (ROPA) up-to-date;
- obtaining guidance from the Schools Data Protection Officer on agreements relating to information and communication technology apps, software and systems;
- ensuring pupils are taught e-safety as an essential part of the curriculum;
- ensuring records are kept of all e-safety incidents and that these are reported to the senior leadership team;
- ensuring information assets and risks within the school are managed;
- ensuring that the necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the school's information and communication technology systems;
- conducting internal audits that monitor compliance;
- ensuring there is a robust process in place to detect and identify data breaches; to investigate and assess breaches including risks and to share any data breach incidents with the Schools Data Protection Officer;
- contacting the Schools Data Protection Officer when implementing or changing a process or system, in order to determine whether a DPIA is required or not;
- establishing a reporting and learning culture to allow the school to establish where problems exist and to develop strategies with the Schools Data Protection Officer to prevent future problems occurring.

5.3. All Staff within the School

All staff employed or volunteering within the school, including teachers, classroom assistants and business support staff are responsible for:

- using information and communication technology in accordance with this policy and the training provided;
- ensuring the safety and well-being of others, both on and offline;
- being aware of the process to access and seek support and guidance relating to raising concerns and responding to online safety concerns;
- working safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology;
- undertaking any e-safety training offered.

5.4. Schools Data Protection Officer

The Schools Data Protection Officer is responsible for:

- monitoring the implementation and compliance of the policy and monitoring security arrangements within the school;
- providing guidance to schools on agreements relating to information and communication technology apps, software and systems;
- ensuring that school staff are adequately trained regarding e-safety;
- assisting the Headteacher to determine whether a DPIA is required or not when implementing or changing a process or system (using new technologies);
- providing advice and support and leading on the reporting of data breaches.

6. What is e-safety?

E-safety involves not only internet technology but also electronic forms of communication such as mobile phones and wireless technology. E-safety establishes safeguards and encourages awareness, ensuring that users manage their online experiences in a safe and positive manner.

The internet is an open communication channel which anyone is free to use. The World Wide Web, e-mail, blogs and social networking can all transmit information around the world by way of the internet at very little cost. Anyone can send messages, discuss ideas and publish material with few restrictions. This makes the internet an invaluable resource that is used by millions of people every day.

Much of the material found on the internet is published for adults, and some of it is inappropriate for children. Information can also be found about weapons, crime and racism, and this is the easiest way to access such information. Pupils also need to learn that publishing personal material can endanger their personal safety and the safety of others.

7. What does electronic communication include?

Electronic communication can include various different methods and styles of communication that includes, but is not limited to:

- ways of interacting on the internet: social networking sites and web-logs (blogs);
- on-line learning; learning via virtual classroom via the internet (synchronous learning and asynchronous learning);
- internet research: websites, search engines and web browsers;
- mobile phones and personal digital aids (PDAs);
- communicating via the internet: e-mail and instant messaging;
- webcams and video conferencing;
- wireless games consoles.

Mobile phone technology has advanced significantly over the last few years - and it continues to evolve. Wireless connections in particular have extended the capabilities of mobile phones, enabling access to a wide range of new content and services globally. Many phones now offer internet and email access, alongside the most often standard functions of messaging, camera, video and sound recording. Mobile phones, alongside other forms of technology are changing the way and speed in which we communicate.

Parents and teachers should be aware that the internet has emerging on-line spaces and social networks which allow individuals to publish unmediated content.

Writing for an audience is important to language development and an essential life skill. However, students should be encouraged to be cautious about revealing too much personal information and about the difficulty of removing inappropriate text, images or other content once it is published.

8. Use of new technology in education

New technologies should be investigated in order to assess their educational benefit, and a **risk assessment** must be made before permission is granted to use the technology in the school.

Schools are making use of a wide variety of new technologies and learning opportunities, including:

- mobile phones powered by computer which can be connected to the internet, Bluetooth and infrared camera;
- on-line learning via technologies such as Microsoft Teams and Google Classroom outside of the school;
- new learning environments such as Moodle and other learning platforms;
- thinking skills that are challenged by games and simulations;
- internet voice messaging such as Skype and IWB link;

- digital storytelling which involves independent thinking and self-motivation;
- podcasting, broadcasting and recording lessons;
- digital video.

Some of these technologies may disappear. Others will evolve. What matters is combining the ability of young people to experiment with the wisdom of teachers in order to develop the appropriate, effective and safe use of technology in teaching and learning.

9. Teaching and learning

9.1. Why is using the internet important?

- the purpose of using the internet in school is to raise educational standards, facilitate pupil attainment, support the professional work of staff and improve the school's managerial functions;
- using the internet is part of the statutory curriculum and an essential tool for learning;
- the internet can provide learning outside of school such as on-line learning at home during periods that schools have to be closed or that pupils cannot attend school;
- internet access is one of the rights of pupils who demonstrate a responsible and mature attitude towards use of the media;
- the internet is an essential element of life in the twenty-first century in relation to education, business and social links. It is the school's duty to provide pupils with easy access to the internet as part of their learning experience;
- pupils make extensive use of the internet outside school, and need to learn how to evaluate the information on the web and be responsible for their own safety.

9.2. How does using the internet benefit education?

The following are some of the benefits of using the internet in education:

- access to learning wherever and whenever it's convenient, including learning on-line at home and as part of blended learning arrangements;
- access to global resources including museums and art galleries;
- being a part of Hwb (National Digital Learning Platform) which links every school in Wales;
- educational and cultural exchanges between pupils across the world;
- vocational, social and leisure resources in libraries, clubs and at home;
- access for pupils and staff to expertise in many areas;
- professional development for staff who can access national developments, educational resources and effective practice for teaching the curriculum;
- co-operation across the support services and professional organisations;
- better access to technical support, including remote control of networks and automatic updates for systems;

- exchanging curriculum and administrative data with the Authority and the Welsh Government.

