Cynnwys

YSGOL GYMUNEDOL PENIEL

Mae'r Polisi Diogelwch Ar-lein hwn yn amlinellu ymrwymiad Ysgol Gymunedol Peniel i ddiogelu aelodau o gymuned ein hysgol ar-lein yn unol ag egwyddorion llywodraeth agored a'r gyfraith. Dylai ysgolion fod yn ymwybodol o'r fframwaith deddfwriaeth a gafodd ei defnyddio i gynhyrchu'r templed Polisi Diogelwch Ar-lein a'r canllaw hwn fel yr amlinellir yn yr Atodiad 'Deddfwriaeth'.

Mae'r Polisi Diogelwch Ar-lein hwn yn berthnasol i holl aelodau cymuned yr ysgol (gan gynnwys staff, dysgwyr, gwirfoddolwyr, rhieni a gofalwyr, ymwelwyr, a defnyddwyr cymunedol) sydd â mynediad at systemau digidol y tu mewn a'r tu allan i'r ysgol ac sy'n eu defnyddio. Mae hefyd yn berthnasol i'r defnydd o dechnoleg ddigidol bersonol ar safle'r ysgol (pan ganiateir hynny).

Bydd Ysgol Gymunedol Peniel yn delio â digwyddiadau o'r fath yn y polisi hwn a pholisïau ymddygiad a gwrth-fwlio cysylltiedig a, lle bo'n hysbys, bydd yn rhoi gwybod i rieni/gofalwyr am ddigwyddiadau o ymddygiad diogelwch ar-lein amhriodol sy'n digwydd y tu allan i'r ysgol.

Datblygu, monitro ac adolygu polisïau

Mae'r Polisi Diogelwch Ar-lein hwn wedi cael ei ddatblygu gan:

- *pennaeth/uwch arweinwyr*
- *arweinydd diogelwch ar-lein*
- *staff - gan gynnwys athrawon/ymarferwyr addysg/staff cymorth/staff technegol*
- *llywodraethwyr*

Ymgynghorwyd â chymuned yr ysgol gyfan mewn amrywiaeth o gyfarfodydd ffurfiol ac anffurfiol.

Amserlen ar gyfer datblygu, monitro ac adolyglu

Cymeradwywyd y Polisi Diogelwch Ar-lein hwn gan *gorff llywodraethu'r ysgol* ar:	***Hydref 2023***
Bydd y canlynol yn monitro sut bydd y Polisi Diogelwch Ar-lein hwn yn cael ei roi ar waith:	**Elen H Powell (Pennaeth)** **Mathew James (Llywodraethwr)**
Bydd monitro yn digwydd yn rheolaidd:	**Yn nhymor yr Hydref**
Bydd y *corff llywodraethu* yn derbyn adroddiad gan y grŵp monitro ar weithredu'r Polisi Diogelwch Ar-lein (bydd yn cynnwys manylion dienw am achosion diogelwch ar-lein) yn rheolaidd:	**Yn nhymor yr Hydref**

Bydd y Polisi Diogelwch Ar-lein yn cael ei adolygu'n flynyddol, neu'n amlach yng ngoleuni datblygiadau newydd arwyddocaol o ran defnyddio technolegau, bygythiadau newydd i ddiogelwch ar-lein neu unrhyw achosion sydd wedi codi. Rhagwelir y bydd y dyddiad adolygu nesaf ar:	**Hydref 2024**
Os bydd yna achosion diogelwch ar-lein difrifol, dylid hysbysu'r personau / asiantaethau allanol hyn:	***Elen H Powell (Pennaeth a Pherson Dynodedig Diogelu)*** ***Dion Thomas (Is berson Dynodedig Diogelu)*** ***Wyn Evnas (Llywodraethwyr a chyfrifoldeb dros Ddiogelu)*** ***Bydd yr ysgol yn cysylltu â'r awdurdod a PC Cath Williams.***

Proses ar gyfer monitro effaith y Polisi Diogelwch Ar-lein

Bydd yr ysgol yn monitro effaith y polisi drwy wneud y canlynol:

- cofnodion o ddigwyddiadau y rhoddwyd gwybod amdanynt
- data mewnol yn monitro gweithgarwch ar y rhwydwaith
- arolygon/holiaduron ar gyfer:
    - dysgwyr
    - rhieni a gofalwyr
    - staff.

Polisi ac arweinyddiaeth

Cyfrifoldebau

Er mwyn sicrhau bod aelodau o gymuned ein hysgol yn cael eu diogelu ar-lein, mae'n bwysig bod pob aelod o'r gymuned honno'n gweithio gyda'i gilydd i ddatblygu ymddygiad ar-lein diogel a chyfrifol, gan ddysgu oddi wrth ei gilydd ac o arferion da mewn mannau eraill, gan roi gwybod am ymddygiadau, pryderon a chamddefnydd amhriodol ar-lein cyn gynted ag y daw'r rhain i'r amlwg. Er mai ymdrech tîm fydd hon, mae'r adrannau canlynol yn amlinellu rolau a chyfrifoldebau diogelwch ar-lein unigolion a grwpiau yn yr ysgol.

Penaethiaid ac uwch arweinwyr

- Dyletswydd y pennaeth yw sicrhau diogelwch (gan gynnwys diogelwch ar-lein) holl aelodau cymuned yr ysgol a meithrin diwylliant o ddiogelu. Y Pennaeth hefyd yw'r Arweinydd Diogelwch Ar-lein.

- Mae'r Pennaeth Cynorthwyol sy'n aelod o'r uwch dîm arwain yn ymwybodol o'r gweithdrefnau sydd angen eu dilyn mewn achos o gyhuddiad difrifol yn ymwneud â diogelwch ar-lein yn erbyn aelod o staff.[1]
- Mae'r pennaeth/uwch arweinwyr yn gyfrifol am sicrhau bod staff yn cyflawni eu cyfrifoldebau'n effeithiol.
- Bydd yr Uwch dîm yn sicrhau bod system yn ei lle i allu monitro a rhoi cymorth i'r rhai sy'n monitro diogelwch ar-lein mewnol yr ysgol.
- Bydd y pennaeth sy'n Arweinydd Diogelwch Ar-lein yn darpari adroddiadau monitro.

Llywodraethwyr

Y llywodraethwyr sy'n gyfrifol am gymeradwyo'r Polisi Diogelwch Ar-lein ac am adolygu effeithiolrwydd y polisi e.e. drwy ofyn y cwestiynau yn nogfen Llywodraeth Cymru a UKCIS Pump o gwestiynau allweddol i gyrff llywodraethu i helpu i herio eu hysgol i ddiogelu eu dysgwyr yn effeithiol. Gwneir hyn gan y Pwyllgor llawn. Bydd yr aelodau hyn yn derbyn gwybodaeth reolaidd ynglŷn â digwyddiadau diogelwch ar-lein ac adroddiadau monitro. Dylai aelod o'r corff llywodraethu ymgymryd â rôl y Llywodraethwr Diogelwch Ar-lein[2] a chyflawni'r canlynol:

- **cyfarfod yn rheolaidd gyda'r Arweinydd Diogelwch Ar-lein**
- **derbyn adroddiadau'n rheolaidd (wedi'u creu a'u gwneud yn ddienw) am ddigwyddiadau diogelwch ar-lein**
- **gwirio bod y ddarpariaeth a amlinellir yn y Polisi Diogelwch Ar-lein (e.e. darpariaeth addysg diogelwch ar-lein a hyfforddiant staff yn digwydd yn ôl y bwriad)**
- **adrodd i'r grŵp llywodraethwyr / cyfarfod perthnasol.**

Bydd y corff llywodraethu hefyd yn cefnogi'r ysgol i annog rhieni/gofalwyr a'r gymuned ehangach i gymryd rhan mewn gweithgareddau diogelwch ar-lein.

Arweinydd Diogelwch Ar-lein

Y Pennaeth yw'r arweinydd diogelwch ar lein a'r Person Diogelu Dynodedig. .

Rôl:

- arwain y Grŵp Diogelwch Ar-lein
- cymryd cyfrifoldeb o ddydd i ddydd dros faterion diogelwch ar-lein, bod yn ymwybodol o'r posibilrwydd o bryderon difrifol ynghylch amddiffyn plant
- chwarae rhan flaenllaw yn y gwaith o sefydlu ac adolygu polisïau/dogfennau diogelwch ar-lein yr ysgol
- hyrwyddo ymwybyddiaeth o addysg diogelwch ar-lein ar draws yr ysgol a thu hwnt, ac ymrwymiad i hynny

---

[1] Gweler y siart llif am ymdrin â digwyddiadau diogelwch ar-lein yn 'Ymateb i achosion o gamddefnyddio' a gweithdrefnau disgyblu Adnoddau Dynol/corff perthnasol arall.

[2] Awgrymir cyfuno'r rôl hon â rôl y llywodraethwr dynodedig ar gyfer diogelu. Mewn sefyllfaoedd eraill, efallai mai'r person hwn yw'r pwyllgor rheoli ar gyfer amddiffyn plant

- cysylltu ag arweinwyr y cwricwlwm i sicrhau bod y cwricwlwm diogelwch ar-lein yn cael ei gynllunio a'i ymgorffori
- sicrhau bod yr holl staff yn ymwybodol o'r gweithdrefnau y dylid eu dilyn mewn achosion o ddigwyddiadau diogelwch ar-lein a bod angen rhoi gwybod ar unwaith am y digwyddiadau hynny
- derbyn adroddiadau ar ddigwyddiadau diogelwch ar-lein[3] a chreu cofnod o ddigwyddiadau er mwyn eu defnyddio i ddatblygu diogelwch ar-lein yn y dyfodol
- rhoi hyfforddiant a chyngor i staff/llywodraethwyr/rhieni/gofalwyr/dysgwyr (neu ganfod ffynonellau priodol o hynny)
- cysylltu â staff technegol (ysgol/awdurdod lleol), staff bugeiliol a staff cefnogi (fel sy'n berthnasol)
- cyfarfod yn rheolaidd gyda'r llywodraethwr diogelwch ar-lein i drafod materion cyfredol, adolygu digwyddiadau (yn ddienw) a hidlo a monitro cofnodion os yw hynny'n bosibl
- mynychu cyfarfodydd/grwpiau perthnasol y corff llywodraethu
- cysylltu â'r awdurdod lleol/corff perthnasol

Person Diogelu Dynodedig

Mae'n bwysig pwysleisio mai materion diogelu ac nid materion technegol yw'r rhain; mae technoleg yn cynnig dulliau ychwanegol o ddatblygu materion diogelu..

Dylai'r Person Diogelu Dynodedig gael hyfforddiant ar faterion diogelwch ar-lein a bod yn ymwybodol o'r materion diogelu difrifol sy'n gallu codi o'r canlynol:

- rhannu data personol [4]
- mynediad i ddeunydd anghyfreithlon/amhriodol
- cyswllt amhriodol ar-lein gydag oedolion/dieithriaid
- digwyddiadau neu bosibiliadau o feithrin perthynas at bwrpas rhyw (*grooming*)
- bwlio ar-lein.

Arweinwyr Cwricwlwm

Bydd Arweinwyr y Cwricwlwm yn cyd-weithio gyda'r arweinydd diogelwch ar-lein i ddatblygu rhaglen addysg diogelwch ar-lein wedi'i chynllunio a'i chydlynu. Bydd hyn yn cael ei ddarparu drwy:

- rhaglen ar wahân
- y Fframwaith Cymhwysedd Digidol
- addysg bersonol a chymdeithasol/addysg rhyw a pherthnasoedd
- gwasanaethau

[3] Bydd angen i'r ysgol benderfynu sut byddant yn ymateb i'r digwyddiadau hyn ac a yw'r ymchwiliad/gweithred yn gyfrifoldeb yr arweinydd diogelwch ar-lein neu aelod arall o staff e.e. pennaeth/uwch arweinydd/Uwch Berson Dynodedig/athro dosbarth/pennaeth blwyddyn, ac ati.

[4] Gweler y 'Polisi data personol' yn yr Atodiad.

- drwy fentrau a chyfleoedd cenedlaethol perthnasol *e.e.* Diwrnod Defnyddio'r Rhyngrwyd yn Fwy Diogel ac Wythnos Gwrth-fwlio.

