Polisi E-ddiogelwch
E-Safety Policy

Ffederasiwn Ysgol Dyffryn Dulas ac Ysgol Pennal

1. Cyflwyniad

1.1 Mae'r Polisi e-Ddiogelwch yn rhan o'r Cynllun Datblygu Ysgol ac mae'n ymwneud â pholisïau eraill gan gynnwys y rhai TGCh, bwlio ac amddiffyn plant.

1.2 Mae ein Polisi e-Ddiogelwch wedi'i gytuno gan yr uwch dîm ac wedi'i gymeradwyo gan y llywodraethwyr.

2. Dysgu ac addysgu

2.1 Mae'r rhyngrwyd a chyfathrebu digidol yn bwysig oherwydd:
- Mae'r rhyngrwyd yn elfen hanfodol ym mywyd yr 21ain ganrif ar gyfer addysg, busnes a rhyngweithio cymdeithasol. Mae'n ddyletswydd ar yr ysgol i gyflwyno mynediad o ansawdd dda i'r rhyngrwyd fel rhan o'u profiad dysgu
- Mae defnyddio'r rhyngrwyd yn rhan o'r cwricwlwm statudol ac mae'n offeryn hanfodol i staff a disgyblion

2.2 Bydd defnyddio'r rhyngrwyd yn fanteisiol i addysg oherwydd iddo:
- Roddi mynediad i adnoddau addysgol ledled y byd
- Alluogi cydweithio ar draws gwasanaethau cefnogi a chymdeithasau proffesiynol
- Gyfnewid data'r cwricwlwm a gweinyddiaeth gyda'r Awdurdod Lleol a Llywodraeth Cynulliad Cymru

2.3 Bydd defnyddio'r rhyngrwyd yn gwella dysgu disgyblion oherwydd:
- Caiff y mynediad i'r rhyngrwyd yn yr ysgol ei ddylunio'n benodol at ddefnydd disgyblion a bydd yn cynnwys hidlo sy'n berthnasol i oedran y disgyblion
- Caiff y disgyblion eu dysgu pa ddefnydd o'r rhyngrwyd sy'n dderbyniol a'r hyn sy'n anerbyniol a rhoi amcanion clir ar gyfer defnyddio'r rhyngrwyd
- Caiff disgyblion eu haddysgu i ddefnyddio'r rhyngrwyd yn effeithiol wrth ymchwilio, gan gynnwys sgiliau gwybodaeth, lleoli, adennill a gwerthuso
- Caiff disgyblion eu dysgu sut i gyhoeddi a chyflwyno gwybodaeth i gynulleidfa ehangach.

2.4 Bydd disgyblion yn dysgu sut i werthuso cynnwys y rhyngrwyd trwy:
- I'r ysgol sicrhau y bydd defnyddio deunyddiau'r rhyngrwyd gan staff a disgyblion yn cydymffurfio â chyfraith hawlfraint
- I ddisgyblion yn dysgu am bwysigrwydd gwirio gwybodaeth cyn derbyn ei bod yn gywir
- I'r disgyblion yn dysgu sut i adrodd am unrhyw gynnwys annymunol ar y rhyngrwyd e.e. defnyddio'r eicon CEOP Adrodd am Gamdriniaeth

3. Rheoli Systemau Gwybodaeth

3.1 Diogelwch systemau gwybodaeth
- Caiff systemau TGCh yr ysgol eu hadolygu'n rheolaidd
- Caiff y system amddiffyn yn erbyn firysau ei diweddaru'n rheolaidd
- Caiff strategaethau diogelwch eu trafod â'r Awdurdod Lleol

3.2 E-bost
- Gall disgyblion ddefnyddio cyfrifon e-bost cymeradwy ar system yr ysgol
- Rhaid i ddisgyblion ddweud wrth athro/athrawes ar unwaith os ydynt yn derbyn e-bost sarhaus
- Wrth gyfathrebu drwy e-bost, ni ddylai disgyblion ddatgelu eu manylion personol na manylion unrhyw un arall, neu drefnu i gwrdd ag unrhyw un heb ganiatâd penodol
- Ni chaniateir anfon llythyron cadwyn

- Dylid trin e-byst sy'n dod i mewn yn amheus ac ni ddylech agor dogfennau wedi'u hatodi nes dod i hyd i'r awdur
- Dylai'r ysgol ystyried sut caiff e-byst gan ddisgyblion i gyrff allanol eu gosod a'u rheoli

3.3 Cynnwys a gyhoeddir a gwefan yr ysgol
- Ni chyhoeddir gwybodaeth gyswllt staff na disgyblion. Dylai'r manylion cyswllt a roddir ar-lein fod yn fanylion swyddfa'r ysgol.
- Bydd y Pennaeth yn gyfrifol am olygu cyffredinol ac yn sicrhau bod y cynnwys yn gywir ac yn addas.