9.3. How can using the internet enhance learning?

- the internet will provide access to on-line learning when the school is not open or when pupils cannot attend school to ensure that learning continues;
- access to the internet will be designed specifically for the use of pupils, and will include a filtering system which is appropriate for the age of pupils;
- staff should give guidance to pupils about online activities that will support learning outcomes planned according to the age and maturity of the pupils;
- pupils receive guidance on acceptable and unacceptable use of the internet, and are given clear objectives when using the internet;
- access to the internet is planned with a view to enhancing and extending learning activities. Access levels will be revised according to curriculum requirement and the age of pupils;
- pupils will be taught to use the internet effectively in research work, including skills that allow them to find, retrieve and evaluate information.

10. Routes to e-safety

Staff and pupils must understand that using the school network is a privilege that can be removed at any time if there is sufficient reason for doing so. The school is able to monitor all use of the network and internet to ensure the safety of pupils.

10.1. General principles

The use of information and communication technology should follow the following general principles:

- the school's information and communication technology systems are intended primarily for educational use and the management and administration of the school;
- data protection legislation must be followed at all times;
- users must not try to use systems for any illegal purposes or materials;
- users should communicate with others in a professional manner;
- users must not disclose their password and they should not write it down or store it where it is possible that another person might steal it;
- users must not attempt to use another person's user-name or password;
- users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the person designated by the school;
- staff should not use personal social networking sites through the school's information and communication technology systems.

10.2. Electronic communication between staff and pupils

Every user is expected to follow rules of etiquette (net-etiquette) when using the network. These include the following:

- be polite;
- use appropriate language;
- do not use offensive language when communicating with others;
- do not reveal your address, phone number or any other details about yourself or others;
- do not use the internet in a way that interferes with the way in which others are using the network;
- illegal activities are forbidden;
- it cannot be guaranteed that an e-mail will be private;
- the system managers monitor and can access every e-mail;
- messages that relate to illegal activities or that support such activities will be brought to the attention of the authorities.

11. Managing Information Systems

The school has measures and processes in place to ensure that information systems are maintained and have the required security measures in place and also that it has appropriate measures in place to ensure that personal information and published information is protected and is shared appropriately.

11.1. How is the safety of information systems maintained?
The school has the following measures in place to maintain information systems:

- the school will seek to ensure that the information and communication technology systems which it uses are as safe and secure as is reasonably possible by taking reputable advice and guidance on the technical requirements for those systems;
- no unmanaged devices should be connected to the school's network without the agreement of the Isle of Anglesey County Council ICT Unit;
- the school will undertake regular reviews of the safety and security of its information and communication technology systems through the use of suitably skilled contractors/support providers;
- anti-virus protection is regularly updated;
- the school's network is segregated into logical sub networks and firewalled according to the needs of the users and security level of the users on that network;
- the school's systems will provide for filtering internet access for all users, preventing access to illegal content, and with additional filtering for different groups of users, for inappropriate content in accordance with the guidelines produced by Welsh Government - recommended-web-filtering-standards-for-schools-in-wales.pdf (gov.wales);
- reserve strategies (including offline and offsite requirements) will be considered and will correspond with school requirements with regard to retrieval in the event of a disaster;
- safety strategies will be discussed with the Isle of Anglesey County Council ICT Service where appropriate;
- personal data sent over the internet will be encrypted or made safe by other means;

- particular attention will be paid to secure password protection and encryption for devices located in the school and mobile devices;
- no portable device may be used without specific permission and being subjected to an examination for viruses;
- permission will not be given for system facilities that have not been approved or files that can be activated within the work of pupils or sent by e-mail;
- files that are kept on the school network are regularly scrutinised;
- the ICT co-ordinator/network manager will review the system's capacity regularly;
- additional monitoring may take place as part of an investigation following evidence of apparent misuse;
- school staff will comply with the *Schools Information Security Policy.*

11.2. How is e-mail regulated?

The school has the following measures in place to regulate the use of e-mails:

- pupils may only use e-mail accounts approved by the school;
- staff may only use official, school e-mail accounts to communicate with pupils;
- pupils must inform a teacher immediately if they receive an offensive e-mail;
- pupils must not reveal personal details about themselves or others in an e-mail message, or arrange to meet anyone without specific consent;
- overuse of social e-mailing can hamper learning, and restrictions are therefore in place;
- care should be taken when e-mailing outside establishments and permission should be sought before sending an e-mail, as with letters written on headed notepaper;
- permission will not be given to send chain letters on to other addresses;
- school staff will comply with the *School Staff E-mail Policy.*

11.3. How is published content regulated?

The school has the following measures in place to regulate published content:

- the school's address, e-mail address and phone number should be included as contact details on the website. Personal information about staff or pupils must not be published;
- the SLT and administrative team will be responsible in general for editing the material and ensuring that it is accurate and appropriate;
- care should be taken when publishing e-mail addresses to avoid receiving spam;
- the school website/social network accounts should correspond with school guidelines for publications, including respect for intellectual property and copyright;
- school staff will comply with the *School Staff Social Media Policy* and *Schools taking Photographs for Publicity Purposes Policy.*

11.4. Can the work or photos of pupils be published?

The school has measures in place to ensure that photographs, images and personal information is shared only in certain circumstances and with the following steps in place:

- photos and images which include pupils are chosen carefully. Text which accompanies pictures should not identify individual pupils;
- pupil names are not used anywhere on the school website or social media accounts in connection with photographs and images;
- written approval is sought from parents/carers before photos of pupils are included on the school website/social media accounts via consent forms;
- work can only be published with the agreement of the pupil and his/her parents/carers;
- the school will comply with the *Schools Taking Photographs for Publicity Purposes Policy.*