Staff dysgu a chymorth

Mae staff yr ysgol yn gyfrifol am sicrhau'r canlynol:

- ymwybyddiaeth gyfredol o faterion/tueddiadau diogelwch ar-lein ac o bolisi ac arferion Diogelwch Ar-lein cyfredol yr ysgol
- eu bod yn deall bod diogelwch ar-lein yn rhan greiddiol o ddiogelu
- eu bod wedi darllen, deall a llofnodi cytundeb defnydd derbyniol (CDD) y staff
- eu bod yn rhoi gwybod ar unwaith am unrhyw gamddefnydd neu broblem a amheuir i Elen H Powell ar gyfer ymchwiliad/gweithredu, yn unol â gweithdrefnau diogelu'r ysgol
- bod yr holl gyfathrebu digidol â dysgwyr a rhieni/gofalwyr yn cael ei wneud ar lefel broffesiynol *ac wrth ddefnyddio systemau swyddogol yr ysgol yn unig*
- bod materion diogelwch ar-lein yn rhan annatod o bob agwedd o'r cwricwlwm a gweithgareddau eraill
- sicrhau bod dysgwyr yn deall ac yn dilyn y Polisi Diogelwch Ar-lein a'r cytundebau defnydd derbyniol, bod ganddynt ddealltwriaeth dda o sgiliau ymchwil a'r angen i osgoi llên-ladrad a chynnal rheoliadau hawlfraint
- eu bod yn goruchwylio ac yn monitro'r defnydd o dechnolegau digidol, dyfeisiau symudol, camerâu ac ati, mewn gwersi a gweithgareddau eraill yr ysgol (lle maent yn cael eu caniatáu) ac yn gweithredu polisïau cyfredol sy'n ymwneud â'r dyfeisiau hyn
- mewn gwersi lle mae defnyddio'r rhyngrwyd wedi'i gynllunio, dylai dysgwyr gael eu cyfeirio at wefannau sydd wedi'u gwirio fel rhai addas i'w defnyddio, *a bod prosesau yn eu lle i ddelio ag unrhyw ddeunydd anaddas sy'n cael ei ddarganfod wrth chwilio ar y rhyngrwyd*
- pan fydd gwersi'n cael eu cyflwyno drwy ffrydio byw neu fideogynadledda, rhaid i staff roi ystyriaeth lawn i ganllawiau diogelu cenedlaethol a pholisïau diogelu lleol a dylent nodi'r canllawiau sydd yn y polisi Ffrydio Byw.
- mae ganddynt agwedd dim goddefgarwch tuag at ddigwyddiadau o fwlio ar-lein, aflonyddu rhywiol, gwahaniaethu, casineb ac ati
- maent yn modelu ymddygiad ar-lein diogel, cyfrifol a phroffesiynol yn eu defnydd eu hunain o dechnoleg, gan gynnwys y tu allan i'r ysgol ac wrth ddefnyddio'r cyfryngau cymdeithasol.

Dysgwyr:

- Maen nhw'n gyfrifol am ddefnyddio systemau technolegau digidol yr ysgol yn unol â'r cytundeb defnydd derbyniol i ddysgwyr (dylai hyn gynnwys dyfeisiau personol – pan ganiateir hynny)
- Rhaid iddynt ddeall pwysigrwydd adrodd ar gam-drin, camddefnydd neu fynediad i ddeunydd amhriodol, a gwybod sut i wneud hynny
- Gwybod beth i'w wneud os ydyn nhw neu rywun maen nhw'n ei adnabod yn teimlo'n agored i niwed wrth ddefnyddio technoleg ar-lein
- Osgoi llên-ladrad a glynu wrth reoliadau hawlfraint
- Bydd disgwyl iddynt wybod a dilyn Polisi Diogelwch Ar-lein yr ysgol

- Rhaid iddynt ddeall pwysigrwydd dilyn arferion diogelwch ar-lein da wrth ddefnyddio technolegau digidol y tu allan i'r ysgol a sylweddoli bod Polisi Diogelwch Ar-lein yr ysgol yn berthnasol y tu allan i'r ysgol, os yw'n ymwneud â bod yn aelod o'r ysgol.

Rhieni a gofalwyr

Mae gan rieni a gofalwyr ran hanfodol mewn sicrhau bod plant yn deall yr angen i ddefnyddio'r rhyngrwyd/dyfeisiau symudol mewn ffordd briodol.

Bydd yr ysgol yn manteisio ar bob cyfle i helpu rhieni a gofalwyr i ddeall y materion hyn drwy wneud y pethau canlynol:

- darparu copi iddynt o gytundeb defnydd derbyniol y dysgwyr
- cyhoeddi gwybodaeth am ddefnydd priodol o gyfryngau cymdeithasol o ran negeseuon sy'n ymwneud â'r ysgol
- gofyn am eu caniatâd ynghylch delweddau digidol, gwasanaethau cwmwl ac ati

Bydd rhieni a gofalwyr yn cael eu hannog i gefnogi'r ysgol i wneud y canlynol:

- atgyfnerthu'r negeseuon diogelwch ar-lein a roddir i ddysgwyr yn yr ysgol
- defnydd eu plant o'u dyfeisiau personol yn yr ysgol (lle caniateir eu defnyddio)

Defnyddwyr cymunedol

Bydd disgwyl i ddefnyddwyr cymunedol sydd yn cael mynediad i systemau/gwefan/Hwb/platfform dysgu'r ysgol fel rhan o ddarpariaeth ehangach yr ysgol, lofnodi Cytundeb Defnydd Derbyniol defnyddiwr cymunedol cyn cael mynediad i systemau'r ysgol.

Mae'r ysgol yn annog cyfranogiad asiantaethau/aelodau o'r gymuned sy'n gallu cyfrannu'n werthfawr at y ddarpariaeth diogelwch ar-lein ac sy'n mynd ati i rannu ei gwybodaeth a'i harferion da gydag ysgolion eraill a'r gymuned.

Safonau proffesiynol

Disgwylir y bydd safonau proffesiynol cenedlaethol yn cael eu cymhwyso i ddiogelwch ar-lein fel mewn agweddau eraill ar fywyd yr ysgol, hynny yw:

- bod pwyslais cyson ar bwysigrwydd canolog llythrennedd, rhifedd a chymhwysedd digidol. Bydd dysgwyr yn cael eu cefnogi i ennill sgiliau ar draws pob maes dysgu a bydd pob cyfle yn cael ei gymryd i ymestyn sgiliau a chymhwysedd dysgwyr
- bod parodrwydd i ddatblygu a chymhwyso technegau newydd sy'n addas ar gyfer dysgu bwriadol mewn dull strwythuredig ac ystyriol ac i ddysgu o'r profiad.
- mae ymarferwyr yn gallu myfyrio ar eu hymarfer, yn unigol ac ar y cyd, yn erbyn safonau ymarfer effeithiol y cytunwyd arnynt yn genedlaethol a chadarnhau a dathlu eu llwyddiannau
- mae polisïau a phrotocolau ar waith ar gyfer defnyddio technoleg cyfathrebu ar-lein rhwng y staff ac aelodau eraill o'r ysgol a'r gymuned ehangach, gan ddefnyddio mecanweithiau ysgolion sydd wedi'u cymeradwyo'n swyddogol.

Polisi Diogelwch Ar-lein yr ysgol:

- gosod disgwyliadau ar gyfer defnyddio technolegau digidol yn ddiogel ac yn gyfrifol ar gyfer dysgu, gweinyddu a chyfathrebu
- dyrannu cyfrifoldebau ar gyfer cyflawni'r polisi
- yn cael ei adolygu'n rheolaidd ar y cyd, gan ystyried digwyddiadau diogelwch ar-lein a newidiadau/tueddiadau mewn technoleg ac ymddygiad cysylltiedig
- sefydlu canllawiau i staff ar sut y gallant ddefnyddio technolegau digidol yn gyfrifol, diogelu eu hunain a'r ysgol a sut y gallant ddefnyddio'r ddealltwriaeth hon i helpu i ddiogelu dysgwyr yn y byd digidol
- disgrifio sut bydd yr ysgol yn helpu i baratoi dysgwyr i fod yn ddiogel ac yn gyfrifol wrth ddefnyddio technolegau ar-lein
- sefydlu gweithdrefnau clir i ganfod, adrodd, ymateb a chofnodi camddefnydd o dechnolegau digidol a digwyddiadau diogelwch ar-lein, gan gynnwys mecanweithiau cymorth allanol
- yn cael ei ategu gan gyfres o gytundebau defnydd derbyniol cysylltiedig
- ar gael i staff adeg cynefino a thrwy sianelau cyfathrebu arferol (i'w disgrifio)
- i'w gyhoeddi ar wefan yr ysgol.

Defnydd derbyniol

Mae'r ysgol wedi diffinio'r hyn mae'n ei ystyried yn ddefnydd derbyniol/annerbyniol a dangosir hyn yn y tablau isod.

Cytundebau defnydd derbyniol

Dogfen sy'n amlinellu disgwyliadau'r ysgol o ran y defnydd cyfrifol o dechnoleg gan ei defnyddwyr yw'r Cytundeb Defnydd Derbyniol

Mae'r Polisi a'r atodiadau Diogelwch Ar-lein yn diffinio defnydd derbyniol yn yr ysgol. Yn yr atodiadau ceir cytundebau defnydd derbyniol ar gyfer y canlynol:

- dysgwyr – wedi'u gwahaniaethu yn ôl oed. Bydd dysgwyr yn cael eu cyflwyno i'r rheolau defnydd derbyniol mewn sesiynau cynefino, ar ddechrau pob blwyddyn ysgol ac yn cael eu hatgyfnerthu'n rheolaidd yn ystod gwersi, gwasanaethau boreol a thrwy bosteri/sgriniau o amgylch yr ysgol
- bydd staff a gwirfoddolwyr yn cytuno ac yn llofnodi'r Cytundeb Defnydd Derbyniol
- mae Cytundeb Defnydd Derbyniol rhieni/gofalwyr yn rhoi gwybod iddynt am y disgwyliadau o ddefnydd derbyniol ar gyfer eu plant ac yn gofyn am ganiatâd ar gyfer delweddau digidol, defnyddio systemau cwmwl ac ati.
- bydd yn ofynnol i ddefnyddwyr cymunedol sy'n defnyddio systemau technoleg ddigidol ysgolion lofnodi Cytundeb Defnydd Derbyniol.

Bydd y cytundebau defnydd derbyniol yn cael eu cyfleu/atgyfnerthu drwy'r canlynol:

- llawlyfr ysgol
- cyflwyniad a llawlyfr staff

- arwyddion digidol
- posteri/hysbysiadau o amgylch mannau lle mae technoleg yn cael ei defnyddio
- cyfathrebu â rhieni/gofalwyr
- wedi'u cynnwys mewn sesiynau addysg
- gwefan yr ysgol
- cymorth gan gymheiriaid.

Gweithredoedd defnyddwyr		Derbyniol	Derbyniol ar adegau penodol	Derbyniol i ddefnyddwyr [illegible]	Annerbyniol	Annerbyniol ac anghyfreithlon
Ni fydd defnyddwyr yn ymweld â gwefannau, nac yn creu, postio, lawrlwytho, llwytho, trosglwyddo data, cyfathrebu na phasio, deunydd, cynigion na sylwadau sy'n cynnwys neu sy'n gysylltiedig â'r canlynol:	delweddau o gam-drin plant yn rhywiol - creu, cynhyrchu neu ddosbarthu delweddau anweddus o blant, yn groes i Ddeddf Amddiffyn Plant 1978 D.S. Dylai ysgolion gyfeirio at ganllawiau ynghylch rhannu lluniau noeth a hanner noeth..					X
	meithrin perthynas i bwrpas rhyw (*grooming*), annog, trefnu neu hwyluso gweithredoedd rhywiol yn erbyn plant, yn groes i Ddeddf Troseddau Rhywiol 2003					X
	meddu ar ddelwedd bornograffig eithafol (sy'n ddychrynllyd o anweddus, ffiaidd neu sydd fel arall o natur anllad), yn groes i Ddeddf Cyfiawnder Troseddol a Mewnfudo 2008					X
	deunydd hiliol troseddol yn y DU - i ysgogi casineb crefyddol (neu gasineb ar sail cyfeiriadedd rhywiol) - yn groes i Ddeddf Trefn Gyhoeddus 1986					X
	pornograffi				X	
	hyrwyddo unrhyw fath o wahaniaethu				X	
	ymddygiad bygythiol, gan gynnwys hyrwyddo trais corfforol neu niwed meddyliol				X	
	hyrwyddo eithafiaeth neu derfysgaeth				X	
	unrhyw wybodaeth arall a allai sarhau cydweithwyr neu ddiffygio cyfanrwydd ethos yr ysgol neu ddwyn anfri ar yr ysgol				X	
Gweithgareddau y gellid eu hystyried yn seiberdrosedd o dan Ddeddf Camddefnyddio Cyfrifiaduron (1990): • Defnyddio enw defnyddiwr neu ID a chyfrinair unigolyn arall i gael mynediad at ddata, rhaglen neu rannau o system nad oes gan y defnyddiwr hawl i'w defnyddio (hyd yn oed os yw'r mynediad cychwynnol wedi'i awdurdodi) • Cael mynediad heb awdurdod at rwydweithiau, data a ffeiliau'r ysgol, drwy ddefnyddio cyfrifiaduron/dyfeisiau • Creu neu ledaenu firysau cyfrifiadurol neu ffeiliau niweidiol eraill • Amlygu neu gyhoeddi gwybodaeth gyfrinachol neu berchnogol (e.e. gwybodaeth gyllidol/personol, cronfeydd data, codau mynediad a chyfrineiriau cyfrifiadurol/rhwydwaith) • Analluogi/Amharu swyddogaethau rhwydwaith drwy ddefnyddio cyfrifiaduron/dyfeisiau • Defnyddio offer profi treiddio (heb ganiatâd perthnasol)						X