3.4 Cyhoeddi delweddau o ddisgyblion a'u gwaith
- Dewisir ffotograffau sy'n cynnwys disgyblion yn ofalus fel na ellir adnabod disgyblion unigol na chamddefnyddio'r delweddau. Byddwn yn ystyried defnyddio ffotograffau grŵp yn hytrach na lluniau o wynebau llawn y plant.
- Ni chaiff enwau llawn disgyblion eu defnyddio yn unman ar wefan yr ysgol neu ar unrhyw wefan arall, yn enwedig gyda ffotograffau.
- Bydd rhaid cael caniatâd gan rieni neu ofalwyr cyn cyhoeddir lluniau o'r disgyblion ar wefan yr ysgol.
- Gellir cyhoeddi gwaith gyda chaniatâd y disgybl a'i rieni/gofalwyr yn unig.
- Ni fydd enwau ffeiliau delweddau plant yn cyfeirio at y plentyn wrth ei enw.
- Dylai rhieni ddeall polisi'r ysgol ar dynnu lluniau a'u cyhoeddi, wrth storio yn yr ysgol ac ar offer electronig annibynnol.

3.5 Diogelu data personol
Caiff data personol ei gofnodi, ei brosesu, ei drosglwyddo a'i wneud ar gael yn unol â Deddf Diogelu Data 2018.

4. Beth mae cyfathrebu electronig yn ei gynnwys?

- Cyfryngau cydweithredu ar y Rhyngrwyd: safleoedd rhwydweithio cymdeithasol a gwe-logiau (blogiau)
- Ymchwil ar y Rhyngrwyd: gwefannau, peiriannau chwilio a phorwyr gwefan
- Ffonau symudol a thabledi cyfrifiadurol
- Cyfathrebu ar y Rhyngrwyd: e-bost a negeseua sydyn
- Gwe-gamerâu a fideogynadledda
- Consolau gêmau diwyfr

4.1 Rhwydweithio cymdeithasol a chyhoeddi personol
- Caiff safleoedd Rhwydweithio Cymdeithasol a grwpiau newyddion eu hidlo oni bai y cymeradwyir defnydd penodol.
- Rhoddir cyngor i ddisgyblion na ddylent gyflwyno manylion o unrhyw fath a allai olygu bod rhywun yn gallu eu hadnabod, adnabod eu ffrindiau na'u lleoliad.
- Yn ddelfrydol, byddai disgyblion yn defnyddio safleoedd rhwydweithio cymdeithasol safonol yn unig, e.e. SuperClubs Plus
- Rhoddir cyngor i ddisgyblion a rhieni y gallai defnyddio safleoedd rhyngweithio cymdeithasol y tu allan i'r ysgol achosi amrywiaeth o beryglon i ddisgyblion.
- Rhoddir cyngor i ddisgyblion ddefnyddio llysenwau ac afatar wrth ddefnyddio safleoedd rhwydweithio cymdeithasol.

5. Gwersi Ffrydio Byw

Mewn amgylchiadau eithriadol gall fod angen defnyddio technoleg ffrydio byw. Mae'r dechnoleg yma'n caniatáu i aelod o staff addysgu criw o ddisgyblion heb fod yn yr un lle. Gall yr athro a'r disgyblion fod yn eu cartrefi e.e

5.1 *Diogelu dysgwyr a'u lles yw'r peth pwysicaf, ac mae hynny'n cael blaenoriaeth dros yr holl ystyriaethau eraill wrth gynllunio gwersi ffrydio byw.*

- Dylech barhau i ddilyn polisïau diogelu'ch ysgol bob amser. Dylid delio â phob mater sy'n ymwneud â diogelwch ar-lein yn yr un ffordd ag y byddech yn delio â mater sy'n ymwneud â dysgu wyneb-yn-wyneb.

- Os oes gennych chi unrhyw bryderon diogelu am blentyn, dylech eu trafod â'r Person Dynodedig sy'n gyfrifol am Amddiffyn Plant.

5.2 Cyn ffrydio gwersi byw dylid ystyried pwrpas, manteision a chyfyngiadau gwers sy'n cael ei ffrydio'n fyw.
- Dylid ystyried a yw dull arall yn fwy addas, e.e. os yw'r athro yn bwriadu dangos sut mae gwneud rhywbeth, efallai y byddai fideo yn fwy addas.

- Meddwl pa ddysgwyr fydd ar gael, e.e. a fydd yr holl ddysgwyr ar gael, a fydd angen i rai ymuno neu adael ar adegau gwahanol? Argymhellir ystyried nifer y dysgwyr ar sesiwn.

5.3 Dylid sicrhau bod hyd y gwersi sy'n cael eu ffrydio'n fyw yn addas ar gyfer eich dysgwyr.

5.4 Dylid sicrhau bod y wers yn cael ei chynllunio ymlaen llaw, a dylid rhoi digon o rybudd i ddysgwyr a rhieni/gofalwyr yn ôl yr angen. Bydd hyn yn cyfrannu tuag at ba mor ddiogel fydd y sesiwn yn ogystal.