11.5. <u>How is social networking and personal publishing regulated?</u>
The school will have the following measures in place to regulate what is accessed in terms of websites and social media and what is published:

- the school will block/filter access to social networking sites. The Isle of Anglesey County Council filtering service currently blocks access to a number of social networking sites. However, schools are responsible for giving information about any other sites they may need to be filtered/blocked;
- inappropriate forums will be blocked;
- pupils are advised never to give out any personal details that give information about their identity or location. Examples include real name, address, mobile phone number or house number, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.;
- pupils should be told not to include personal photos on any social network space. They should consider how public the information may be, and consider using private areas. Advice should be given about any background details in the photo that might identify the pupil or his/her location e.g. house number, street name or school;
- passwords should be used to safeguard blogs or official wikis made by teachers, and these should be run on the school website. Teachers should be advised not to run social networking spaces for the personal use of pupils;
- pupils should be advised about safety and encouraged to create passwords, refuse access to individuals they do not know, and be trained on how to prevent unwelcome messages. Pupils should be encouraged to invite only friends, and to refuse access to others;
- pupils should be advised to refrain from publishing specific, detailed private thoughts;
- schools should be aware that bullying can occur through social networking, in particular where a space has been created which is unprotected by a password and others have been invited to view the bully's comments;

- school staff will comply with the *Schools taking Photographs for Publicity Purposes Policy* and *School Staff Social Media Policy;* and *Schools Information Security Policy.*

11.6. How is filtering regulated?

The school has the following measures in places to regulate filtering:

- the school will work with the Isle of Anglesey County Council ICT Service to ensure that systems that protect pupils are regularly revised and improved;
- if staff or pupils discover inappropriate websites, the URL must be given to the ICT Co-ordinator and systems manager, to be forwarded immediately to the Isle of Anglesey County Council IT Services Helpdesk and distributed to every school system;
- all access to the internet in school will be logged;
- internet use will be randomly monitored to ensure that it conforms with school policy;
- all internet access within the school is filtered. Under rare circumstances, there will be a genuine need to bypass technical restrictions by using an unfiltered connection. The Headteacher should give personal permission every time the internet is used without a filter, and review the need for regular access;
- the school uses a combination of Walled Garden access and filtered access which is appropriate for the age of pupils, to support pedagogical objectives;
- the *Schools E-Safety Policy* is compatible with the school's policy with regard to discipline;
- senior members of staff will ensure that filtering methods are regularly reviewed to ensure that those methods are appropriate, effective and reasonable;
- the appropriate agencies must be informed about any material that the school believes to be illegal;
- school staff will comply with the *Schools Information Security Policy.*

11.7. How is videoconferencing monitored?

The school has the following measures in place regarding videoconferencing:

- all videoconferencing equipment in class should be switched off when not in use;
- equipment that is connected to Lifelong Learning Wales Network use the national E.164 numbering system;
- external IP addresses should not be made available to other sites;
- videoconferencing contact information should not be included on the school website;
- the equipment must be kept safe and locked up if necessary when not in use;
- videoconferencing equipment should not be taken away from the school site without permission. The way a network is used cannot be monitored or controlled on any network apart from the educational network.

11.7.1. Users

- pupils should seek the permission of the supervising teacher before making or answering a videoconferencing call;
- videoconferencing should be appropriately supervised according to the age of the pupils;
- great care must be taken when delegating responsibility for the use of videoconferencing equipment outside school hours;
- only key members of staff should have access to the videoconferencing system, website or other remote control page which is available on larger systems;
- only members of staff should have access to any unique logon details and passwords for the educational videoconferencing services, and these details should be kept in a safe place.

11.7.2. Content

- when recording a videoconferencing lesson, the reason for the recording must be given, and at the start of the conference it should be made clear to all who take part that the conference is being recorded;
- material that is being recorded must be stored safely according to the *Schools Retention Schedule;*
- if material belonging to a third party is included, staff should ensure that making a recording is acceptable to avoid transgressing the intellectual property rights of the third party;
- videoconferencing is a challenging activity that provides pupils with a wide variety of learning benefits. Preparation and evaluation are essential parts of the whole activity;
- dialogue should be held with others who are involved in the conference before taking part in the videoconference. If the conference is taking place on a different site, away from the school, it is important that it provides material that is appropriate for the class.

11.8. How is on-line learning monitored?

The school has the following measures in place regarding on-line learning:

- pupils are encouraged to work from a suitable shared home location where they feel comfortable;
- it is recommended that teachers and pupils use the facility that can change or blur background display;
- pupils do not have to switch their camera on- turning the camera on is optional;
- an agreement is in place between the school (teacher) and with parents/carers regarding expectations and behaviours of pupils and parents/carers during on-line lessons;
- some lessons may be recorded for safeguarding purposes. Participants will be told when the lesson is being recorded;

- the school has a *Recording Livestreaming Sessions Policy* and a *Recording Retention Policy.*
- the school has a guidebook on on-line learning for both staff and parents.

11.8.1. Teachers agree to:

- be punctual at the start and end of each lesson;
- discuss roles and responsibilities with pupils at the outset of all lessons;
- create and agree on basic rules and clear behaviour standards based on the school's current behaviour management policy;
- clearly communicate that 'classroom standard' behaviour is expected from everyone present;
- establish expectations from the start and explain the rules by giving an introduction to the session (e.g. who is allowed to speak, how to ask a question or ask for help);
- notify the school's senior management team, pupils and parents/carers of any scheduled lessons, cancelled lessons or changes in arrangements;
- ensure that they keep themselves up-to-date with all relevant policies and procedures, including online safety, safeguarding and data protection policies;
- prevent a one-to-one situation at the end of an online class by disconnecting all participants at the close of the lesson.