D.S. Bydd angen i ysgolion benderfynu a ddylid delio â'r rhain yn fewnol ynteu gan yr heddlu. Dylid rhoi gwybod i'r heddlu am droseddau difrifol neu droseddau sy'n digwydd dro ar ôl tro. O dan yr agenda Atal Seiberdroseddu, mae gan yr Asiantaeth Troseddu Cenedlaethol gylch gwaith i atal dysgwyr rhag ymwneud â seiberdroseddu a ffrwyno eu gweithgarwch mewn ffyrdd cadarnhaol – rhagor o wybodaeth yma					
Defnyddio systemau'r ysgol i redeg busnes preifat				X	
Defnyddio systemau, apiau, gwefannau neu fecanweithiau eraill sy'n osgoi hidlo neu broses arall o ddiogelu sy'n cael ei defnyddio gan yr ysgol				X	
Torri hawlfraint				X	
Amlygu neu gyhoeddi gwybodaeth gyfrinachol neu berchnogol (e.e. gwybodaeth gyllidol/personol, cronfeydd data, codau mynediad a chyfrineiriau cyfrifiadurol/rhwydwaith)				X	
Creu neu ledaenu firysau cyfrifiadurol neu ffeiliau niweidiol eraill				X	
Defnydd annheg (lawrlwytho/llwytho ffeiliau mawr sy'n rhwystro eraill rhag defnyddio'r rhyngrwyd)				X	
Chwarae gemau ar-lein (addysgiadol)		X			
Chwarae gemau ar-lein (ddim yn addysgiadol)		X			
Gamblo ar-lein				X	
Siopa/masnach ar-lein					
Rhannu ffeiliau		X			
Defnyddio cyfryngau cymdeithasol * Trydar yr ysgol		X*			
Defnyddio apiau anfon negeseuon					
Darlledu fideos e.e. YouTube		X			

	Staff ac oedolion eraill						
	Caniateir	Caniateir ar adegau penodol	Caniateir i staff penodol	Chewch chi ddim	Caniateir	Caniateir ar adegau penodol	Caniateir gyda chaniatâd staff
Caniateir dod â ffonau symudol i'r ysgol	X						
Defnyddio ffonau symudol mewn gwersi							X
Defnyddio ffonau symudol yn ystod cyfnodau cymdeithasol		X					
Tynnu lluniau ar ffonau symudol / camerâu							X
Defnyddio dyfeisiau symudol eraill e.e. tabledi, dyfeisiau chwarae gemau							X
Defnyddio cyfeiriadau e-bost personol yn yr ysgol, neu ar rwydwaith yr ysgol	X						
Defnyddio e-bost yr ysgol ar gyfer e-byst personol				X			
Defnyddio apiau anfon negeseuon		X					
Defnyddio cyfryngau cymdeithasol		X					

Wrth ddefnyddio technolegau cyfathrebu, mae'r ysgol yn ystyried yr arferion canlynol fel enghreifftiau o rai da:

- **gall gwasanaeth e-bost swyddogol yr ysgol gael ei ystyried yn ddiogel ac mae'n cael ei fonitro. Dylai defnyddwyr fod yn ymwybodol bod cyfathrebiadau e-bost yn cael eu monitro.** *Felly, dim ond gwasanaeth e-bost yr ysgol y dylai staff a dysgwyr ei ddefnyddio i gyfathrebu â phobl eraill pan fyddant yn yr ysgol, neu ar systemau'r ysgol (e.e. drwy gysylltiad o bell)*
- **yn unol â pholisi'r ysgol, dylai dysgwyr roi gwybod i'r person enwebedig yn syth os ydynt yn cael unrhyw neges sy'n gwneud iddynt deimlo'n anghyffyrddus, os yw natur y neges yn sarhaus, yn wahaniaethol, yn fygythiol, neu'n neges sy'n bwlio. Ni ddylid ateb y fath negeseuon**
- **mae'n rhaid i unrhyw gyfathrebu digidol rhwng y staff â'r dysgwyr neu rieni/gofalwyr (e-bost, sgwrsio, platfform dysgu ac ati) fod yn broffesiynol o ran naws a chynnwys.** *Dim ond ar systemau swyddogol yr ysgol (sy'n cael eu monitro) y caniateir y math hwn o gyfathrebu. Ni ddylid defnyddio cyfeiriadau e-bost personol, negeseuon testun na chyfryngau cymdeithasol ar gyfer y math hwn o gyfathrebu*

- *dylid addysgu dysgwyr am faterion diogelwch ar-lein, fel y peryglon sy'n gysylltiedig â rhannu manylion personol. Dylid hefyd eu dysgu am strategaethau ynglŷn â sut i ddelio â chyfathrebiadau amhriodol, a'u hatgoffa o ddinasyddiaeth ddigidol a'r angen i gyfathrebu'n briodol wrth ddefnyddio technolegau digidol.*
- *ni ddylid postio gwybodaeth bersonol ar wefan yr ysgol a dim ond cyfeiriadau e-bost swyddogol y dylid eu defnyddio i gysylltu ag aelodau o'r staff*

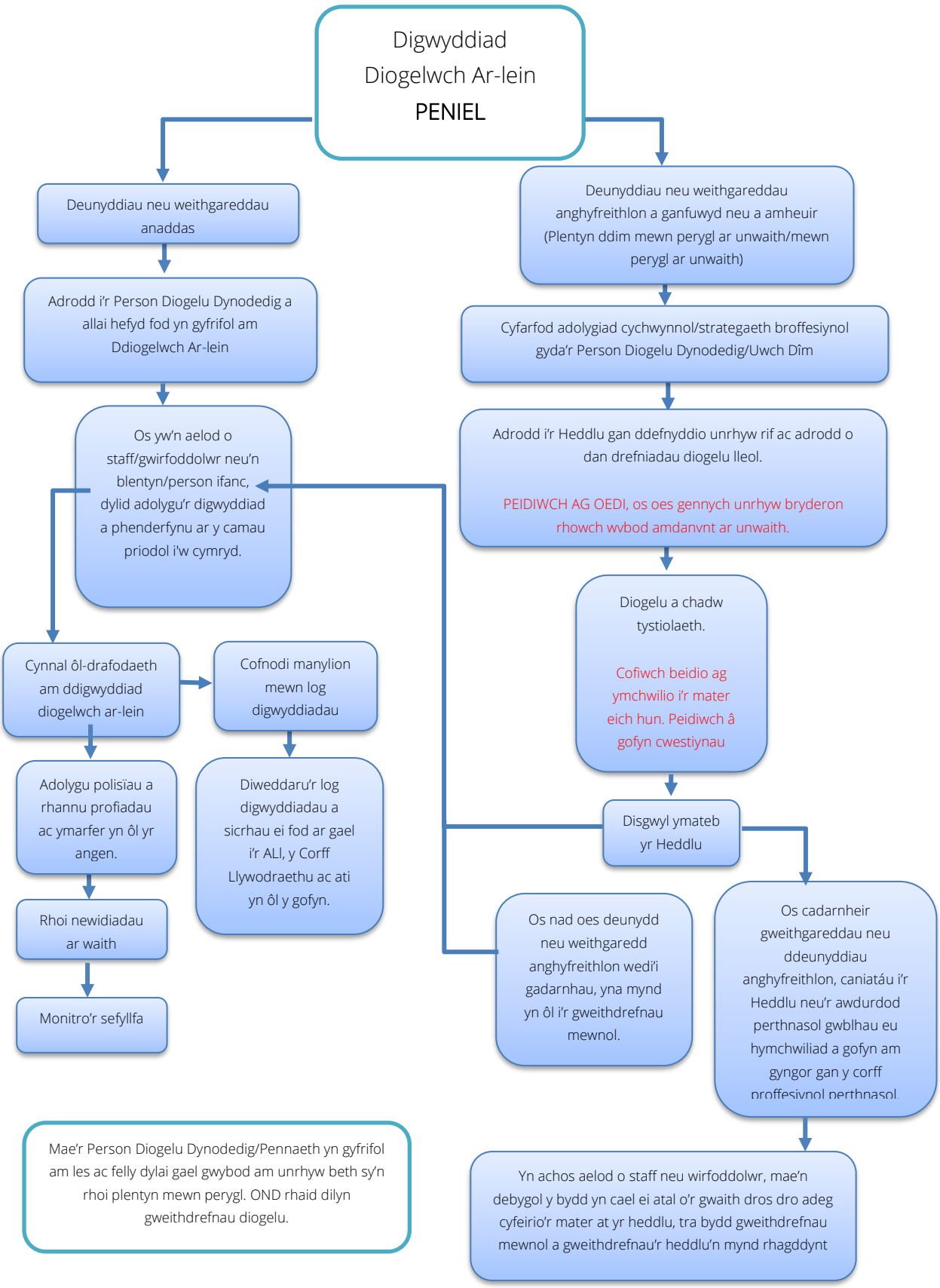
Adrodd ac ymateb

Bydd yr ysgol yn cymryd pob cam rhesymol i sicrhau diogelwch ar-lein i holl ddefnyddwyr yr ysgol, ond mae'n cydnabod y gall digwyddiadau ddigwydd y tu mewn a'r tu allan i'r ysgol (gan effeithio ar yr ysgol) a fydd angen ymyrryd. Bydd yr ysgol yn sicrhau canlynol:

- **bod llwybrau adrodd clir sy'n cael eu deall a'u dilyn gan holl aelodau cymuned yr ysgol sy'n gyson â gweithdrefnau diogelu'r ysgol, ac â pholisïau chwythu'r chwiban, cwynion a rheoli honiadau.**
- **bydd holl aelodau cymuned yr ysgol yn cael gwybod am yr angen i roi gwybod ar unwaith am faterion/digwyddiadau diogelwch ar-lein**
- **ymdrinnir ag adroddiadau cyn gynted ag y bo'n ymarferol bosibl ar ôl eu cael**
- **bod gan y Person Diogelu Dynodedig, yr Arweinydd Diogelwch Ar-lein a staff cyfrifol eraill y sgiliau a'r hyfforddiant priodol i ddelio â'r gwahanol risgiau sy'n gysylltiedig â diogelwch ar-lein**
- **os oes unrhyw amheuaeth bod delweddau o gam-drin plant, unrhyw weithgarwch anghyfreithlon arall neu'r posibilrwydd o niwed difrifol yn rhan o'r digwyddiad** (gweler y siart lif a'r siart camau gweithredu i ddefnyddwyr yn yr atodiad), **rhaid uwchgyfeirio'r digwyddiad drwy weithdrefnau diogelu arferol yr ysgol a rhoi gwybod i'r heddlu. Yn yr amgylchiadau hyn, dylid ynysu unrhyw ddyfais sy'n gysylltiedig i gefnogi ymchwiliad posibl gan yr heddlu. Yn ogystal â delweddau o gam-drin plant, byddai digwyddiadau o'r fath yn cynnwys:**
    - digwyddiadau o feithrin perthynas i bwrpas rhyw (*grooming*)
    - anfon deunydd anweddus i blentyn
    - deunydd ar gyfer oedolion sydd o bosibl yn torri'r Ddeddf Cyhoeddiadau Anweddus
    - deunydd hiliol troseddol
    - hyrwyddo eithafiaeth neu derfysgaeth
    - ymddygiad, gweithgaredd neu ddeunydd troseddol arall
- bydd unrhyw bryder am gamddefnydd gan staff yn cael ei adrodd i'r Pennaeth ar unwaith, oni bai fod y pryder yn ymwneud â'r Pennaeth, ac os felly, caiff y gŵyn ei chyfeirio at Gadeirydd y Llywodraethwyr a'r awdurdod lleol
- cyn belled nad oes amheuaeth o weithgarwch anghyfreithlon, gellir gwirio dyfeisiau gan ddefnyddio'r gweithdrefnau canlynol:
    - dylai un neu fwy o aelodau staff uwch fod yn rhan o'r broses hon. Mae hyn yn hanfodol i amddiffyn unigolion os caiff y cyhuddiadau eu hadrodd yn ddiweddarach.
    - cynnal y weithdrefn gan ddefnyddio cyfrifiadur dynodedig na fydd yn cael ei ddefnyddio gan ddysgwyr ac y gellir ei gludo oddi ar y safle gan yr heddlu os oes angen (pe digwydd i weithgarwch anghyfreithiol gael ei amau'n ddiweddarach). Defnyddio'r un cyfrifiadur drwy gydol y weithdrefn.