- Dylid sicrhau bod yr holl gynnwys yn briodol, ac ar gyfer unrhyw dasgau a fydd yn golygu gwneud ymchwil ar-lein, gwneud yn siŵr bod y gwefannau'n addas cyn y wers.

- Dylid sicrhau bod gan yr holl ddysgwyr fynediad at raglenni meddalwedd angenrheidiol.

- Os yw'r wers yn cynnwys tasgau, cofiwch y bydd angen mwy o amser ar rai dysgwyr o bosib.

5.5 Dylid sicrhau caniatâd yr uwch dim rheoli i ffrydio gwersi byw gan roi gwybod iddyn nhw beth yw'r amserlen ar gyfer pob gwers. Ni ddylid cynnal gwersi ffrydio byw heb yn wybod i'r uwch dim rheoli.

5.6 Dylid gwneud yn siŵr bod cytundebau defnydd priodol yn eu lle ar gyfer yr holl ddysgwyr sy'n rhan o wers sy'n cael ei ffrydio'n fyw. Bydd y cytundeb yn nodi disgwyliadau clir pob parti, ac yn nodi'r camau a fydd yn cael eu cymryd os na fydd rhywun yn cydymffurfio â'r cytundeb.

5.7 **Ymddygiad proffesiynol**

Dylai unrhyw waith ffrydio byw ddigwydd yn wirfoddol, a dylai ymarferwyr addysg sy'n dewis ffrydio'n fyw barhau i weithio mewn ffordd broffesiynol fel y byddent yn yr ystafell ddosbarth. Dylai athrawon wneud y canlynol.
- Cadw at safonau proffesiynol o ran gwisg pan fyddan nhw o flaen y camera.
- Peidio â chael gwersi un-i-un, sy'n cael eu ffrydio'n fyw, â dysgwyr.
- Bod yn ymwybodol bod sylwadau'n cael eu clywed gan nifer o ddysgwyr mewn amgylchedd ar-lein, ac y byddai'n hawdd camddehongli'r sylwadau.

- Sicrhau eu bod yn dod â'r sesiwn i ben i bawb, gan wneud yn siŵr nad oes dysgwyr yn cael eu gadael ar eu pen eu hunain a heb oruchwyliaeth mewn sesiwn ar ôl i'r athro adael.
- Bod yn ymwybodol o'r angen am gyfrinachedd; yn enwedig os ydych chi'n ffrydio gwers yn fyw o leoliad lle mae oedolion neu blant eraill yn bresennol.

5.8 Recordio sesiynau ffrydio byw

Mae cyfleuster recordio ar gael yn Microsoft Teams a Google Meet. **Mae'n rhaid recordio pob sesiwn dysgu byw.**

Gan fod recordiad ffrydio byw yn gyfystyr â data personol, rhaid i chi gydymffurfio â pholisïau diogelu data eich ysgol a rheoliadau GDPR.

5.9 Ymddygiad y dysgwyr

Wrth weithio gyda phlant a phobl ifanc, dylech ddweud yn glir ar ddechrau pob sesiwn beth sy'n ddisgwyliedig a pha ymddygiad sy'n dderbyniol.

Dylai ymarferwyr addysg wneud y canlynol.

- Cyfleu'n glir y disgwylir ymddygiad 'o safon ystafell ddosbarth' gan bawb sy'n bresennol.
- Gosod y disgwyliadau o'r cychwyn.
- Creu a chytuno ar reolau sylfaenol clir ac ar safonau ymddygiad, sy'n seiliedig ar bolisi rheoli ymddygiad presennol yr ysgol.
- Egluro'r rheolau wrth gyflwyno'r wers, e.e. pwy sy'n cael siarad, sut mae gofyn cwestiwn neu ofyn am help. Os dyma'r tro cyntaf i wersi gael eu cynnal ar-lein, efallai y bydd yn cymryd ychydig o amser i ymgyfarwyddo â'r amgylchedd newydd. Wrth ddefnyddio'r swyddogaeth sgwrsio, bydd modd ymgysylltu mewn ffordd strwythuredig â'r rheini sy'n bresennol.
- Parhau i atgoffa'r dysgwyr am y rheolau a gytunwyd ar ddechrau pob gwers (Atodiad 2), ac egluro sut gallan nhw fynegi pryderon os oes angen.

6. Rheoli hidlo

- Os yw staff neu ddisgyblion yn dod ar draws deunyddiau anaddas ar-lein, rhaid adrodd am y safle i'r Cydlynydd e-Ddiogelwch.
- Bydd uwch staff yn sicrhau y cynhelir gwiriadau rheolaidd er mwyn sicrhau bod y dulliau hidlo a ddewisir yn addas, yn effeithiol ac yn rhesymol.

7. Rheoli technoleg ddatblygol
- Caiff technoleg ddatblygol ei hastudio am fanteision addysgu a gwneir asesiad risg cyn bod yr ysgol yn cael ei defnyddio.
- Dylai'r uwch dîm rheoli nodi y gall technoleg megis ffonau symudol â mynediad diwifr i'r rhyngrwyd fod y tu hwnt i systemau hidlo'r ysgol a gallant gyflwyno llwybr arall i ddeunyddiau a chyfathrebu annymunol a pheryglus.
- Ni chaiff ffonau symudol eu defnyddio yn ystod gwersi neu amser ysgol ffurfiol. Mae anfon negeseuon testun neu ffeiliau ymosodol neu anaddas drwy Bluetooth neu unrhyw ffordd arall wedi'i wahardd.