11.8.2. Parents/carers agree to:

Parents/carers agree that their child will adhere to the rules and expectation of use:

- pupil will be permitted to join the school's online lessons provided that the pupil as a learner and the parent/carer commit to the code of conduct;
- parent/carer to undertake to read and discuss the code of conduct with the pupil;
- pupil will be punctual to each lesson;
- pupil has access to the relevant files for each lesson in advance and have the materials to hand;
- pupil's device (laptop/Chromebook/PC etc.) is ready before the lesson starts with the pupil already logged in to their account;
- parent/carer to do their best to make sure the pupil is properly dressed. Parent/carer understand that wearing nightwear is not considered as appropriate clothing;
- parent/carer to try to ensure that the pupil is in a suitable room e.g. living room or dining room and give consideration to background, camera angle, privacy, etc.;
- parent/carer to try to make sure nothing else is going on in the room e.g. will try to make sure that the siblings in the room are not playing, that the TV is turned off and that nothing distracts or interrupts the lesson/meeting. If this is not possible will do their best to ensure that the atmosphere of the room is suitable for the pupil to have a lesson with a group of other pupils. If this is not

possible, the microphone will be muted in order to prevent the noise in the room from disrupting the lesson;

- parent/carer understand that the same standards of behavior are expected as if the pupil was in school. Parent/carer understands that the teacher will break contact if the pupil displays any inappropriate behavior;
- parent/carer to try to ensure that the pupil shows respect for everyone in the online classroom and seek to contribute to the class in a positive manner and not be disruptive at any time;
- that no part of the lesson/meeting is recorded on any device or photos are taken by anyone in the home;
- on no account will parent/carer join in or disrupt the lesson/meeting;
- if parent/carer has a concern, they understand that this should not be expressed during the lesson/meeting. Parent/carer can discuss the concern by contacting the school after the lesson.

11.9. <u>How do pupils learn how to evaluate internet content?</u>

- the school will ensure that materials obtained from the internet that are copied or used on other occasions by staff and pupils conform to copyright law;
- pupils should be taught to be critically aware of the materials they read, and should be shown how to verify information before accepting it as accurate;
- pupils will be taught to acknowledge the source of the information they are using and to respect copyright when using internet materials in their work.

11.10. <u>How can the latest technology be regulated?</u>

The school will have the following measures in place to regulate technology:

- the latest technologies will be examined for their educational value, and a risk assessment will be made before permission is granted to use them in the school;
- mobile phones must not be used during lessons or formal lesson time; abusive or inappropriate text messages are banned;
- the school will comply with the *Schools Information Security Policy.*

12. How is personal data protected?

The school will ensure that its information and communication technology systems comply with data protection legislation requirements. Personal data is recorded, processed, transferred and made available online in accordance with the *UK General Data Protection Regulation (UK GDPR)* and the *Data Protection Act 2018.*

All users will comply with the *Schools Data Protection Policy* and *Schools Information Security Policy*, including the requirement for secure storage of information.

In the event of a data breach arising from the use of the internet, website, social media account, on-line learning etc., the school will immediately inform the Schools Data Protection Officer and will comply with the *Schools Data Breach Policy.*

13. Policy Decisions

13.1. How is access to the internet authorised?

- the school will keep an ongoing record of every staff member and pupil who has permission to access the school's electronic links;
- pupils must apply individually for access to the internet by agreeing to conform to the e-safety rules;
- parents are asked to sign and return a form granting permission for pupils to access the internet;
- parents are informed that pupils will be granted access to the internet under supervision.

13.2. How is risk assessed?

Technology can provide security and reassurance; however there are also associated risks. Pupils need to understand these risks in order to help them develop appropriate strategies for keeping themselves safe.

Risks to children and young people can be broadly categorised under the headings of content, contact and conduct and can be managed by reducing availability, restricting access and increasing resilience.

The school promotes safe and appropriate practice through establishing clear and robust acceptable use guidelines. This is achieved through balancing protection against potential misuse with the recognition that technology is an effective communication tool.

The school will take every reasonable step to ensure that users have access to appropriate material only. Despite this, because of the global nature of the internet and its subject links, it is impossible to guarantee that inappropriate material will never be accessed on a school computer. Neither the school nor the Isle of Anglesey County Council can accept responsibility for the material that is accessed or for any consequences that may result from use of the internet.

It may be appropriate to undertake a Data Protection Impact Assessment (DPIA) for types of processing likely to result in a *high risk* to individuals' interests. It should be considered whether a DPIA is needed **before** using any new technology. The Schools Data Protection Officer can provide advice and guidance regarding DPIAs.

Using computer systems without permission or for inappropriate purposes can be a crime under the *Computer Misuse Act 1990.*

The methods of recognising, assessing and reducing the risks are regularly reviewed.

13.3. How are complaints about e-safety dealt with?

- a senior member of staff deals with complaints about misuse of the internet;
- any complaints about staff misusing the internet must be directed to the Headteacher;
- pupils and parents are informed about the complaints procedure;
- parents and pupils must work in partnership with staff to resolve matters;
- discussions are held with the local Police Public Protection Unit to establish procedures for dealing with possible crimes;
- the punishments cited in the school's policy include the following:

    - interview/counselling from the head of year;
    - informing parents and guardians;
    - banning access to the internet or a computer for a specific period of time.

13.4. How is the internet used across the community?

- the school will contact local organisations to ensure that there is a common approach towards e-safety;
- the school will demonstrate sensitivity when dealing with matters involving the internet that pupils discover outside school, e.g. social networking sites, and offer appropriate advice.