        - mae'n bwysig sicrhau bod gan staff perthnasol fynediad priodol i'r rhyngrwyd er mwyn iddynt allu cynnal y weithdrefn, ond bod y gwefannau a'r cynnwys yr ymwelir â hwy yn cael eu monitro'n agos a'u cofnodi (i ddarparu amddiffyniad pellach).
        - cofnodi URL unrhyw safle sy'n cynnwys y camddefnydd honedig a disgrifio natur y cynnwys sy'n achosi pryder. Efallai y bydd rhaid hefyd gofnodi a chadw sgrinluniau o'r cynnwys ar y peiriant sy'n cael ei ddefnyddio ar gyfer yr ymchwiliad. Gallai'r rhain gael eu hargraffu, eu llofnodi a'u hatodi i'r ffurflen (**ac eithrio mewn achosion o ddelweddau o gam-drin plant yn rhywiol - gweler isod**).
        - ar ôl i hyn gael ei gwblhau a'i archwilio'n llawn bydd angen i'r grŵp benderfynu a oes sylwedd i'r pryder hwn ai peidio. Os oes, bydd angen gweithredu'n briodol a gall hyn gynnwys y camau canlynol:
            - ymateb mewnol neu weithdrefnau disgyblu
            - ymwneud gan awdurdod lleol (fel y bo'n berthnasol)
            - ymwneud a/neu weithredu gan yr heddlu
- mae'n bwysig bod y rhai sy'n adrodd am ddigwyddiad diogelwch ar-lein yn hyderus y caiff yr adroddiad ei drin o ddifrif ac y delir ag ef yn effeithiol
- mae strategaethau cefnogi ar waith e.e. cymorth gan gymheiriaid ar gyfer y rheini sy'n rhoi gwybod am ddigwyddiad diogelwch ar-lein neu sy'n cael eu heffeithio gan ddigwyddiad o'r fath
- mae staff perthnasol yn ymwybodol o ffynonellau allanol o gymorth ac arweiniad wrth ddelio â materion diogelwch ar-lein, e.e. awdurdod lleol; yr heddlu; Llinell Gymorth i Weithwyr Proffesiynol ar Ddiogelwch Ar-lein; Rhoi Gwybod am Gynnwys Niweidiol; CEOP: Cadw'n ddiogel ar-lein ar Hwb
- bydd y rhai sy'n gysylltiedig â'r digwyddiad yn derbyn adborth am ganlyniad yr ymchwiliad a chamau dilynol
- bydd dysgu o'r digwyddiad (neu batrwm o ddigwyddiadau) yn cael ei ddarparu i'r:
    - *Arweinydd Diogelwch Ar-lein i ystyried diweddariadau i bolisïau neu raglenni addysg ac i adolygu pa mor effeithiol yr ymdriniwyd â'r adroddiad*
    - *staff, drwy gyfarfodydd briffio rheolaidd*
    - *dysgwyr, drwy wasanaethau/gwersi*
    - *rhieni/gofalwyr, drwy gylchlythyrau, cyfryngau cymdeithasol yr ysgol, gwefan*
    - *llywodraethwyr, drwy ddiweddariadau diogelu rheolaidd*
    - *awdurdod lleol/asiantaethau allanol, fel y bo'n berthnasol*

Bydd yr ysgol yn sicrhau bod y siart llif isod ar gael i staff i gefnogi'r broses o wneud penderfyniadau ar gyfer delio â digwyddiadau diogelwch ar-lein.


Digwyddiad Diogelwch Ar-lein
PENIEL
Deunyddiau neu weithgareddau anaddas
Adrodd i'r Person Diogelu Dynodedig a allai hefyd fod yn gyfrifol am Ddiogelwch Ar-lein
Os yw'n aelod o staff/gwirfoddolwr neu'n blentyn/person ifanc, dylid adolygu'r digwyddiad a phenderfynu ar y camau priodol i'w cymryd.
Cynnal ôl-drafodaeth am ddigwyddiad diogelwch ar-lein
Cofnodi manylion mewn log digwyddiadau
Adolygu polisïau a rhannu profiadau ac ymarfer yn ôl yr angen.
Diweddaru'r log digwyddiadau a sicrhau ei fod ar gael i'r ALl, y Corff Llywodraethu ac ati yn ôl y gofyn.
Rhoi newidiadau ar waith
Monitro'r sefyllfa
Mae'r Person Diogelu Dynodedig/Pennaeth yn gyfrifol am les ac felly dylai gael gwybod am unrhyw beth sy'n rhoi plentyn mewn perygl. OND rhaid dilyn gweithdrefnau diogelu.
Deunyddiau neu weithgareddau anghyfreithlon a ganfuwyd neu a amheuir (Plentyn ddim mewn perygl ar unwaith/mewn perygl ar unwaith)
Cyfarfod adolygiad cychwynnol/strategaeth broffesiynol gyda'r Person Diogelu Dynodedig/Uwch Dîm
Adrodd i'r Heddlu gan ddefnyddio unrhyw rif ac adrodd o dan drefniadau diogelu lleol.
PEIDIWCH AG OEDI, os oes gennych unrhyw bryderon rhowch wybod amdanynt ar unwaith.
Diogelu a chadw tystiolaeth.
Cofiwch beidio ag ymchwilio i'r mater eich hun. Peidiwch â gofyn cwestiynau
Disgwyl ymateb yr Heddlu
Os nad oes deunydd neu weithgaredd anghyfreithlon wedi'i gadarnhau, yna mynd yn ôl i'r gweithdrefnau mewnol.
Os cadarnheir gweithgareddau neu ddeunyddiau anghyfreithlon, caniatáu i'r Heddlu neu'r awdurdod perthnasol gwblhau eu hymchwiliad a gofyn am gyngor gan y corff proffesiynol perthnasol.
Yn achos aelod o staff neu wirfoddolwr, mae'n debygol y bydd yn cael ei atal o'r gwaith dros dro adeg cyfeirio'r mater at yr heddlu, tra bydd gweithdrefnau mewnol a gweithdrefnau'r heddlu'n mynd rhagddynt

Camau gweithredu gan ysgolion

Mae'n fwy tebygol mai'r ysgol fydd yn delio â digwyddiadau sy'n cynnwys camddefnydd amhriodol yn hytrach nag anghyfreithlon. Mae'n bwysig ymdrin ag unrhyw ddigwyddiadau cyn gynted â phosibl mewn modd cymesur, a bod aelodau o gymuned yr ysgol yn ymwybodol y deliwyd â ddigwyddiadau. Y bwriad yw ymdrin â digwyddiadau o gamddefnydd drwy weithdrefnau ymddygiad/disgyblu arferol fel a ganlyn:

Gweithredoedd dysgwyr

Digwyddiadau	Cyfeirio at athro / tiwtor dosbarth	Cyfeirio at Bennaeth Adran / Pennaeth Blwyddyn / arall	Cyfeirio at y Pennaeth	Cyfeirio at yr Heddlu	Cyfeirio at staff cymorth technegol ar gyfer gweithredu o ran hidlo/diogelwch ayb	Hysbysu rhieni/gofalwyr	Tynnu hawliau mynediad i'r rhwydwaith/rhyngrwyd	Rhoi rhybudd	Sancsiwn pellach e.e. cadw ar ôl /gwaharddiad
Cyrchu'n fwriadol neu geisio cael mynediad at ddeunydd sy'n gallu cael ei ystyried yn anghyfreithlon (gweler y rhestr mewn adran gynharach ar weithgareddau anaddas/amhriodol).		X	X	X					
Defnyddio gwefannau nad ydynt yn addysgiadol yn ystod gwersi heb awdurdod.	X	X							
Defnyddio ffonau symudol/camera digidol/dyfeisiau symudol eraill heb awdurdod.		X				X		X	
Defnyddio cyfryngau cymdeithasol/apiau anfon negeseuon/e-bost personol heb awdurdod.	X	X				X		X	
Lawrlwytho neu lwytho ffeiliau heb awdurdod.	X								
Caniatáu i eraill gael mynediad at rwydwaith yr ysgol wrth rannu enw defnyddiwr a chyfrineiriau.	X	X	X			X		X	
Ceisio mynediad, neu gael mynediad at rwydwaith yr ysgol gan ddefnyddio cyfrif dysgwr arall.	X	X	X			X		X	
Ceisio mynediad, neu gael mynediad at rwydwaith yr ysgol gan ddefnyddio cyfrif aelod o staff.	X	X	X			X		X	X
Llygru neu ddinistrio data defnyddwyr eraill.	X	X	X			X	X	X	
Gyrru e-bost, testun neu neges sy'n cael ei ystyried yn un sarhaus, sy'n aflonyddu neu sydd â natur bwlio.	X	X	X			X	X	X	X

Torri'r rheolau uchod yn barhaus, yn dilyn rhybuddion neu sancsiynau blaenorol.	X	X	X			X	X	X	X
Gweithgareddau a all ddwyn anfri ar yr ysgol neu ddifetha gonestrwydd neu ethos yr ysgol.	X	X	X			X	X	X	
Cael mynediad i ddeunydd sarhaus neu bornograffig ar ddamwain a pheidio hysbysu rhywun am y digwyddiad.	X	X	X	X	X	X			
Cael, neu geisio cael mynediad at ddeunydd sarhaus neu bornograffig yn fwriadol.	X	X	X	X	X	X	X	X	X
Cael neu drosglwyddo deunydd sydd yn torri hawlfraint person arall neu'n torri'r Ddeddf Diogelu Data.	X	X	X			X	X	X	X

Camau Gweithredu'r Staff

Digwyddiadau	Cyfeirio at y rheolwr llinell	Cyfeirio at y Pennaeth	Cyfeirio at awdurdod lleol/Adnoddau Dynol	Cyfeirio at yr Heddlu	Cyfeirio at Staff Cymorth Technegol ar gyfer gweithredu o ran hidlo, ac ati	Rhoi rhybudd	Atal dros dro	Camau disgyblu
Cyrchu'n fwriadol neu geisio cael mynediad at ddeunydd sy'n gallu cael ei ystyried yn anghyfreithlon (gweler y rhestr mewn adran gynharach ar weithgareddau anaddas/amhriodol).		X	X	X				
Defnydd personol amhriodol o'r rhyngrwyd/cyfryngau cymdeithasol/e-bost personol		X				X		
Lawrlwytho neu lwytho ffeiliau heb awdurdod.		X						
Caniatáu i eraill gael mynediad at rwydwaith ysgol drwy rannu enw defnyddiwr a chyfrineiriau neu geisio cael mynediad at rwydwaith yr ysgol neu gael mynediad ato, gan ddefnyddio cyfrif rhywun arall.		X	X		X	X		

Defnydd diofal o ddata personol, e.e. dangos, dal neu drosglwyddo data mewn modd anniogel		X						
Gweithredoedd bwriadol i dorri rheolau diogelu data neu ddiogelwch rhwydwaith.		X	X			X		
Llygru neu ddinistrio data defnyddwyr eraill neu achosi difrod bwriadol i galedwedd neu feddalwedd		X	X	X		X	X	X
Gyrru e-bost, testun neu neges sy'n cael ei ystyried yn un sarhaus, sy'n aflonyddu neu sydd â natur bwlio.		X	X			X		X
Defnyddio negeseuon e-bost/rhwydweithio cymdeithasol personol i gyfathrebu'n ddigidol â dysgwyr a rhieni/gofalwyr		X	X			X		
Camau gweithredu a allai beryglu statws proffesiynol yr aelod o staff		X	X			X		X
Gweithgareddau a all ddwyn anfri ar yr ysgol neu ddifetha gonestrwydd neu ethos yr ysgol.		X	X			X		X
Cael mynediad i ddeunydd sarhaus neu bornograffig ar ddamwain a pheidio hysbysu rhywun am y digwyddiad.		X	X			X		
Cael, neu geisio cael mynediad at ddeunydd sarhaus neu bornograffig yn fwriadol.		X	X	X		X	X	X
Torri rheoliadau hawlfraint neu drwyddedu.		X						
Torri'r rheolau uchod yn barhaus, yn dilyn rhybuddion neu sancsiynau blaenorol.		X	X	X		X	X	X

Addysg

Rhaglen Addysg Diogelwch Ar-lein

Tra bo rheoleiddio ac atebion technegol yn bwysig iawn, rhaid i'w defnydd gael ei gydbwyso ag addysgu dysgwyr i weithredu'n gyfrifol. Mae addysgu dysgwyr am ddiogelwch ar-lein felly'n rhan hanfodol o ddarpariaeth diogelwch ar-lein yr ysgol. Mae angen cymorth a chefnogaeth yr ysgol ar ddysgwyr i adnabod ac osgoi risgiau i ddiogelwch ar-lein a datblygu eu gwytnwch.