8. Penderfyniadau'r Polisi

8.1 Awdurdodi Mynediad i'r Rhyngrwyd
- Bydd yr ysgol yn cynnal cofnod diweddar o'r holl staff a disgyblion sy'n cael mynediad i systemau TGCh yr ysgol.

- Caniateir mynediad i'r rhyngrwyd yn unig wrth i oedolyn arddangos gyda goruchwyliaeth uniongyrchol wrth edrych ar ddeunyddiau ar-lein penodol a gymeradwywyd.
- Bydd gofyn i rieni lofnodi a dychwelyd ffurflen ganiatâd.
- Bydd gofyn i unrhyw un na chaiff ei gyflogi gan yr ysgol lofnodi dogfen defnydd derbyniol o adnoddau TGCh yr ysgol cyn cael mynediad i'r rhyngrwyd o safle'r ysgol.

8.2   Asesu risgiau
- Bydd yr ysgol yn cymryd yr holl ragofalon rhesymol i atal mynediad i ddeunyddiau anaddas. Fodd bynnag, oherwydd y raddfa ryngwladol a natur gysylltiedig cynnwys y rhyngrwyd, nid yw'n bosib gwarantu na fydd deunyddiau anaddas yn ymddangos ar gyfrifiadur sydd wedi'i gysylltu â rhwydwaith yr ysgol. Ni all yr ysgol dderbyn atebolrwydd dros unrhyw ddeunyddiau y deuir o hyd iddynt nag unrhyw ganlyniad cael mynediad i'r rhyngrwyd.
- Dylai'r ysgol archwilio TGCh i bennu a yw'r polisi e-ddiogelwch yn foddhaol a bod y polisi e-ddiogelwch yn cael ei roi ar waith mewn modd priodol ac effeithiol.

8.3   Cyfrifoldebau Staff
- Y mae aelod o staff sy'n mynd yn groes i gyngor ar ddiogelwch neu'n defnyddio e-bost neu'r rhyngrwyd at ddibenion amhriodol, yn agored i gael ei ddisgyblu.
- Mae staff sy'n rheoli'r systemau hidlo neu'n monitro'r defnydd a wneir o TGCh yn ysgwyddo cryn gyfrifoldeb, a rhaid eu goruchwylio'n briodol. Rhaid i'r gweithdrefnau ddiffinio sut i ddwyn defnydd amhriodol neu ddefnydd anghyfreithlon o'r TGCh i sylw'r uwch reolwyr.
- Rhaid i'r staff fod yn ymwybodol o'r peryglon iddynt hwy eu hunain wrth reoli'r defnydd a wneir o TGCh, megis edrych ar ddelweddau amhriodol i ymchwilio eu tarddiad, a sicrhau bod mesurau diogelwch priodol yn eu lle i ddiogelu eu hunain.
- Rhaid dwyn unrhyw honiad o ymddygiad amhriodol i sylw'r uwch reolwyr a dilyn y camau priodol yn dilyn derbyn y gwybodaeth.

8.4   Defnydd cymunedol o'r rhyngrwyd
Bydd yr ysgol yn cysylltu â sefydliadau lleol i bennu ymagwedd gyffredin at e-ddiogelwch.

9.   Mynd i'r afael â chwynion e-ddiogelwch
- Bydd uwch aelod o staff yn mynd i'r afael â chwynion yng nghyswllt camddefnyddio'r rhyngrwyd.
- Dylid cyfeirio unrhyw bryder am gamddefnydd gan staff at y Pennaeth.
- Rhaid delio â chwynion amddiffyn plant yn unol â gweithdrefnau amddiffyn plant yr ysgol.
- Caiff disgyblion a rhieni wybod am y weithdrefn gwyno.
- Bydd disgyblion a rhieni'n cael gwybod beth fydd yn digwydd i ddisgyblion sy'n camddefnyddio'r rhyngrwyd.
- Cynhelir trafodaethau â'r Swyddog Heddlu Cymunedol i bennu gweithdrefnau ar gyfer mynd i'r afael â materion anghyfreithlon posib.

9.1   Sut rydym yn ymateb?
Gall y Person Dynodedig Amddiffyn Plant ddarparu arweiniad os ydych yn pryderu am sut y mae plentyn, person ifanc neu aelod o staff yn defnyddio'r rhyngrwyd.

9.2   Ymateb i Achos o Bryder
- Mae technolegau'r rhyngrwyd a chyfathrebu electronig yn rhoi cyfle i blant a phobl ifanc ehangu eu profiadau dysgu a datblygu'u gallu i fod yn greadigol yn yr ysgol a thu allan i'r ysgol. Serch hynny, mae'n bwysig cofio yn ogystal y peryglon sy'n gysylltiedig â'r modd y gellir defnyddio'r technolegau hyn.