14. Communication Policy

14.1. How is the policy presented to the pupils?

- e-safety rules will be displayed in rooms that have internet access;
- pupils are made aware that all use of the internet is monitored;
- a e-safety programme is presented to raise awareness of the importance of using the internet safely and responsibly;
- guidelines should be given on how to use the internet responsibly and safely before allowing access to the internet;
- a module on e-safety will be included in the PSE/ICT programmes that encompass use of the internet in the school and at home.

14.2. How is the policy discussed with staff?

- every member of staff receives a copy of the school's *E-safety Policy* and an explanation of how to implement the policy and the importance of the policy;
- staff should be aware that internet traffic can be monitored and tracked; Acting wisely and behaving in a professional manner is of the utmost importance;
- staff who manage the filtering systems or monitor the use of ICT are supervised by senior managers, and have clear procedures for reporting any matters of concern;

- training is provided on how to use the internet safely and responsibly and on the school's *E-safety Policy* whenever necessary.

14.3. How is the policy shared with parents/carers?

- Parents/carers are made aware of the school's policy by means of newsletters; the school handbook and the school website;
- matters relating to the internet are treated with sensitivity, and parents/carers are informed of any steps that have been taken;
- working in partnership with parents/carers is encouraged. This can include parents' evenings that include displays and suggestions on how to use the internet safely at home;
- parents/carers are given advice about filtering systems and educational and leisure activities which include using the internet;
- parents/carers who are interested are directed to the organisations listed in section 18.

15. Responding to an incident that causes concern

Internet technology and electronic communication provides children and young people with the opportunity to broaden their experiences and develops their creative ability within school and beyond. However, it is important to be aware of the dangers of using these technologies.

The risks to e-safety occur because of people who act inappropriately or even illegally. Any personal matter that arises must be dealt with. Teachers are the front line of defence; it is they who observe the pupils, and this is crucial with regard to becoming aware of risks to pupils and gaining the trust of pupils so that matters can be dealt with. Incidents can vary from a thoughtless action or piece of mischief to illegal action that has been carefully planned.

15.1. What are the dangers?

Some potential dangers of such technologies include:

- receiving inappropriate content;
- grooming and cultivating an inappropriate relationship;
- requests for personal information;
- viewing sites that 'encourage';
- bullying and threats;
- identity theft;
- publication of inappropriate content;
- online gambling;
- abuse of computer systems;
- publication of personal information;
- hacking and breaking safety rules;
- corrupting or misusing data;

- providers that do not supply any solid ownership or contact information for their sites;
- the dangers inherent when sites can be set up using a false name and e-mail address with no identity checking;
- the posting of anonymous comments that may be malicious;
- sites that give safety of users a low priority;
- sites that celebrate inappropriate and unacceptable behaviour.

15.2. How the school should respond?

The Child Protection Officer can provide guidance when a member of staff is concerned about the use made of the internet by a child, young person or member of staff.

Please refer to APPENDIX A. The flowchart shows the steps that must be taken when dealing with a matter of concern. This diagram should only be a starting point, as the Learning Service and Children & Families Service provide additional documents to help schools respond to incidents which involve child safety.

16. The Legal Framework

Many young people and even members of staff regularly use the internet without realising that some of the activities they are doing are possibly illegal. The law develops rapidly and recent changes have been enforced by means of the following:

- The *Sexual Offences Act 2003* deals with new offences such as fostering an inappropriate relationship online, and making/distributing indecent images of children, has raised the age of a child to 18;
- The *Racial and Religious Hatred Act 2006*, which creates new offences involving incitement of hatred based on religious belief; and
- The *Police and Justice Act 2006* extends the limits of the *Computer Misuse Act (1990)* by criminalising failing to prevent an attack on the system.

16.1. The Children's Code

As of 2 September 2021, online services need to follow a set of standards when using children's data. These standards are known as the Children's Code.

The Children's Code is a set of rules designed to make the internet a safer place for children to learn, explore and play. It requires organisations to put the best interests of the child first when they are designing and developing apps, games, connected toys and websites that are likely to be accessed by young people.

Websites and products need to provide additional layers of protection for children's data. This might involve restricting or removing certain features to children if they're under 18 resulting in:

- privacy settings being automatically set to very high;

- children and their parents/carers being given more control of the privacy settings;
- non-essential location tracking being switched off;
- children no longer being 'nudged' by sites through notifications to lower their privacy settings; and
- clearer and more accessible tools being in place to help children exercise their data protection rights (including parental consent tools).

The ICO has developed resources for schools to help children identify where they can go to for support, including what they should do if they suspect an app, game or website is misusing their data or not conforming to the Children's Code.

Resources can be found on the ICOs website:

Information for primary schools: https://ico.org.uk/for-organisations/posters-stickers-and-e-learning/school-resources/wales-primary/

Information for secondary schools: https://ico.org.uk/for-organisations/posters-stickers-and-e-learning/school-resources/wales-secondary/

16.2. Relevant Legislation

The following legislation also deals with different aspects of e-safety:

Racial and Religious Hatred Act 2006	This Act criminalises the act of threatening people because of their religious beliefs, or inciting religious hatred by showing, publishing or distributing written material that is threatening. Other laws already protect people against threats based on race, gender or ethnic background.
Sexual Offences Act 2003	The new offence of cultivating an inappropriate relationship online is committed if you are 18 years old and have communicated with a child under 16 years of age at least twice (including by phone or over the internet). It is an offence to meet them or to travel to meet them anywhere in the world with the intention of committing a sexual offence. Forcing a child of under 16 years of age to watch a sexual act, including looking at videos, photographs or a web camera, for your own pleasure is illegal. It is also an offence for a person in a position of trust to commit a sexual act with any person under 18 years of age over whom they have a position of trust. (Teachers, social workers, your workers and health professionals are all included in this category of trust). Anyone who has sexual intercourse with a child of under 13 years of age is committing rape.