Dylai diogelwch ar-lein fod yn ffocws ym mhob rhan o'r cwricwlwm a dylai staff atgyfnerthu negeseuon diogelwch ar-lein ar draws y cwricwlwm. Dylai'r cwricwlwm diogelwch ar-lein fod yn

eang, yn berthnasol a darparu cynnydd, gyda chyfleoedd ar gyfer gweithgareddau creadigol a bydd yn cael ei ddarparu yn y ffyrdd canlynol:

- **cwricwlwm diogelwch ar-lein wedi'i gynllunio ar draws pob blwyddyn oedran ac ystod o bynciau, (e.e. DCF/ABCh/RSE/Iechyd a Lles) a dylid ailymweld â meysydd pwnc yn rheolaidd**
- **dylid atgyfnerthu negeseuon diogelwch ar-lein hanfodol fel rhan o raglen gwasanaethau boreol a gweithgareddau tiwtorial/bugeiliol sydd wedi'u chynllunio.**
- **mae'n cynnwys/defnyddio cynlluniau a chyfleoedd cenedlaethol perthnasol e.e.** Diwrnod Defnyddio'r Rhyngrwyd yn Fwy Diogel **ac** Wythnos Gwrth-fwlio
- **bydd y rhaglen ar gael i ddysgwyr o wahanol oedrannau a galluoedd, fel y rheini sydd ag anghenion dysgu ychwanegol neu'r rheini sydd â Saesneg fel iaith ychwanegol. Mae dysgwyr y credir eu bod mewn mwy o berygl ar-lein (e.e. plant mewn gofal, dysgwyr Anghenion Addysgol Arbennig ac Anabledd, dysgwyr sy'n profi colled neu drawma neu broblemau iechyd meddwl) yn cael addysg diogelwch ar-lein wedi'i thargedu neu wedi'i gwahaniaethu**
- **dylid dysgu dysgwyr ymhob gwers i fod yn ymwybodol iawn o'r deunydd/cynnwys maent yn cael mynediad ato ar-lein a'u hannog i ddilysu cywirdeb gwybodaeth**
- **dylid dysgu pob dysgwr i gydnabod ffynhonnell yr wybodaeth a ddefnyddir ac i barchu hawlfraint wrth ddefnyddio deunydd a gyrchir ar y rhyngrwyd.**
- dylai staff weithredu fel modelau rôl o ran defnyddio technolegau digidol, y rhyngrwyd a dyfeisiau symudol.
- pan fydd gwersi wedi cael eu cynllunio i ddefnyddio'r rhyngrwyd, yr arfer gorau fyddai cyfeirio'r dysgwyr at wefannau sydd wedi'u gwirio fel eu bod yn addas i'w defnyddio a bod prosesau yn eu lle i ddelio ag unrhyw ddeunydd anaddas y maent yn dod ar ei draws wrth chwilio'r rhyngrwyd.
- pan fydd dysgwyr yn cael rhyddid i chwilio'r rhyngrwyd, dylai staff fod yn wyliadwrus wrth oruchwylio'r dysgwyr a monitro cynnwys y gwefannau y mae'r bobl ifanc yn ymweld â nhw
- oherwydd rhesymau addysgiadol, rhaid derbyn o bryd i'w gilydd bod ar ddysgwyr angen ymchwilio pynciau a fyddai fel arfer yn cael eu gwahardd wrth ddefnyddio'r rhyngrwyd (e.e. hiliaeth, cyffuriau, gwahaniaethu). Mewn sefyllfa o'r fath, gall staff ofyn i staff technegol (neu berson enwebedig arall) dynnu'r safleoedd hynny oddi ar y rhestr hidlo dros dro ar gyfer y cyfnod astudio. Dylid gallu archwilio unrhyw gais i wneud hyn, a dangos rhesymau clir dros yr angen.
- bydd y rhaglen addysg diogelwch ar-lein yn cael ei harchwilio a'i gwerthuso'n rheolaidd i sicrhau ansawdd y dysgu a'r canlyniadau.

Cyfraniad Dysgwyr

Mae'r ysgol yn cydnabod, yn dysgu oddi wrth, ac yn defnyddio sgiliau a gwybodaeth dysgwyr wrth ddefnyddio technolegau newydd. Rydym yn cydnabod y potensial i hyn siapio'r strategaeth diogelwch ar-lein ar gyfer cymuned yr ysgol a sut mae hyn yn cyfrannu'n gadarnhaol at ddatblygiad personol pobl ifanc. Caiff eu cyfraniad ei gydnabod drwy:

- dulliau i gasglu adborth a barn dysgwyr.
- penodi dewiniaid digidol
- mae dysgwyr yn cyfrannu at y rhaglen addysg diogelwch ar-lein e.e. addysg i gymheiriaid, arweinwyr digidol yn arwain gwersi i ddysgwyr iau, ymgyrchoedd diogelwch ar-lein
- dysgwyr yn dylunio/diweddaru cytundebau defnydd derbyniol
- cyfrannu'n weithredol at ddigwyddiadau diogelwch ar-lein gyda chymuned ehangach yr ysgol e.e. nosweithiau rhieni, rhaglenni dysgu teuluol ac ati.

Staff/gwirfoddolwyr

Mae'n hanfodol bod yr holl staff yn derbyn hyfforddiant diogelwch ar-lein ac yn deall eu cyfrifoldebau, fel yr amlinellir yn y polisi hwn. Bydd yr hyfforddiant canlynol yn cael ei gynnig:

- **bydd rhaglen o hyfforddiant ar ddiogelwch ar-lein ffurfiol a diogelu data ar gael i'r holl staff. Caiff y rhaglen hon ei diweddaru a'i hategu. Cynhelir archwiliad o anghenion hyfforddiant diogelwch ar-lein yr holl staff yn gyson.** *Disgwylir y bydd rhai o'r staff yn nodi anghenion hyfforddiant diogelwch ar-lein o dan y broses rheoli perfformiad*
- **bydd yr hyfforddiant yn rhan annatod o hyfforddiant diogelu a hyfforddiant diogelu data blynyddol yr ysgol ar gyfer yr holl staff**
- **bydd pob aelod newydd o staff gael hyfforddiant diogelwch ar-lein fel rhan o'r rhaglen gynefino er mwyn sicrhau eu bod yn deall polisi diogelwch ar-lein a chytundebau defnydd derbyniol yr ysgol yn llwyr. Mae'n cynnwys cyfeiriad penodol at reoli ystafell ddosbarth, ymddygiad proffesiynol, enw da ar-lein a'r angen i fodelu ymddygiad cadarnhaol**
- bydd yr Arweinydd Diogelwch Ar-lein/ Person Diogelu Dynodedig yn cael yr wybodaeth ddiweddaraf yn rheolaidd trwy fynychu hyfforddiant allanol (e.e. Digwyddiadau Cadw'n Ddiogel Ar-lein Hwb, gan y Consortiwm Rhanbarthol/SWGfL/ALl/sefydliadau perthnasol eraill) a thrwy adolygu dogfennau sy'n cynnig arweiniad gan sefydliadau perthnasol eraill.
- bydd y Polisi Diogelwch Ar-lein a'r diweddariadau iddo, yn cael ei gyflwyno i staff er mwyn iddynt ei drafod mewn cyfarfodydd staff/tîm neu ddiwrnodau HMS.
- bydd yr Arweinydd Diogelwch Ar-lein yn darparu cyngor/arweiniad/hyfforddiant i unigolion yn ôl yr angen.

Llywodraethwyr

Dylai llywodraethwyr gymryd rhan mewn hyfforddiant/sesiynau ymwybyddiaeth diogelwch ar-lein, yn enwedig y rhai sy'n aelodau o unrhyw is-bwyllgor/grŵp sy'n gysylltiedig â thechnoleg/diogelwch ar-lein/iechyd a diogelwch/diogelu. Gellir cynnig hyn mewn sawl ffordd:

- Hyfforddiant Hwb – Diogelwch ar-lein ar gyfer llywodraethwyr
- bod yn bresennol mewn hyfforddiant a ddarperir gan yr awdurdod lleol neu sefydliad perthnasol arall (e.e. SWGfL).
- cymryd rhan mewn sesiynau hyfforddiant/gwybodaeth yr ysgol i staff neu rieni (gall hyn olygu bod yn bresennol mewn gwasanaethau boreol/gwersi).

Bydd lefel uwch o hyfforddiant ar gael i'r Llywodraethwr Diogelwch Ar-lein (o leiaf).

Dylai ysgolion ystyried darparu cyfrif Hwb i bob llywodraethwr er mwyn defnyddio'r offer a'r gwasanaethau diogel sydd ar gael *e.e.* Microsoft Outlook, Teams ac ati yn ogystal â darparu hyfforddiant penodol ar raglenni. Byddai hyn yn golygu na fyddai angen i lywodraethwyr ddefnyddio cyfrifon e-bost personol, gan leihau'r risg i ddata.

Teuluoedd

Dim ond dealltwriaeth gyfyng iawn o risgiau a materion diogelwch ar-lein sydd gan lawer o rieni a gofalwyr, ond maent yn chwarae rhan hanfodol yn addysg eu plant ac mewn monitro/rheoleiddio ymddygiad eu plant ar-lein. Mae'n debygol nad yw rhieni'n sylweddoli pa mor aml mae plant a phobl ifanc yn dod ar draws deunydd amhriodol a all fod yn niweidiol ar-lein, ac nad ydynt yn siŵr sut i ymateb.

Bydd yr ysgol yn ceisio darparu gwybodaeth i rieni a gofalwyr a chodi eu hymwybyddiaeth trwy:

- cyfathrebu, codi ymwybyddiaeth ac ymgysylltu'n rheolaidd ar faterion diogelwch ar-lein, gweithgareddau'r cwricwlwm a llwybrau adrodd
- cyfleoedd rheolaidd i ymgysylltu â rhieni/gofalwyr ar faterion diogelwch ar-lein drwy weithdai ymwybyddiaeth/ nosweithiau rhieni/gofalwyr ac ati
- y dysgwyr – annog nhw i drosglwyddo i'w rhieni y negeseuon diogelwch ar-lein maen nhw wedi'u dysgu mewn gwersi a gan ddysgwyr sy'n arwain sesiynau mewn nosweithiau rhieni/gofalwyr.
- llythyrau, cylchlythyrau, gwefan, platfform dysgu, Hwb
- digwyddiadau/ymgyrchoedd amlwg *e.e.* Diwrnod Defnyddio'r Rhyngrwyd yn Fwy Diogel
- cyfeirio at y gwefannau/cyhoeddiadau perthnasol, *e.e.* Hwb Cadw'n ddiogel ar-lein, www.saferinternet.org.uk/ www.childnet.com/parents-and-carers (gweler yr Atodiad am ragor o ddolenni/adnoddau).

Oedolion ac Asiantaethau

Bydd yr ysgol yn darparu cyfleoedd i grwpiau cymunedol lleol ac aelodau o'r gymuned ehangach allu elwa o wybodaeth a phrofiad diogelwch ar-lein yr ysgol. Bydd hyn yn cael ei gynnig drwy sawl ffordd:

- darparu cyrsiau i deuluoedd ddysgu defnyddio technolegau digidol newydd a diogelwch ar-lein
- negeseuon diogelwch ar-lein sy'n targedu teuluoedd a pherthnasoedd.
- bydd yr ysgol yn darparu gwybodaeth am ddiogelwch ar-lein i'r gymuned ehangach drwy ei phlatfform dysgu, ei gwefan a'r cyfryngau cymdeithasol
- cefnogi grwpiau cymunedol *e.e.* sefydliadau blynyddoedd cynnar, gwarchodwyr plant, grwpiau ieuenctid/chwaraeon/gwirfoddol i wella eu darpariaethau diogelwch ar-lein

Hidlo

- mae uwch arweinwyr a staff technegol yn cytuno ar bolisïau hidlo'r ysgol ac maent yn cael eu hadolygu a'u diweddaru'n rheolaidd mewn ymateb i newidiadau mewn technoleg a phatrymau o ddigwyddiadau/ymddygiadau diogelwch ar-lein
- mae'r ysgol yn rheoli mynediad at gynnwys ar draws ei systemau i bob defnyddiwr. Mae'r rheolau hidlo sydd ar waith yn bodloni'r safonau a nodir yn Safonau a argymhellir gan Lywodraeth Cymru ar gyfer hidlo'r we mewn ysgolion a Rheolau hidlo priodol yr UK Safer Internet Centre.
- mae mynediad pob defnyddiwr i'r rhyngrwyd yn cael ei hidlo.
- mae cynnwys anghyfreithlon (e.e. delweddau lle mae plant yn cael eu cam-drin yn rhywiol) yn cael ei hidlo gan ddarparwr y gwasanaeth hidlo neu'r darparwr band eang drwy ddefnyddio rhestr CAIC yr Internet Watch Foundation yn ogystal â rhestr yr heddlu o gynnwys terfysgol anghyfreithlon, a gynhyrchir ar ran y Swyddfa Gartref. Mae rhestrau cynnwys yn cael eu diweddaru'n rheolaidd
- mae llwybrau sefydledig ac effeithiol sy'n galluogi defnyddwyr i roi gwybod am gynnwys amhriodol
- gweithredir proses glir sy'n delio â cheisiadau am newidiadau hidlo (gweler yr Atodiad am ragor o fanylion) – rhaid gwneud hyn drwy'r awdurdod lleol/
- mae logiau hidlo yn cael eu hadolygu'n rheolaidd ac yn rhybuddio'r ysgol am achosion o dorri'r polisi hidlo, er mwyn gweithredu arnynt – yr awdurdod sy'n gyfrifol am hyn.
- pan fydd dyfeisiau symudol personol yn cael mynediad i'r rhyngrwyd ar rwydwaith yr ysgol, rheolir ar y cynnwys sy'n ymddangos mewn modd sy'n unol ag arferion a pholisi'r ysgol.
- mae'r system yn rheoli mynediad at gynnwys drwy wasanaethau heblaw am borwr (e.e. apiau a thechnolegau symudol eraill)

Os bydd angen, bydd yr ysgol yn gofyn am gyngor gan safle Riportio Cynnwys Niweidiol SWGfL ac yn riportio digwyddiadau yna hefyd.

Monitro

Mae'r ysgol yn dilyn canllawiau Monitro Priodol yr UK Safer Internet Centre ac yn diogelu defnyddwyr a systemau'r ysgol drwy:

- monitro corfforol (oedolion yn goruchwylio yn yr ystafell ddosbarth)
- logio defnydd o'r rhyngrwyd, a bod hynny'n cael ei fonitro a'i adolygu'n rheolaidd
- dadansoddi logiau hidlo yn rheolaidd a rhoddir gwybod i uwch arweinwyr am achosion o dorri'r rheolau
- rhybuddion rhagweithiol yn rhoi gwybod i'r ysgol am achosion o dorri'r polisi hidlo, gan ganiatáu ymyrraeth effeithiol.