- Dylai cydnabod a cheisio datblygu'r sgiliau sydd eu hangen ar blant a phobl ifainc wrth gyfathrebu a defnyddio'r technolegau hyn yn briodol, tra'n cadw'n ddiogel, a dangos parch tuag at eraill.
- Mae'r risgiau hyn i e-ddiogelwch yn codi oherwydd bod pobl yn gweithredu'n amhriodol neu hyd yn oed yn anghyfreithlon. Rhaid delio ag unrhyw fater a all godi ar lefel bersonol.
- Athrawon yw llinell flaen yr amddiffyn; hwy sy'n arsylwi ymddygiad y disgyblion ac y mae hynny'n hanfodol o ran canfod perygl i ddisgyblion ac o ran datblygu ymddiriedaeth fel bod materion yn derbyn sylw. Bydd digwyddiadau yn amrywio o'r drygioni neu weithred ddifeddwl i weithred anghyfreithlon a gynlluniwyd yn ofalus.
- Bydd yr adran hon yn gymorth i'r staff benderfynu pa gamau i'w cymryd a pha bryd i roi gwybod am ddigwyddiad sy'n peri pryder i'r person sydd â chyfrifoldeb am Ddiogelu Plant neu e-Ddiogelwch o fewn yr ysgol. Yn dilyn ymgynghori â'r person dynodedig amddiffyn plant gellir cyfeirio materion wedyn at Swyddog yr Awdurdod ar Ddiogelu Plant neu at yr Heddlu os bernir bod angen hynny.

10. Cyfathrebu

10.1 Cyflwyno'r polisi e-ddiogelwch i ddisgyblion
- Bydd rheolau e-ddiogelwch i'w gweld ym mhob ystafell lle defnyddir cyfrifiaduron a bydd trafodaethau rheolaidd â disgyblion.
- Caiff disgyblion wybod y bydd defnydd o'r rhwydwaith a'r rhyngrwyd yn cael ei fonitro mewn modd addas.
- Caiff rhaglen o hyfforddiant e-ddysgu ei ddatblygu.
- Caiff hyfforddiant e-ddiogelwch ei gynnwys yn y cynllun gwaith TGCh a/neu'r cwricwlwm Addysg Bersonol a Chymdeithasol (ABCh).

10.2 Staff a'r polisi e-ddiogelwch
- Bydd pob aelod o staff yn derbyn Polisi e-Ddiogelwch yr Ysgol a chaiff pwysigrwydd y polisi ei esbonio wrthynt.
- Rhaid i staff fod yn ymwybodol y gellir monitro ac olrhain y rhwydwaith a thraffig y rhyngrwyd i'r defnyddiwr unigol.
- Caiff aelodau staff sy'n rheoli'r systemau hidlo neu fonitro defnydd TGCh eu goruchwylio gan yr uwch dîm rheoli gan weithio i weithdrefnau clir ar gyfer cofnodi materion.
- Bydd staff yn defnyddio peiriant chwilio sy'n ddiogel i blant pob amser wrth fynd ar y rhyngrwyd gyda disgyblion.

10.3 Cyflwyno'r Polisi i rieni a gofalwyr
- Tynnir sylw rhieni a gofalwyr at Bolisi e-Ddiogelwch yr Ysgol mewn cylchlythyron, llawlyfr yr ysgol ac ar wefan yr ysgol.
- Bydd yr ysgol yn rheadru rhestr o adnoddau e-ddiogelwch i rieni/gofalwyr.
- Bydd yr ysgol yn gofyn i bob rhiant newydd lofnodi'r cytundeb rhieni/disgyblion wrth gofrestru'r plant yn yr ysgol.