	The following document contains useful information: "*Children & Families: Safer from Sexual Crime*": Sending a message or other content that is extremely offensive or of an indecent, obscene or threatening nature via the internet; or sending false messages via the internet or using the internet constantly to unnecessarily anger, inconvenience or worry someone, is guilty of a crime that may lead to a period in prison. This wording is important as an offence has been committed as soon as the message has been sent: it is not necessary to prove any intent or purpose.
UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018	These require that anyone who deals with personal information must conform to important principles of data protection when dealing with personal data relating to a living person. These also grant individuals the right to see the personal information relating to them that is being held, receive compensation and prevent processing of the information.
Computer Misuse Act (1990) (sections 1-3)	Irrespective of the individual's motive, the Act dictates that it is a crime to: • access computer files or software without permission (e.g. using someone else's password to gain access to files); • access without permission, as above, in order to commit another offence (such as deception); or • interfere with a computer or programme's ability to function (for example caused by a virus or by failing to prevent an attack on the system). UK citizens or residents can be extradited to another country if it is suspected that they have committed one of the above offences.
Malicious Communications Act 1988 (section 1)	This legislation dictates that it is a crime to send an electronic message (e-mail) that conveys indecent, extremely offensive, threatening or untrue information; or that is of an indecent nature or extremely offensive if the intention was to cause the recipient concern or anxiety.
Copyright, Designs and Patents Act 1988	Copyright is an individual's right to prevent others from copying or using his or her "work" without permission. The material under copyright (known as "work") must be a work that was created by the author themselves and the product of skill and judgement. Copyright arises when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programmes are all eligible for protection by copyright. It is usually the author of the work

	who owns the copyright, but if the work was created during employment, then it is the employer who owns the copyright. Making a copy of the whole or a substantial part of anyone's work without the author's permission is an infringement of copyright. There will usually be a certificate accompanying the work that permits the user to copy or use it for restricted purposes. It is always wise to read the terms of the license before making a copy or using anyone else's material. It is also illegal to adapt or use software without a license or in any way that is prohibited by the conditions of the software license.
Public Order Act 1986 (sections 17-29)	This Act dictates that it is an offence to incite racial hatred by showing, publishing or distributing written material that is threatening. As in the case of the *Racial and Religious Hatred Act 2006* it is also an offence to be in possession of inflammatory material with the intention of releasing it.
Children Act 1989	It is an offence to take, give permission to take, make, possess, show, distribute or advertise indecent photographs of children in Great Britain. In this case, a child means anyone under 18 years of age. Looking at an image of a child on your computer means that you have made a digital image. An image of a child also includes making false images (digitally altered or otherwise). A person who is found guilty of such a crime could face a period of 10 years in jail.
Social Services and Well-being (Wales) Act 2014 (section 130)	There is a duty to report children at risk if there is reasonable cause to suspect that a child is a child at risk and appears to be within the authority's area. This could be relevant in terms of e-safety if a child is at risk.
Obscene Publications Act 1959	Publishing an "obscene" article is a crime. Publishing includes electronic transfer.
Protection from Harassment Act 1997	A person must not behave in a manner that causes harassment to another person, when he or she knows, or should know, that the behaviour is causing harassment. A person behaving in a manner that causes another person, on at least two occasions, to believe that violence will be inflicted on them, is guilty of an offence if they know or should know that their behaviour is causing another person fear.
Regulation of Investigatory Powers Act 2000	The *Regulation of Investigatory Powers Act 2000* regulates the process of intercepting communications and makes it an offence to intercept or monitor communications without the permission of the parties who are involved in the communications. This Act was passed to conform to the *Human Rights Act 1998*. However, *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*, permits

	a certain amount of monitoring and record keeping, for example, to ensure that the communication is relevant to a school's activities or in order to investigate or discover use made of the internet without permission. Despite this, before monitoring, permission should be obtained based on information, which means that steps must be taken to ensure that everyone who is going to use the system knows that the communication is going to be monitored. Secretly monitoring without informing the users that someone is doing so risks infringing data protection legislation and privacy legislation.
Communications Act 2003 (section 127)	It is an offence to send by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character, or false for the purpose of causing annoyance, inconvenience or needless anxiety to another.
Coroners and Justice Act 2009 (section 62)	This covers the possession of prohibited images of children.
The Cookie Law	The Cookie Law is a piece of privacy legislation that requires websites to get consent from visitors to store or retrieve any information on a computer, smartphone or tablet. http://www.cookielaw.org/the-cookie-law/

17. E-safety Contact Names and Addresses

Child Exploitation & Online Protection Centre http://www.ceop.gov.uk	Think U Know website http://www.thinkuknow.co.uk/
Wise Kids website www.wisekids.org.uk	Internet Watch Foundation http://www.iwf.org.uk/
Childline http://www.childline.org.uk/	Internet Safety Zone http://www.internetsafetyzone.com/
Childnet International https://www.childnet.com/	NSPCC https://www.nspcc.org.uk/
Virtual Global Taskforce – Report Abuse http://www.virtualglobaltaskforce.com/	Internet Matters www.internetmatters.org
Internet Watch Foundation (IWF) www.iwf.org.uk	Lucy Faithfull Foundation www.lucyfaithfull.org

Net Aware www.net-aware.org.uk	The Marie Collins Foundation www.mariecollinsfoundation.org.uk
UK Safer Internet Centre www.saferinternet.org.uk	Professional Online Safety Helpline www.saferinternet.org.uk/about/helpline
360 Safe Self-Review tool for schools www.360safe.org.uk	Action Fraud www.actionfraud.police.uk
Get Safe Online www.getsafeonline.org	

18. Training

The Headteacher and the Schools Data Protection Officer will ensure that staff, including school governors, are adequately trained regarding e-safety.