Mae defnyddwyr yn cael gwybod, drwy'r cytundebau defnydd derbyniol, bod y monitro hyn ar waith. (efallai bydd ysgolion yn dymuno ychwanegu manylion y rhaglenni monitro a ddefnyddir).

Diogelwch Technegol

- bydd systemau technegol ysgolion yn cael eu rheoli mewn ffyrdd sy'n sicrhau bod yr ysgol yn bodloni'r gofynion technegol sy'n cael eu hawgrymu
- caiff diogelwch systemau technegol yr ysgol ei adolygu a'u harchwilio'n rheolaidd
- mae gweinyddion, systemau diwifr a cheblau yn cael eu cadw mewn lle diogel a dylid cyfyngu ar fynediad pobl atynt
- mae trefniadau wrth gefn cadarn a dilys, gan gynnwys cadw copïau oddi ar y safle neu yn y cwmwl
- **bydd gan bob defnyddiwr hawliau mynediad i systemau technegol a dyfeisiau'r ysgol, sydd wedi cael eu diffinio'n glir.** Bydd Rheolwr y Rhwydwaith (neu unigolyn arall) yn cofnodi manylion yr hawliau mynediad sydd ar gael i grwpiau o ddefnyddwyr. **Bydd yr Uwch dîm** yn adolygu'r rhain unwaith y flwyddyn o leiaf
- **mae pob defnyddiwr (oedolion a dysgwyr) yn gyfrifol am gadw eu henw defnyddiwr a'u cyfrinair yn ddiogel. Ni ddylent ganiatáu i ddefnyddiwr arall ddefnyddio eu manylion mewngofnodi i gael mynediad i'r systemau. Gallai rhannu cyfrineiriau neu IDs arwain at gyflawni trosedd o dan Ddeddf Camddefnyddio Cyfrifiaduron 1990.** Rhaid i ddefnyddwyr roi gwybod ar unwaith am unrhyw amheuaeth neu dystiolaeth o dorri rheolau diogelwch
- **bydd holl rwydweithiau a systemau'r ysgol yn cael eu diogelu gan gyfrineiriau diogel. Ni ddylid rhannu cyfrineiriau ag unrhyw un. Bydd Elen H Powell yn rhoi enw defnyddiwr a chyfrinair i bawb** a bydd yn cadw cofnod cyfredol o ddefnyddwyr a'u henwau defnyddwyr
- **mae cyfrineiriau prif gyfrifon systemau'r ysgol yn cael eu cadw mewn man diogel e.e. sêff dan glo yr ysgol.**
- **dylai cyfrineiriau fod yn hir.** ***Mae arferion da yn nodi bod cyfrineiriau sy'n cynnwys dros 12 nod yn anoddach i'w cracio. Mae cyfrineiriau sy'n defnyddio cyfuniad o eiriau nad ydynt yn gysylltiedig â'i gilydd, ac sy'n cynnwys dros 16 nod yn arbennig o anodd eu dyfalu. Mae cyfrineiriau hir yn fwy diogel nag unrhyw ofynion arbennig eraill fel llythrennau bach/priflythrennau, rhifau a nodau arbennig. Dylid annog defnyddwyr i beidio â defnyddio rhifau mewn trefn neu batrwm o rifau yn eu cyfrineiriau. Dylai cyfrineiriau/codau cyfrin fod yn hawdd eu cofio ond yn anodd eu dyfalu.***
- mae modd cadw cofnod o enwau defnyddwyr a chyfrineiriau dysgwyr yn y Cyfnod Sylfaen ar ffurf electronig neu bapur, ond mae'n rhaid iddynt gael eu cadw'n ddiogel pan na fydd y defnyddiwr eu hangen. *Ni ddylai cyfrineiriau fod mor gymhleth ar gyfer y cyfnod sylfaen (er enghraifft, o leiaf 6 nod) ac ni ddylent gynnwys nodau arbennig. Pan fydd gan systemau allanol wahanol ofynion o ran cyfrineiriau, dylid annog defnyddio geiriau neu ymadroddion ar hap*
- dylai gofynion cyfrineiriau ar gyfer dysgwyr Cyfnod Allweddol 2 ac uwch gynyddu wrth i ddysgwyr symud ymlaen drwy'r ysgol
- Elen H Powell sy'n gyfrifol am sicrhau bod cofnodion trwyddedau meddalwedd yn gywir ac wedi'u diweddaru ac y gwneir archwiliadau rheolaidd i sicrhau bod nifer y trwyddedau a brynwyd yn cyfateb i nifer y cyfrifiaduron y gosodwyd meddalwedd arnynt
- mae system briodol yn mewn lle er mwyn i ddefnyddwyr adrodd wrth y person priodol am unrhyw ddigwyddiadau gwirioneddol neu bosib o dorri rheolau diogelwch ar-lein, fel y cytunwyd

- mae mesurau diogelwch yn eu lle i ddiogelu'r gweinyddwyr, muriau gwarchod, llwybryddion, systemau di-wifr, gweithfannau, dyfeisiau symudol ac ati rhag unrhyw ymgais ddamweiniol neu faleisus a allai fygwth diogelwch systemau a data'r ysgol. Mae'r rhain yn cael eu profi'n gyson. Mae seilwaith a gweithfannau unigol yr ysgol yn cael eu diogelu gan feddalwedd firws cyfredol.
- Bydd polisi y cytunwyd arno yn ei le ynghylch faint o ddefnydd personol y caniateir i ddefnyddwyr (staff/dysgwyr/defnyddwyr cymunedol) ac aelodau eu teulu ei gael ar ddyfeisiau'r ysgol wrth eu defnyddio y tu allan i'r ysgol
- mae polisi y cytunwyd arno yn ei le sy'n caniatáu neu'n gwahardd staff rhag lawrlwytho ffeiliau gweithredadwy a gosod rhaglenni ar ddyfeisiau'r ysgol.
- mae polisi y cytunwyd arno yn ei le sy'n ymwneud â defnyddio cyfryngau symudol (e.e. cof bach/CDs/DVDs) ar ddyfeisiau'r ysgol. Ni cheir anfon data personol dros y rhyngrwyd na'u tynnu oddi ar safle'r ysgol oni byddant wedi'u hamgryptio'n ddiogel neu eu diogelu trwy ddull arall.

Technolegau symudol

Gall dyfeisiau technoleg symudol fod yn eiddo i/cael eu darparu gan yr ysgol neu fod yn eiddo personol. Gall y rhain gynnwys: ffôn clyfar, tabled, dyfeisiau clyfar y gellir eu gwisgo, gliniadur neu dechnoleg arall sydd fel rheol yn gallu defnyddio rhwydwaith di-wifr yr ysgol. Felly, mae gan y ddyfais fynediad i'r rhyngrwyd ehangach, a all gynnwys platfform dysgu'r ysgol a gwasanaethau eraill ar y cwmwl, fel e-bost a storio data.

Dylai'r holl ddefnyddwyr ddeall mai prif bwrpas defnyddio dyfeisiau symudol/personol yng nghyd-destun ysgol yw at ddibenion addysgol. Dylai'r polisi technolegau symudol fod yn gyson ac yn rhyng-gysylltiedig â pholisïau eraill perthnasol yr ysgol, gan gynnwys y polisïau canlynol, ond heb fod yn gyfyngedig iddynt – diogelu, ymddygiad, gwrth-fwlio, defnydd derbyniol, a pholisïau perthnasol i ddwyn neu ddifrod maleisus. Dylid cynnwys addysgu am ddefnydd diogel a phriodol o dechnolegau symudol fel rhan o raglen addysgol ynglŷn â diogelwch ar-lein yr ysgol.

Wrth baratoi polisi technolegau symudol, dylai'r ysgol ystyried y problemau a'r risgiau posib. Gallai hyn gynnwys:

- risgiau diogelwch o ran caniatáu cyswllt â rhwydwaith eich ysgol
- hidlo dyfeisiau personol
- offer yn torri ac yswiriant
- mynediad i ddyfeisiau i'r holl ddysgwyr
- osgoi tarfu posib ar yr ystafell ddosbarth
- cyflymder cyswllt y rhwydwaith, y mathau o ddyfeisiau
- cyfleusterau gwefru
- cyfanswm cost perchnogaeth.

- Mae cytundebau defnydd derbyniol yr ysgol ar gyfer staff, dysgwyr, rhieni a gofalwyr yn amlinellu'r disgwyliadau ynghylch defnyddio technolegau symudol
- Mae'r ysgol yn caniatáu'r canlynol:

	Dyfeisiau'r ysgol			Dyfeisiau personol	
	Eiddo'r ysgol ar gyfer defnyddiwr unigol	**Eiddo'r ysgol ar gyfer nifer o ddefnyddwyr**	**Dyfeisiau awdurdodedig** [5]	**Eiddo'r myfyriwr**	**Eiddo i staff**
Caniateir yn yr ysgol				Na	Iawn
Cysylltiad llawn i'r rhwydwaith	Iawn	Iawn	Iawn		Iawn *amodol
Rhyngrwyd yn unig	Iawn	Iawn	Iawn		
Dim mynediad rhwydwaith				Iawn	

Dyfeisiau sy'n eiddo i/cael eu darparu gan yr ysgol:

- i bwy fyddant yn cael eu dosbarthu
- ble, pryd a sut y caniateir eu defnyddio – amseroedd/lleoliadau/y tu allan i'r ysgol
- a yw defnydd personol yn cael ei ganiatáu
- lefelau mynediad i'r rhwydweithiau/rhyngrwyd (gweler uchod)
- rheoli dyfeisiau/gosod apiau/newid gosodiadau/monitro
- capasiti'r rhwydwaith/band eang
- cymorth technegol
- hidlo dyfeisiau
- mynediad i wasanaethau cwmwl
- defnyddio ar dripiau/digwyddiadau y tu allan i'r ysgol
- diogelu data
- tynnu lluniau, storio/defnyddio delweddau
- prosesau gadael, beth sy'n digwydd i ddyfeisiau/meddalwedd/apiau/data wedi'i storio os yw'r defnyddiwr yn gadael yr ysgol
- atebolrwydd am ddifrod
- hyfforddiant staff.

[5] Dyfeisiau awdurdodedig – prynwyd gan y dysgwr/teulu drwy gynllun a drefnir gan yr ysgol. Gellir rhoi mynediad llawn i'r rhwydwaith i'r ddyfais yma, fel pe bai'n eiddo i'r ysgol.

Dyfeisiau personol

- pa ddefnyddwyr sy'n cael defnyddio dyfeisiau symudol personol yn yr ysgol (staff/dysgwyr/ymwelwyr)
- cyfyngiadau ar ble, pryd a sut gallant gael eu defnyddio yn yr ysgol – wele polisi dyfeisiadau personol
- os ydynt yn cael eu defnyddio i gefnogi'r dysgu, sut bydd staff yn cynllunio eu gwersi gan ystyried yr amrywiaeth posibl o fodelau dyfeisiau a systemau gweithredu gwahanol
- storio
- a fydd staff yn cael defnyddio dyfeisiau personol ar gyfer materion yn ymwneud â'r ysgol
- diogelu data
- tynnu lluniau, storio/defnyddio delweddau
- atebolrwydd am golled/difrod neu ddiffygion ar ôl cael mynediad i'r rhwydwaith (ymwadiad ynglŷn â chyfrifoldebau'r ysgol fwy na thebyg).
- adnabod/labelu dyfeisiau personol
- sut i roi gwybod i ymwelwyr am ofynion yr ysgol
- sut y bydd addysg am ddefnyddio dyfeisiau symudol yn ddiogel ac yn gyfrifol yn cael ei chynnwys yn rhaglen addysgol yr ysgol ynglŷn â diogelwch ar-lein
- sut byddai'r ysgol yn delio â chamddefnydd

Cyfryngau cymdeithasol

O ganlyniad i'r cynnydd yn y defnydd o bob math o gyfryngau cymdeithasol, a hynny at ddibenion proffesiynol a phersonol, mae polisi sy'n pennu canllawiau clir i staff ar reoli risg ac ymddygiad ar-lein yn hollbwysig. Un o'r prif negeseuon yw sicrhau bod y dysgwyr, yr ysgol ac unigolion yn cael eu hamddiffyn wrth gyhoeddi unrhyw ddeunydd ar-lein.

Gosodir disgwyliadau ymddygiad proffesiynol ar gyfer staff gan Gyngor Addysgu Cyffredinol Cymru, ond rhaid i bob oedolyn sy'n gweithio gyda phlant a phobl ifanc ddeall bod natur eu gwaith a'u cyfrifoldebau yn eu rhoi mewn swydd gyfrifol, a dylai eu hymddygiad adlewyrchu hynny.