Atodiad 1: Defnyddio'r rhyngrwyd - Gweithgareddau dysgu ac addysgu posib

Gweithgareddau	Materion e-ddiogelwch allweddol
Creu cyfeiriaduron gwe i ddarparu mynediad cyfleus i wefannau addas.	Dylid cael caniatâd rhieni. Dylid goruchwylio disgyblion. Dylid cyfeirio disgyblion at ddeunyddiau penodol, cymeradwy ar-lein.
Defnyddio peiriannau chwilio i gael gwybodaeth amrywiaeth o wefannau.	Rhaid bod y system hidlo'n actif ac yn cael ei gwirio'n aml. Dylid cael caniatâd rhieni. Dylai disgyblion gael eu goruchwylio. Dylai disgyblion ddysgu pa ddefnydd o'r rhyngrwyd sy'n dderbyniol a'r hyn y dylent wneud os ydynt yn dod ar draws deunydd nad ydynt yn gyfforddus ag ef.
Cyfnewid gwybodaeth â disgyblion eraill a gofyn cwestiynau i arbenigwyr trwy e-bost neu flogiau.	Dylai disgyblion ddefnyddio cyfrifon e-bost neu flogiau cymeradwy. Ni ddylai disgyblion fyth gyflwyno gwybodaeth bersonol. Ystyried defnyddio systemau sy'n darparu cymedroli ar-lein e.e. SuperClubs Plus.
Cyhoeddi gwaith disgyblion ar wefan yr ysgol neu ar wefannau eraill.	Dylid cael caniatâd disgyblion a rhieni cyn cyhoeddi unrhyw beth. Dylid hepgor enwau llawn disgyblion a gwybodaeth bersonol arall. Dylai gwaith disgyblion gael ei gyhoeddi ar 'safleoedd a gymedrolir' yn unig.
Cyhoeddi delweddau gan gynnwys ffotograffau o'r disgyblion.	Dylid cael caniatâd rhieni i gyhoeddi ffotograffau. Ni ddylai disgyblion fedru cael eu hadnabod io'r ffotograffau. Ni ddylai enwau ffeiliau gyfeirio at y disgyblion wrth eu henwau. Rhaid i'r staff sicrhau nad yw delweddau a gyhoeddir yn torri cyfreithiau hawlfraint.
Cyfathrebu syniadau mewn ystafelloedd sgwrsio neu fforymau ar-lein.	Dim ond ystafelloedd sgwrsio sy'n benodol at ddefnydd addysgol ac sydd wedi'u cymedroli y dylid eu defnyddio. Dylid atal mynediad i safleoedd rhwydweithio cymdeithasol eraill. Ni ddylai disgyblion fyth gyflwyno gwybodaeth bersonol.
Fideo-gynadledda a chynadledda clywedol i gasglu a rhannu gwaith disgyblion.	Dylid goruchwylio disgyblion. Dylai ysgolion ddefnyddio rhaglenni a reolir gan Awdurdodau Lleol a Chyflenwyr Addysgol cymeradwy yn unig.

Atodiad 2: Adnoddau defnyddiol i athrawon a rhieni

Canolfan Camfanteisio ar Blant a'u Hamddiffyn Ar-lein (CEOP
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen
www.digizen.org/
Kidsmart
www.kidsmart.org.uk/
Think U Know
www.thinkuknow.co.uk/
South West Grid for Learning
http://swgfl.org.uk/
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Internet Safety Zone
www.internetsafetyzone.com
School Beat
https://www.schoolbeat.org/cy/
Parth e-ddiogelwch HWB
http://hwb.wales.gov.uk/esafety-index

1.   Introduction

1.1   The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and child protection.

1.2   Our e-Safety Policy has been agreed by senior management and approved by the governors.

2.   Learning and teaching

2.1   The Internet and digital communications are important because:
- The Internet is a vital element in 21st century life for education, business and social interaction.
- The school has a duty to deliver good quality access to the internet as part of their learning experience of Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

2.2   Internet use will benefit education because it:
- Gives access to educational resources from around the world
- Enables collaboration across support services and professional associations
- The exchange of curriculum and administration data with the Local Authority and the Welsh Assembly Government

2.3   Internet use will improve pupils' learning because:
- The internet access at the school is designed specifically for pupil's use and will include filtering appropriate to the age of pupils
- The pupils are learning from what Internet use is acceptable and what is unacceptable and given clear objectives for using internet
- Pupils will be taught to use the Internet effectively in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be taught how to publish and present information to a wider audience.

2.4   Pupils will learn how to evaluate Internet content:
- To ensure that school of materials used by Internet staff and pupils complies with copyright law
- For pupils from learning about the importance of checking information before accept that it is correct
- For pupils to learn how to report any objectionable content e.g. how to use the CEOP Report Abuse icon

3.   Management Information Systems

3.1   Safety information systems
- School ICT systems are reviewed regularly
- The system of protection against viruses is regularly updated and security strategies discussed with the Local Authority

3.2   Email
- Pupils can use approved e-mail accounts on the school system
- Pupils must tell a teacher / teacher immediately if they receive offensive e-mail
- In relation to communications via email, pupils must not reveal their personal details or any other details, or arrange to meet anyone without specific permission
- Sending chain letters are not allowed
- Be suspicious of incoming emails and do not open until identifying who the author is
- Schools should consider how emails from pupils to external bodies are monitored

3.3 Published content and the school website
- Contact information for staff or pupils will not be published
- On-line contact details should be kept in the school office
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing pupil's images and work
- Photographs that include pupils will be carefully selected in order to ensure that individuals cannot be identified and images cannot be misused. can not be identified or their image misused.
- We will consider using group photographs rather than photos of individual photos of children.
- Pupils' full names will not be used anywhere on the school's website or any other website, especially with photographs.
- Permission must be sought from parents or carers before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil and parents / carers.
- Children's full names will not be used on the website, especially with photographs.
- Parents should understand the school's photographing and publishing policy, how they are stored at school and on independent electronic equipment.

3.5 Protection of personal data
- Personal data is recorded, processed, transferred and made available in accordance with the Data Protection Act 1998.