The training will be linked to training about child protection and data protection. It will cover related matters such as the law on copyright of electronic materials.

The Headteacher will keep a record of attendance and a register of who has completed e-safety training and when they have completed it.

The school will offer education and information to parents, carers about e-safety.

19. 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.

Non-compliance by a member of staff may therefore be subject to the school's disciplinary procedure. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

20. Review of Policy and Oversight Arrangements

This policy will be reviewed by the Schools Data Protection Officer every two years, unless changes to legislation, codes of practice, or guidance requires the policy to be updated sooner.

This policy will be approved by the Learning Service Senior Management Team with the input of the Schools Data Protection Operational Group 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.

The school will appoint a specific member of staff who will be responsible for e-safety/ICT.

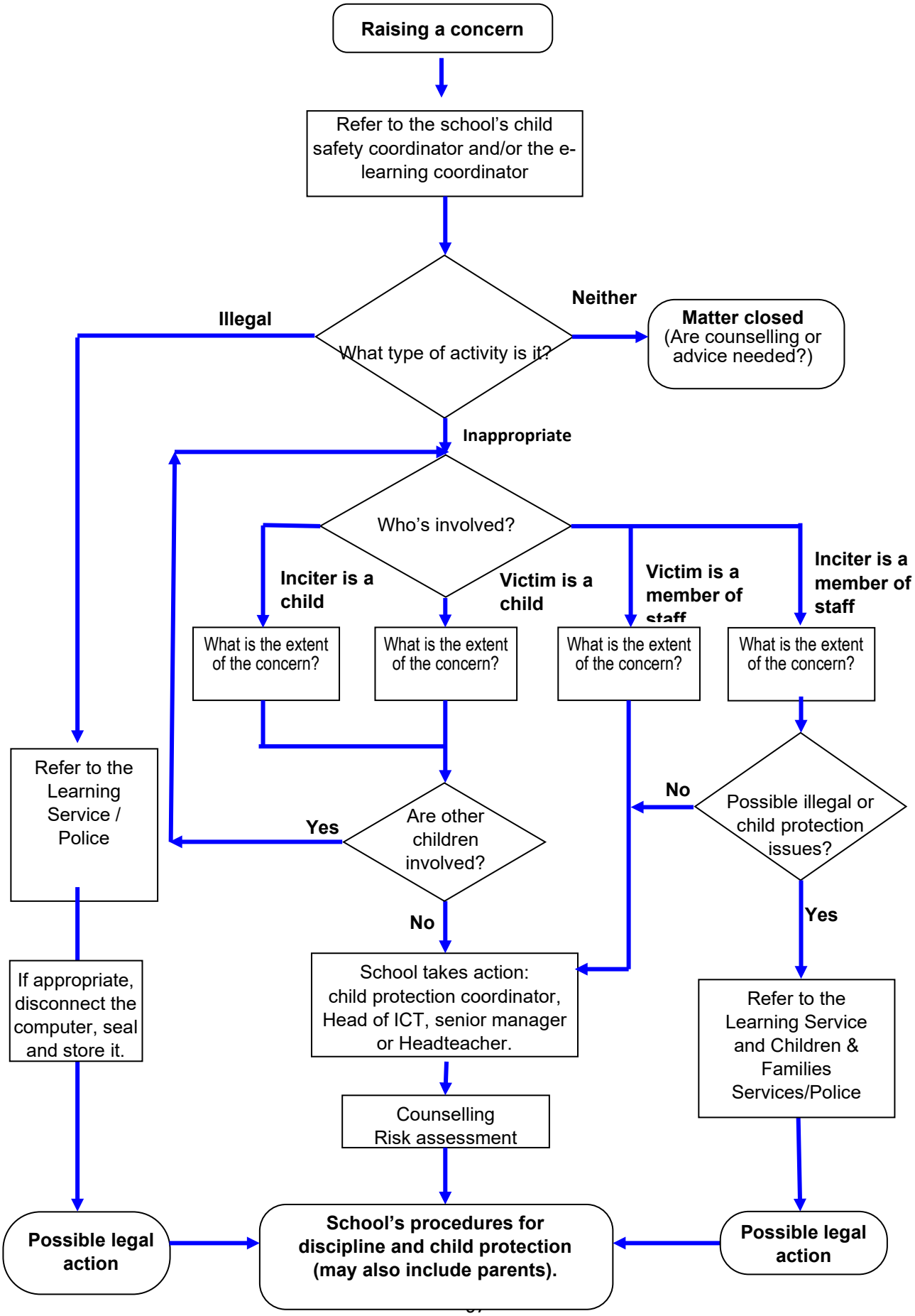
If there are any queries or concerns about anything contained in this policy, the Schools Data Protection Officer should be contacted without hesitation:

E-mail: dpoysgolionmon@ynysmon.llyw.cymru

Telephone: 01248 751833

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

APPENDIX A- Responding to an incident that causes concern



APPENDIX B

Schools E-Safety 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 E-Safety 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	This policy has been shared with all school staff and volunteers and an explanation provided of how to implement the policy and the importance of the policy.	
4	Staff have received appropriate training in e-safety and this is given high priority across the school.	
5	The Headteacher maintains a record of attendance and a register of who has completed e-safety training and when they have completed it.	
6	A specific member of staff who will be responsible for e-safety/ICT has been appointed and this person has adequate support from, and provides support to, other school staff, particularly the designated senior person for safeguarding.	
7	Personal information within the school is kept and processed in line with *UK GDPR* and the *Data Protection Act 2018.*	
8	There is a process in place to protect all personal and special category information within the school.	
9	Details of the arrangements of e-safety is regularly discussed and reviewed with all school staff.	
10	The level of access to be granted to specific individuals has been determined.	
11	The school's Information Asset Register and Records of Processing Activities (ROPA) are regularly reviewed and are kept up-to-date.	