Mae gan yr ysgol ac awdurdod lleol ddyletswydd gofal i ddarparu amgylchedd dysgu diogel i ddisgyblion a staff. Yn anuniongyrchol, gall ysgolion ac awdurdodau lleol gael eu gweld yn gyfrifol am weithredoedd eu gweithwyr yn ystod eu cyflogaeth. Os bydd aelod o staff yn poenydio, yn bwlio ar-lein, yn gwahaniaethu ar sail rhyw, hil neu anabledd, neu yn difenwi trydydd parti, gall beri i'r ysgol neu'r awdurdod lleol fod yn atebol i'r dioddefwr. Rhaid penderfynu ar gamau rhesymol er mwyn atal niwed rhagweladwy. Disgwylir i'r holl staff sy'n gweithio mewn unrhyw sefydliad addysgol ddilyn yr ymddygiad proffesiynol a bennir gan Gyngor Addysgu Cyffredinol Cymru gan barchu dysgwyr, eu teuluoedd, eu cydweithwyr a'r ysgol.

Er mwyn sicrhau bod camau rhesymol yn eu lle i leihau'r perygl o niwed, mae'r ysgol yn darparu'r mesurau canlynol:

- sicrhau nad yw gwybodaeth bersonol yn cael ei chyhoeddi

- darparu addysg/hyfforddiant sy'n cynnwys defnydd derbyniol, cyfyngiadau oed, peryglon cyfryngau cymdeithasol, polisi ar ddelweddau digidol a fideos, gwirio gosodiadau, diogelu data ac adrodd ar faterion
- rhoi arweiniad ar adrodd, gan gynnwys cyfrifoldebau, trefn a sancsiynau
- asesiad risg, gan gynnwys risg cyfreithiol
- canllawiau i ddysgwyr, rhieni/gofalwyr

Dylai staff yr ysgol sicrhau:

- nad oes unrhyw gyfeiriad tuag at ddysgwyr, rhieni/gofalwyr nac at staff yr ysgol ar gyfryngau cymdeithasol
- nad ydynt yn trafod materion personol ar-lein sy'n ymwneud ag aelodau o gymuned yr ysgol
- nad yw barn bersonol yn cael ei phriodoli i'r ysgol nac i'r awdurdod lleol
- bod gosodiadau diogelwch ar broffiliau cyfryngau cymdeithasol personol yn cael eu gwirio'n aml i leihau'r perygl o golli gwybodaeth bersonol
- maent yn fodelau rôl cadarnhaol wrth ddefnyddio'r cyfryngau cymdeithasol

Pan fydd cyfrifon cyfryngau cymdeithasol swyddogol yr ysgol yn cael eu sefydlu, dylid sicrhau bod ganddynt y canlynol:

- proses ar gyfer cymeradwyaeth uwch swyddogion
- prosesau clir ar gyfer gweinyddu a monitro'r cyfrifon – gan gynnwys o leiaf dau aelod o staff
- cod ymddygiad ar gyfer defnyddwyr y cyfrifon
- systemau ar gyfer adrodd a delio â cham-drin a chamddefnydd
- dealltwriaeth o sut y gellir ymdrin ag achosion o dan weithdrefnau disgyblu'r ysgol

Defnydd personol

- cyfathrebu personol yw'r cyfathrebu a wneir ar gyfrifon cyfryngau cymdeithasol personol. Ym mhob achos, os defnyddir cyfrif personol sy'n ei gysylltu ei hun â'r ysgol neu sy'n effeithio ar yr ysgol, rhaid datgan yn glir nad yw'r aelod o staff yn cyfathrebu ar ran yr ysgol gydag ymwadiad priodol. Mae cyfathrebu personol o'r fath oddi mewn i gwmpas y polisi hwn
- mae unrhyw gyfathrebu personol nad yw'n cyfeirio at yr ysgol, nac yn effeithio arni, y tu allan i gwmpas y polisi hwn.
- os oes amheuaeth o ddefnydd personol gormodol o gyfryngau cymdeithasol yn yr ysgol, ac os credir bod hynny'n ymyrryd â dyletswyddau perthnasol, efallai y cymerir camau disgyblu.
- mae'r ysgol yn caniatáu mynediad rhesymol a phriodol i safleoedd cyfryngau cymdeithasol preifat

Monitro cyfryngau cymdeithasol cyhoeddus

- Fel rhan o ymwneud â'r cyfryngau cymdeithasol yn gyffredinol, bydd yr ysgol yn monitro'r Rhyngrwyd yn gyson am sylwadau cyhoeddus am yr ysgol.

- gallai'r ysgol ymateb yn effeithiol i sylwadau ar gyfryngau cymdeithasol a wneir gan eraill, yn unol â pholisi neu broses benodol
- pan fydd rhieni/gofalwyr yn mynegi pryderon am yr ysgol ar y cyfryngau cymdeithasol, byddwn yn eu hannog i gysylltu'n uniongyrchol â'r ysgol, yn breifat, i ddatrys y mater. Os nad oes modd datrys hyn, dylid rhoi gwybod i rieni/gofalwyr am drefn gwyno'r ysgol.

Bydd defnydd yr ysgol o gyfryngau cymdeithasol ar gyfer dibenion proffesiynol yn cael ei wirio'n rheolaidd gan uwch arweinydd i sicrhau cydymffurfio â pholisïau cyfryngau cymdeithasol, diogelu data, cyfathrebu, delweddau digidol a fideos. Os nad yw'r ysgol yn gallu datrys unrhyw faterion yn ymwneud â'r cyfryngau cymdeithasol, gellir gofyn am gymorth gan y Llinell Gymorth Diogelwch Ar-lein i Weithwyr Proffesiynol.

Delweddau digidol a fideos

Mae datblygiad technolegau delweddu digidol wedi creu manteision sylweddol wrth addysgu. Maent yn caniatáu i staff a dysgwyr allu defnyddio delweddau y maent wedi eu recordio eu hunain, neu wedi eu lawrlwytho o'r rhyngrwyd, ar unwaith. Ond, mae angen i staff, rhieni/gofalwyr a dysgwyr fod yn ymwybodol o'r peryglon sy'n gysylltiedig â chyhoeddi delweddau digidol ar y rhyngrwyd. Gall y fath ddelweddau arwain at achosion o fwlio ar-lein. Gall delweddau digidol aros ar y rhyngrwyd am byth a gallant achosi niwed neu gywilydd i unigolion yn y tymor byr neu'r tymor hir. Mae'n beth cyffredin i gyflogwyr edrych ar y rhyngrwyd am wybodaeth am ddarpar weithwyr neu weithwyr presennol.

Bydd yr ysgol yn hysbysu ac yn addysgu defnyddwyr ynglŷn â'r peryglon hyn ac yn gweithredu polisïau i leihau'r tebygolrwydd o niwed posib:

- **os yw lleoliad neu ysgol a gynhelir yn dewis defnyddio ffrydio byw neu fideogynadledda, rhaid i gyrff llywodraethol, prifathrawon, a staff ystyried yn llawn y canllawiau a'r polisïau diogelu cenedlaethol a lleol, gan roi sylw i'r arweiniad yn y polisi ffrydio byw.**
- **wrth ddefnyddio delweddau digidol, dylai staff hysbysu ac addysgu'r dysgwyr am y peryglon sy'n gysylltiedig â thynnu lluniau, defnyddio, rhannu, cyhoeddi a dosbarthu delweddau. Yn benodol, dylent adnabod y peryglon sy'n gysylltiedig â chyhoeddi eu delweddau eu hunain ar y rhyngrwyd e.e. ar wefannau rhwydweithio cymdeithasol**
- yn unol ag arweiniad gan Swyddfa'r Comisiynydd Gwybodaeth, mae croeso i rieni/gofalwyr dynnu delweddau digidol/fideo o'u plant yn nigwyddiadau'r ysgol ar gyfer defnydd personol (gan nad yw'r fath ddefnydd yn cael ei grybwyll yn y Ddeddf Diogelu Data). I barchu preifatrwydd pawb, ac er diogelwch mewn rhai achosion, ni ddylid eu cyhoeddi/eu gwneud yn gyhoeddus ar wefannau rhwydweithio cymdeithasol, ac ni ddylai rhieni/gofalwyr wneud sylw ar unrhyw weithgareddau sy'n cynnwys *dysgwyr* eraill yn y delweddau digidol/fideo
- mae gan staff a gwirfoddolwyr hawl i dynnu lluniau digidol/fideo i gefnogi nodau addysgiadol, ond rhaid dilyn polisïau'r ysgol ynglŷn â rhannu, storio, dosbarthu a chyhoeddi'r delweddau hyn. Rhaid i staff/gwirfoddolwyr fod yn ymwybodol o'r dysgwyr hynny na ddylid tynnu eu lluniau na chyhoeddi'r lluniau. Dim ond ar gyfarpar yr ysgol y dylid tynnu'r lluniau hynny. Ni ddylid defnyddio cyfarpar personol y staff i'r fath bwrpas.

- dylid cymryd gofal wrth dynnu delweddau digidol/fideo bod dysgwyr wedi'u gwisgo'n addas ac nad ydynt yn cymryd rhan mewn gweithgareddau a all ddwyn anfri ar yr unigolyn neu'r ysgol
- ni ddylai dysgwyr dynnu lluniau, defnyddio, rhannu, cyhoeddi na dosbarthu delweddau o eraill heb ganiatâd.
- bydd lluniau sy'n cynnwys dysgwyr a gyhoeddir ar y wefan neu yn rhywle arall yn cael eu dewis yn ofalus ac yn cydymffurfio ag arweiniad ar arferion da wrth ddefnyddio delweddau o'r fath.
- ni ddefnyddir enwau llawn dysgwyr ar wefannau nac ar flogiau, yn enwedig rhai sydd wedi'u cysylltu â lluniau
- rhaid cael caniatâd ysgrifenedig gan rieni neu ofalwyr cyn tynnu lluniau o ddysgwyr i'w defnyddio yn yr ysgol neu eu cyhoeddi ar wefan yr ysgol/cyfryngau cymdeithasol.
- bydd delweddau'n cael eu storio'n ddiogel ar rwydwaith yr ysgol yn unol â pholisi cadw'r ysgol
- dim ond gyda chaniatâd y dysgwyr a'r rhieni/gofalwyr y gellir cyhoeddi gwaith dysgwr.

Cyhoeddi ar-lein

Mae'r ysgol wedi ymgynghori â rhieni/gofalwyr a'r gymuned ehangach ac yn hyrwyddo'r ysgol drwy'r dulliau canlynol:

- Gwefan gyhoeddus
- Cyfryngau cymdeithasol
- Cylchlythyron ar-lein
- Arall

Caiff gwefan yr ysgol ei rheoli/lletya gan Elen H Powell a swyddog cynnal yr ysgol. Mae'r ysgol yn sicrhau ei bod yn cadw at arfer da wrth gyhoeddi ar-lein e.e. defnyddio delweddau a fideos digidol, hawlfraint, adnabod pobl ifanc, cyhoeddi calendrau ysgol a gwybodaeth bersonol – ac yn sicrhau nad oes risg i aelodau o gymuned yr ysgol, drwy gyhoeddiadau o'r fath.

Pan fydd gwaith, delweddau neu fideos o ddysgwyr yn cael eu cyhoeddi, ni chyhoeddir eu henwau llawn a diogelir eu manylion adnabod.

Mae cyhoeddiadau ar-lein cyhoeddus yr ysgol yn rhoi gwybodaeth am ddiogelwch ar-lein e.e. cyhoeddi Polisi Diogelwch Ar-lein yr ysgol; casglu'r cyngor a'r arweiniad diweddaraf; erthyglau newyddion ac ati, gan greu tudalen diogelwch ar-lein ar wefan yr ysgol.

Mae'r wefan yn cynnwys proses adrodd ar-lein i rieni a'r gymuned ehangach gofrestru materion a phryderon i ategu'r broses adrodd fewnol

Diogelu Data

Bydd data personol yn cael ei gofnodi, ei brosesu, ei drosglwyddo a'i ryddhau yn unol â'r ddeddfwriaeth diogelu data bresennol.