4. What does electronic communication include?

- Internet collaboration tools: social networking sites and web logs (blogs)
- Internet research: websites, search engines and web browsers
- Mobile phones and tablets, computers with internet communications: e-mail and instant messaging
- Webcams and videoconferencing
- Wireless games consoles

4.1 Social networking and personal publishing

- Social Network sites and newsgroups will be filtered unless specific use is approved
- Pupils will be advised not to introduce any sort of details that could mean someone can identify them, their friends or their location
- Ideally, pupils would use only moderated social networking sites, eg SuperClubs Plus
- Students and parents will be advised that the use of social network spaces outside school a range of dangers for pupils
- Pupils will be advised to use nicknames and avatars in the use of social networking sites

5.
In exceptional circumstances it may be necessary to use live streaming technology. This technology allows a member of staff to teach a group of pupils without being in the same place as them. The teacher and pupils can be in their homes e.g.

5.1 Safeguarding learners and their wellbeing is paramount, both take precedence over all other considerations when planning live streaming lessons.

- Always follow your school's safeguarding policies. All online security issues should be dealt with in the same way as you would for an face-to-face learning issue.
- If you have any safeguarding concerns about a child, you should discuss them with the Designated Person responsible for Child Protection.

5.2 Before streaming live lessons the purpose, benefits and limitations of a live streaming lesson should be considered:
- Consideration should be given to whether another method is more suitable, e.g. if the teacher intends to show how to do something, a video may be more appropriate.
- Think about which learners will be available, e.g. will all learners be available at the same time, will some need to join or leave at different times? It is recommended to consider the number of learners on a session

5.3 Make sure that the length of live-streamed lessons is suitable for your learners.

5.4 The lesson should be planned in advance, and learners and parents / carers should be given sufficient notice. This will also contribute to how safe the session will be.

- Ensure all content is appropriate, and for any tasks that involve researching online, make sure the websites are suitable before the lesson.

- All learners should have access to necessary software programs.

- If the lesson involves tasks, remember that some learners may need more time.

5.5 Permission should be obtained from the senior management team to stream live lessons informing them of the timetable for each lesson. A live streaming lesson should not be run without the knowledge of the senior management team.

5.6 It should be ensured that appropriate usage agreements are in place for all learners involved in a live-streamed lesson. The agreement will set out the clear expectations of all parties, and set out the steps that will be taken if the agreement is not complied with.

5.7 Professional conduct

Any live streaming work should take place on a voluntary basis, and education practitioners who choose live streaming should continue to work in a professional manner as they would in the classroom. Teachers should do the following:

- Adhere to professional standards of dress when in front of the camera.
- Not have one-to-one live-streamed lessons with learners.
- Be aware that comments are being heard by many learners in an online environment, and that it would be easy to misinterpret comments.
- Make sure they end the session for everyone, making sure learners are not left alone and unsupervised in a session after the teacher has left.
- Be aware of the need for confidentiality; especially if you are streaming a lesson live from a location where other adults or children are present.

5.8 Recording live streaming sessions

A recording facility is available on Microsoft Teams and Google Meet. **All live learning sessions must be recorded.**

Because live streaming recording is synonymous with personal data, you must comply with your school's data protection policies and GDPR regulations

5.9   Learners' behaviour

When working with children and young people, you should make clear at the beginning of each session what is expected and what behaviour is acceptable.

Education practitioners should do the following:

- Make it clear that 'classroom standard' behaviour is expected of all present.
- Set expectations from the start.
- Create and agree clear ground rules and standards of behaviour, based on the school's current behaviour management policy.
- Explain the rules when presenting the lesson, e.g. who can speak, how to ask a question or ask for help. If this is the first time that lessons have been held online, it may take a while to get used to the new environment. By using the chat function, it will be possible to engage in a structured way with those present.
- Continue to remind learners of the rules agreed at the start of each lesson (Appendix 2), and explain how they can raise concerns if necessary.

6.   Management filter

- If staff or pupils come across unsuitable material online, the site must be reported to the eSafety coordinator
- Senior staff will ensure that regular checks are completed in order to ensure that the filtering methods selected are appropriate, effective and reasonable

7.   Managing emerging technologies
- Emerging technologies will be of educational benefit and they are examined for risk assessment before being used at the school
- The senior management team should note that technologies such as mobile phones that access wireless internet may go beyond the school's filtering systems and can present a new route to undesirable material and communications that may be dangerous
- Mobile phones may not be used during lessons or formal school time
- Texting an offensive or inappropriate files via Bluetooth or any other way is prohibited.