12	A risk assessment is undertaken on any new technologies before permission is granted to use the technology in the school. The Schools Data Protection Officer is always contacted when implementing or changing a process or system, in order to determine whether a DPIA is required or not.	
13	Information assets and risks within the school are managed.	
14	Guidance is obtained from the Schools Data Protection Officer on agreements relating to information and communication technology apps, software and systems.	
15	Records are kept of all e-safety incidents and these are reported to the senior leadership team.	
16	Internal audits that monitor compliance are conducted at least once a term.	
17	There is a robust process in place to detect and identify data breaches; to investigate and assess breaches including risks and to share any data breach incidents with the Schools Data Protection Officer.	
18	A reporting and learning culture has been established to allow the school to establish where problems exist and to develop strategies with the Schools Data Protection Officer to prevent future problems occurring.	
19	Staff are aware of the process to access and seek support and guidance relating to raising concerns and responding to online safety concerns.	
20	The necessary steps have been taken to protect the technical infrastructure and they meet technical requirements of the school's information and communication technology systems.	
21	Regular checks are conducted on information and communication technology systems to ensure they are as safe and secure as is reasonably possible. Advice and guidance on the technical requirements for those systems is sought.	
22	The school undertakes regular reviews of the safety and security of its information and communication technology systems through the use of suitably skilled contractors/support providers.	
23	Anti-virus protection is regularly updated.	
24	No unmanaged devices are connected to the school's network without the agreement of the Isle of Anglesey County Council ICT Unit.	

25	The school's network is segregated into logical sub networks and firewalled according to the needs of the users and security level of the users on that network.	
26	The school's systems provides for filtering internet access for all users, prevents access to illegal content, and has additional filtering for different groups of users.	
27	Personal data sent over the internet is encrypted or is made safe by other means.	
28	The school has reserve strategies (including offline and offsite requirements) that correspond with school requirements with regard to retrieval in the event of a disaster.	
29	Safety strategies are discussed with the Isle of Anglesey County Council ICT Service where appropriate.	
30	No portable devices are used without specific permission and without being subjected to an examination for viruses.	
31	Files that are kept on the school network are regularly scrutinised.	
32	The ICT co-ordinator/network manager regularly reviews the system's capacity.	
33	Staff only use official, school e-mail accounts to communicate with pupils.	
34	Pupils are aware that they must inform a teacher immediately if they receive an offensive e-mail.	
35	Pupils are aware that they must not reveal personal details about themselves or others in an e-mail message, or arrange to meet anyone without specific consent.	
36	Restrictions are in place to prevent the overuse of social e-mailing.	
37	The school's address, e-mail address and phone number has been included as contact details on the website (if relevant).	
38	The school website/social network accounts correspond with school guidelines for publications, including respect for intellectual property and copyright.	
39	Pupil names are not used anywhere on the school website or social media accounts in connection with photographs and images.	
40	Written approval is sought from parents/carers before photos of pupils are included on the school website/social media accounts via consent forms.	

41	Work is only published with the agreement of the pupil and his/her parents/carers.	
42	The SLT and administrative team edit the material for the school website and social media accounts and ensure that it is accurate and appropriate.	
43	The school blocks/filters access to social networking sites.	
44	Inappropriate forums are blocked.	
45	The school works with the Isle of Anglesey County Council ICT Service to ensure that systems that protect pupils are regularly revised and improved.	
46	Internet use is randomly monitored to ensure that it conforms to school policy.	
47	The Headteacher always gives personal permission every time the internet is used without a filter, and reviews the need for regular access.	
48	Senior members of staff ensures that filtering methods are regularly reviewed to ensure that those methods are appropriate, effective and reasonable.	
49	Staff who manage the filtering systems or monitor the use of ICT are supervised by senior managers, and have clear procedures for reporting any matters of concern.	
49	All videoconferencing equipment in class is switched off and is kept locked when necessary when not in use.	
50	Videoconferencing contact information is not included on the school website.	
51	Videoconferencing equipment is not taken away from the school site without permission.	
52	Videoconferencing is appropriately supervised according to the age of the pupils.	
53	Only key members of staff have access to the videoconferencing system, website or other remote control page which is available on larger systems.	
54	Only members of staff have access to any unique logon details and passwords for the educational videoconferencing services, and these details are kept in a safe place.	

55	When recording a videoconferencing lesson, the reason for the recording is always given at the start of the conference and it is made clear to all who take part that the conference is being recorded.	
56	Material that is being recorded is stored safely according to the *Schools Retention Schedule.*	
57	Teachers and pupils use the facility that can change or blur background display whilst on an on-line lesson.	
58	There is an agreement is in place between the school (teacher) and with parents/carers regarding expectations and behaviours of pupils and parents/carers during on-line lessons.	
59	The school has a *Recording Livestreaming Sessions Policy* and a *Recording Retention Policy.*	
60	The school has a guidebook on on-line learning for both staff and parents.	
61	The school ensures that materials obtained from the internet that are copied or used on other occasions by staff and pupils conform to copyright law.	
62	The school keeps an ongoing record of every staff member and pupil who has permission to access the school's electronic links.	
63	Pupils have to apply individually for access to the internet by agreeing to conform to the e-safety rules.	
64	Parents are asked to sign and return a form granting permission for pupils to access the internet and parents are informed that pupils will be granted access to the internet under supervision.	
65	A senior member of staff has been designated to deal with complaints about misuse of the internet and any complaints about staff misusing the internet are directed to the Headteacher.	
66	E-safety rules are displayed in rooms that have internet access.	
67	Staff respond to an incident that causes concern by following the steps in the flowchart that is include in Appendix A.	
68	School staff are aware of the set of standards within the Children's Code.	