8.   Policy Decisions

8.1   Internet Access Authorization
- The school will maintain a record all staff and pupils who are granted access to the school's IT systems
- Internet access is permitted only by adult demonstration with direct supervision and by looking at specific online materials that are approved
- Parents will be required to sign and return a consent form
- Any person that is not employed by the school will be required to sign acceptable use of the school's IT policy before accessing the internet from the school site

8.2   Assessing risks
- The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and internet content, it is not possible to guarantee that unsuitable material will not appear on the computer connected to the school network

- The school can not accept liability for any materials found on any computer or any consequences of internet access
- The school should audit IT use to establish whether the e-safety policy is adequate and that the e-safety policy is being implemented in an appropriate and effective manner

8.3 Staff Responsibilities
- Any member of staff that does not comply with the school's policy and uses email or the Internet for inappropriate use is liable to be disciplined
- Staff who manage filtering systems or monitor the use of IT have a great responsibility, and must be properly supervised. The procedures define how to bring improper use or illegal use of IT to the attention of senior management.
- Staff must be aware of the risks to themselves in managing the use of IT, such as viewing inappropriate images to investigate their origin, and to ensure that appropriate security measures are in place to protect themselves
- Any allegation of inappropriate behavior must be brough to the attention of senior management and appropriate steps followed following receiving such information.

8.4 Community use of the internet
The school will liaise with local organizations to establish a common approach to e-safety.

9. Tackling e-safety complaints

- Senior staff will address complaints in relation to Internet misuse
- Any concerns regarding staff should be directed to the Head
- Child protection complaints will be dealt with in accordance with the school's child protection procedures
- Pupils and parents are aware of the complaints procedure
- Pupils and parents will be told what will happen to pupils misusing the Internet
- Discussions will be held with a Community Police Officer to establish procedures for tackling potentially illegal issues.

9.1 How do we respond?
The Designated Person Child Protection can provide guidance if you are concerned about how the child, young person or staff member's use of the Internet.

9.2 Response to an Incident of Concern

- Internet technologies and electronic communications provide an opportunity for children and young people to broaden their learning experiences and develop the ability to be creative at school and outside school. Nevertheless, it is important to remember the risks associated with using such technologies.
- Recognise and seek to develop skills needed for children and young people in communicating and using these technologies appropriately, whilst keeping them safe, and show respect for others.
- The risks of e-safety are caused by people acting inappropriately or even illegally
- We need to deal with any issues that may arise on a personal level.
- Teachers are the front line of defense; their observation of behavior of pupils is crucial in detecting dangers to pupils and in developing trust so that issues are addressed
- Events will range from mischief or unconsidered action to illegal incidents that are carefully planned

- This section will help staff to determine what action to take and when to report an incident of concern to the person with responsibility for Child Protection or e-Safety within the school
- Following consultation with the designated child protection person, issues can then be referred to the Authority's Child Safeguarding Officer or to the Police if deemed necessary

10. Communication Policy

10.1 Introducing the e-safety policy to pupils
- E-safety rules will be posted in all rooms where computers are used and discussed with pupils regularly
- Pupils will know that the use of the network and Internet will be monitored in an appropriate manner
- An E-learning training program will be developed
- E-safety training will be included in the work plan of IT and / or curriculum PSE (PSE).

10.2 Staff and the e-safety policy
- All staff will receive the School e-Safety Policy and the importance of the policy will be explained
- Staff must be aware that it can monitor and track the network and Internet traffic to the individual user
- Staff that manage filtering systems or monitor IT use will be supervised by the senior management team working with procedures for reporting issues
- Staff will use a search engine that is safe for children at all times when on the internet with pupils

10.3 Introducing Policy to parents and carers
- Parents and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website
- The school will cascade a list of e-safety resources for parents / carers
- The school will ask parents to sign the parent / pupil agreement when registering children at school

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety matters
Web directories created to provide access to suitable websites.	There should be parental consent. Pupils should be supervised. Pupils should be referred to specific materials that have been approved on-line.
Use search engines to gain information for numerous sites.	The filtration system must be active and be checked frequently. There should be parental consent. Pupils should be supervised. Pupils should learn what Internet use is acceptable and what they should do if they encounter material they are uncomfortable with.
Exchange information with other pupils and ask bloggers and experts questions (via email).	Pupils should use e-mail accounts or blogs approved. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.
Pupils work published on the school website or on other websites	Parental and pupil's consent should be sought prior to publishing any material. Pupil's full names and any other personal details should be removed. Pupil's work should only be published on 'moderated sites' only.
Pupils work published on the school website or on other websites	Parents consent should be sought prior to publishing photographs. Pupils should not be able to be identified from photographs. File names should not refer to the pupils by name. Staff must ensure that the images published is not breaking any copyright laws.
Communicating ideas in chat rooms or online forums	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites will be prevented. Pupils should never give out personal information.
Audio conferencing and video conferencing to gather and share pupils' work.	Pupils should be supervised. Schools should use the programs managed by local authorities and approved Educational Suppliers only.

Appendix 2: Useful resources for teachers and parents

Canolfan Camfanteisio ar Blant a'u Hmddiffyn Ar-lein (CEOP)
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen
www.digizen.org/
Kidsmart
www.kidsmart.org.uk/
Think U Know
www.thinkuknow.co.uk/
South West Grid for Learning
http://swgfl.org.uk/
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Internet Safety Zone
www.internetsafetyzone.com
School Beat
https://www.schoolbeat.org/cy/
Parth e-ddiogelwch HWB
http://hwb.wales.gov.uk/esafety-index