Mae'r ysgol:

- **yn meddu ar Bolisi Diogelu Data**
- **yn rhoi egwyddorion diogelu data ar waith ac yn gallu dangos hynny**
- **wedi talu'r ffi briodol i Swyddfa'r Comisiynydd Gwybodaeth**
- **wedi penodi Swyddog Diogelu Data priodol sydd â lefel uchel o ddealltwriaeth o'r gyfraith diogelu data, ac yn rhydd o wrthdaro buddiannau.**
- **yn meddu ar 'Gofnod o Weithgareddau Prosesu' ac mae'n gwybod yn union pa ddata personol sydd ganddynt, ym mhle, pam a pha aelod o staff sy'n gyfrifol am ei reoli**
- **mae'r Cofnod o Weithgareddau Prosesu yn rhestru'r sail gyfreithlon dros brosesu data personol (gan gynnwys caniatâd, pan fo hynny'n berthnasol). Pan fydd data categori arbennig yn cael ei brosesu, bydd sail gyfreithlon ychwanegol yn cael ei nodi**
- **yn meddu ar 'gofrestr asedau gwybodaeth' ac mae'n gwybod yn union pa ddata personol a gedwir, ym mhle, pam a pha aelod o staff sy'n gyfrifol am ei reoli**
- **mae'r gofrestr asedau gwybodaeth yn rhestru'r sail gyfreithlon dros brosesu data personol (gan gynnwys caniatâd, pan fo hynny'n berthnasol). Pan fydd data categori arbennig yn cael ei brosesu, bydd sail gyfreithlon ychwanegol yn cael ei nodi hefyd**
- **bydd yn cadw'r data personol sylfaenol sy'n ofynnol er mwyn gallu cyflawni ei swyddogaethau, ac ni fydd yn cadw'r data am gyfnod hwy na'r diben y cafodd ei gasglu ar ei gyfer. Mae 'amserlen cadw' yr ysgol yn cefnogi hyn**
- **mae'r data a gedwir yn gywir ac yn gyfredol ac yn cael ei ddal dim ond at y diben y cafodd ei ddal. Systemau ar waith i adnabod gwallau, megis gofyn i rieni wirio manylion cyswllt mewn argyfwng ar adegau priodol**
- **rhoi'r wybodaeth i staff, rhieni, gwirfoddolwyr, pobl ifanc a phlant hŷn am sut mae'r ysgol yn gofalu am eu data a'u hawliau mewn Hysbysiad Preifatrwydd clir (edrychwch ar adran Hysbysiad Preifatrwydd yr atodiad)**
- **rhaid cael gweithdrefnau i ymdrin â hawliau unigol gwrthrych y data**
- **yn cynnal Asesiadau o'r Effaith ar Ddiogelu Data pan fo angen, e.e. er mwyn sicrhau bod data personol yn cael ei ddiogelu pan fydd yn cael ei gyrchu drwy fynediad o bell, neu pan fydd cysylltiad yn cael ei greu â chyflenwr newydd**
- mae diogelwch y system TG yn cael ei sicrhau a'i brofi'n rheolaidd. Bod patshys a diweddariadau diogelu hanfodol eraill yn cael eu rhoi ar waith yn syth i ddiogelu'r data personol ar y systemau. Dylent wneud yn siŵr bod systemau gweinyddol ar wahân i'r systemau sydd ar gael yn y dosbarth/i ddysgwyr
- **wedi dilyn trefn diwydrwydd dyladwy ac mae'n meddu ar gontractau sy'n cydymffurfio â rheolau diogelu data gydag unrhyw broseswyr data**
- **yn deall sut i rannu data gyda rheolyddion data perthnasol eraill yn gyfreithlon ac yn ddiogel.**
- **yn meddu ar bolisïau a threfn arferol clir ar gael ar gyfer dileu a gwaredu data**
- **Fel ysgol a gynhelir, mae Polisi Rhyddid Gwybodaeth sy'n nodi sut y bydd yn delio â cheisiadau Rhyddid Gwybodaeth.**
- **darparu hyfforddiant ar ddiogelu i'r holl staff yn ystod y cyfnod cynefino a rhoi hyfforddiant gloywi priodol wedi hynny. Hefyd, dylent wneud yn siŵr y bydd y staff sy'n**

ymgymryd â swyddogaethau diogelu data, megis delio â cheisiadau dan hawliau'r unigolyn, yn derbyn hyfforddiant priodol ar gyfer eu swyddogaeth ynghyd â'r hyfforddiant craidd a ddarperir i'r holl staff

Pan gaiff data personol ei storio ar unrhyw ddyfais symudol neu ar gyfryngau y gellir eu tynnu:

- **bydd y data wedi'i amgryptio a'i ddiogelu â chyfrinair.**
- **bydd y ddyfais wedi'i diogelu â chyfrinair.**
- **bydd y ddyfais wedi'i gwarchod drwy feddalwedd gwirio feirysau a drwgwedd cyfredol**
- **bydd data'n cael ei ddileu'n ddiogel oddi ar y ddyfais, yn unol â pholisi'r ysgol (isod) ar ôl ei drosglwyddo neu ar ôl gorffen ei ddefnyddio.**

Mae angen i staff sicrhau eu bod nhw'n gwneud y canlynol:

- **bod yn ofalus bob amser i wneud yn siŵr bod data personol yn cael ei gadw'n ddiogel, gan leihau'r risg o golli neu gamddefnyddio'r data**
- **adnabod achos posibl o fynediad di-awdurdod at ddata, deall yr angen i frysio, a gwybod at bwy yn yr ysgol y dylent riportio achos o'r fath**
- **gwneud yn siŵr eu bod nhw'n gallu helpu gwrthrychau'r data i ddeall eu hawliau a'u bod yn gwybod sut i ddelio â chais ar lafar neu'n ysgrifenedig, ac yn gwybod i bwy y dylai roi gwybod am hynny yn yr ysgol**
- **dim ond defnyddio dyfeisiau symudol wedi'u hamgryptio (gan gynnwys USBs) ar gyfer data personol, yn enwedig pan fo hynny'n ymwneud â phlant**
- **gwneud yn siŵr nad ydynt yn trosglwyddo unrhyw ddata personol ysgol i ddyfeisiau personol**
- **dim ond defnyddio data personol ar gyfrifiaduron a dyfeisiau diogel eraill sydd wedi'u diogelu gan gyfrinair, gan sicrhau eu bod wedi "allgofnodi" ar ddiwedd unrhyw sesiwn pan fyddant yn defnyddio data personol**
- **trosglwyddo data gan ddefnyddio amgryptio, cyfrif e-bost diogel (lle bo hynny'n briodol), a dyfeisiau sydd wedi'u diogelu gan gyfrinair diogel.**

Canlyniadau

Caiff effaith y Polisi a'r arferion Diogelwch Ar-lein ei gwerthuso'n rheolaidd drwy adolygu cofnodion digwyddiadau diogelwch ar-lein; adroddiadau ymddygiad/bwlio; arolygon staff, dysgwyr; rhieni/gofalwyr, a'i hadrodd i'r grwpiau perthnasol:

- ceir trafodaeth broffesiynol gytbwys am y dystiolaeth a gymerwyd o'r adolygiadau/logiau ac effaith gwaith ataliol e.e. addysg, ymwybyddiaeth a hyfforddiant diogelwch ar-lein.
- mae llwybrau wedi'u sefydlu i roi gwybod yn rheolaidd am batrymau canlyniadau a digwyddiadau diogelwch ar-lein i dîm arwain a Llywodraethwyr yr ysgol
- rhoddir gwybod i rieni/gofalwyr am batrymau digwyddiadau diogelwch ar-lein fel rhan o'r gwaith o godi ymwybyddiaeth diogelwch ar-lein yr ysgol.

- mae polisïau a gweithdrefnau diogelwch ar-lein (a rhai cysylltiedig) yn cael eu diweddaru'n rheolaidd mewn ymateb i'r dystiolaeth a gasglwyd o'r adolygiadau/archwiliadau/trafodaeth broffesiynol hyn
- mae'r dystiolaeth o effaith yn cael ei rhannu ag ysgolion eraill, asiantaethau ac ALlau i helpu i sicrhau bod strategaeth diogelwch ar-lein leol gyson ac effeithiol yn cael ei datblygu.

Atodiad

SWGfL sy'n berchen ar hawlfraint y templedi polisi hyn. Caniateir i ysgolion a sefydliadau addysgiadol eraill ddefnyddio'r templedi polisi hyn am ddim er mwyn adolygu a datblygu polisïau. Dylai unrhyw berson neu sefydliad sydd am ddefnyddio'r ddogfen i ddiben arall ofyn am ganiatâd gan SWGfL (onlinesafety@swgfl.org.uk) a chydnabod ei ddefnydd.

Mae pob ymdrech wedi cael ei wneud i sicrhau bod yr wybodaeth yn y ddogfen hon yn gywir ar ddyddiad ei chyhoeddi ym mis Ionawr 2021. Fodd bynnag, ni all SWGfL warantu ei chywirdeb, ac nid yw'n derbyn cyfrifoldeb mewn perthynas â defnyddio'r deunydd.

Contents

This Online Safety Policy outlines the commitment of Ysgol Gymunedol Peniel to safeguard members of our school community online in accordance with principles of open government and with the law. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Ysgol Gymunedol Peniel will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy development, monitoring and review

This Online Safety Policy has been developed by the *[insert group/committee name e.g. Online Safety Group]* made up of: (delete/add as appropriate)

- *headteacher/senior leaders*
- *online safety lead*
- *staff – including teachers/education practitioners/support staff/technical staff*
- *governors*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	***October 2023***
The implementation of this Online Safety Policy will be monitored by:	***Elen H Powell (Headteacher)*** ***Mathew James (Governor)***
Monitoring will take place at regular intervals:	***Autumn term***
The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	***Autumn term***
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	**October 2024**
Should serious online safety incidents take place, the following external persons/agencies should be informed:	**Elen H Powell (Headteacher and designated safeguarding officer)** **Dion Thomas (Deputy safeguarding officer)** **Wyn Evans (Governor with responsibility for safeguarding)** **The school will contact the local authority and PC Cath Williams**

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
    - *learners*
    - *parents and carers*
    - *staff.*

Policy and leadership

Responsibilities

In order to ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals[6] and groups within the school.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[7].
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the Welsh Government and UKCIS document Five key questions for governing bodies to help challenge their school to effectively safeguard their learners. This will be carried out by the whole governing body whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor[8]

---

[6] In a small school some of the roles described may be combined, though it is important to ensure that there is sufficient 'separation of responsibility' should this be the case.

[7] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority HR/other relevant body disciplinary procedures.

[8] It is suggested that the role may be combined with that of the designated governor for safeguarding. In other settings this may be the management committee person for child protection

to include:

- **regular meetings with the Online Safety Lead**
- **regularly receiving (collated and anonymised) reports of online safety incidents**
- **checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)**
- **reporting to relevant *governors group/meeting***

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Lead

The headteacher is the designated safeguarding lead in the school and is responsible for online safety.

The online safety lead will:

- lead the Online Safety Group
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned and embedded
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents[9] and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with (school/local authority) technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings/groups
- liaises with the local authority/relevant body.

Designated Safeguarding Person (DSP)

It is important to emphasise that these online safety issues are safeguarding, not technical issues; the technology provides additional means for safeguarding issues to develop.

[9] The school will need to decide how these incidents will be dealt with and whether the investigation/action will be the responsibility of the online safety lead or another member of staff, e.g. headteacher/senior leader/Designated Safeguarding Person/class teacher/head of year, etc.

The Designated Safeguarding Person should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data (See 'Personal data policy' in the Appendix.)
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

Curriculum Leads

Curriculum Leads will work with the online safety lead to develop a planned and coordinated online safety education programme. This will be provided through:

- a discrete programme
- the Digital Competence Framework
- personal and social education/sex and relationships education
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to *(insert relevant person)* for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the live streaming policy.

- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement (this should include personal devices – where allowed)
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should avoid plagiarism and uphold copyright regulations
- will be expected to know and follow school Online Safety Policy
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc
- *providing opportunities for parents and carers to improve their understanding of online safety through parents'/carers' evenings, newsletters, letters, website, Hwb, learning platform and information about national/local online safety campaigns and literature*

Parents and carers will be encouraged to support the school in:

- *reinforcing the online safety messages provided to learners in school*
- *the use of their children's personal devices in the school (where this is allowed)*

Community users

Community users who access school systems/website/Hwb/learning platforms as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Professional Standards

There is an expectation that national professional standards will be applied to online safety as in other aspects of school life i.e.

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of learning and every opportunity will be taken to extend learners' skills and competence
- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience.
- practitioners are able to reflect on their practice, individually and collectively, against nationally agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they can use digital technologies responsibly, protecting themselves and the school and how they can use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels (to be described)
- is published on the school website.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users.

The Online Safety Policy and appendices define acceptable use at the school. Within the appendices there are acceptable use agreements for:

- learners – differentiated by age. Learners will be introduced to the acceptable use rules at induction, the start of each school year and regularly re-enforced during lessons, assemblies and by posters/splash screens around the school. *Learner groups (to be described) are encouraged to suggest child friendly versions of the rules.*
- staff /volunteer AUAs will be agreed and signed by staff and volunteers
- parent/carer AUAs inform them of the expectations of acceptable use for their children and seek permissions for digital images, the use of cloud systems etc.
- community users that access school digital technology systems will be required to sign an AUA.

The acceptable use agreements will be communicated/re-enforced through: (amend as appropriate)

- student handbook
- staff induction and handbook
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer support.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	N.B. Schools should refer to guidance about dealing with self-generated images/sexting - guidance about dealing with nudes and semi-nudes being shared.					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – read more about this: NCA Cyber Choices Programme					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes: **Schools may wish to add further activities to this list.**	**Staff and other adults**				**Learners**			
	Not allowed	**Allowed**	**Allowed at certain times**	**Allowed for selected staff**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff permission/awarene ss**
Online gaming								
Online shopping/commerce								
File sharing								
Social media								
Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to school								
Use of mobile phones for learning at school								

Use of mobile phones in social time at school								
Taking photos on mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								
Use of personal e-mail in school, or on school network/wi-fi								
Use of school e-mail for personal e-mails								

When using communication technologies the school considers the following as good practice:

- **when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school**
- **any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content.** *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- **staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community**
- **users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication**
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.*

Reporting and responding

The school has in place procedures for identifying and reporting cases, or suspected cases, of online safeguarding issues/incidents and understands that because of our day-to-day contact with children our staff are well placed to observe the outward signs of these issues.

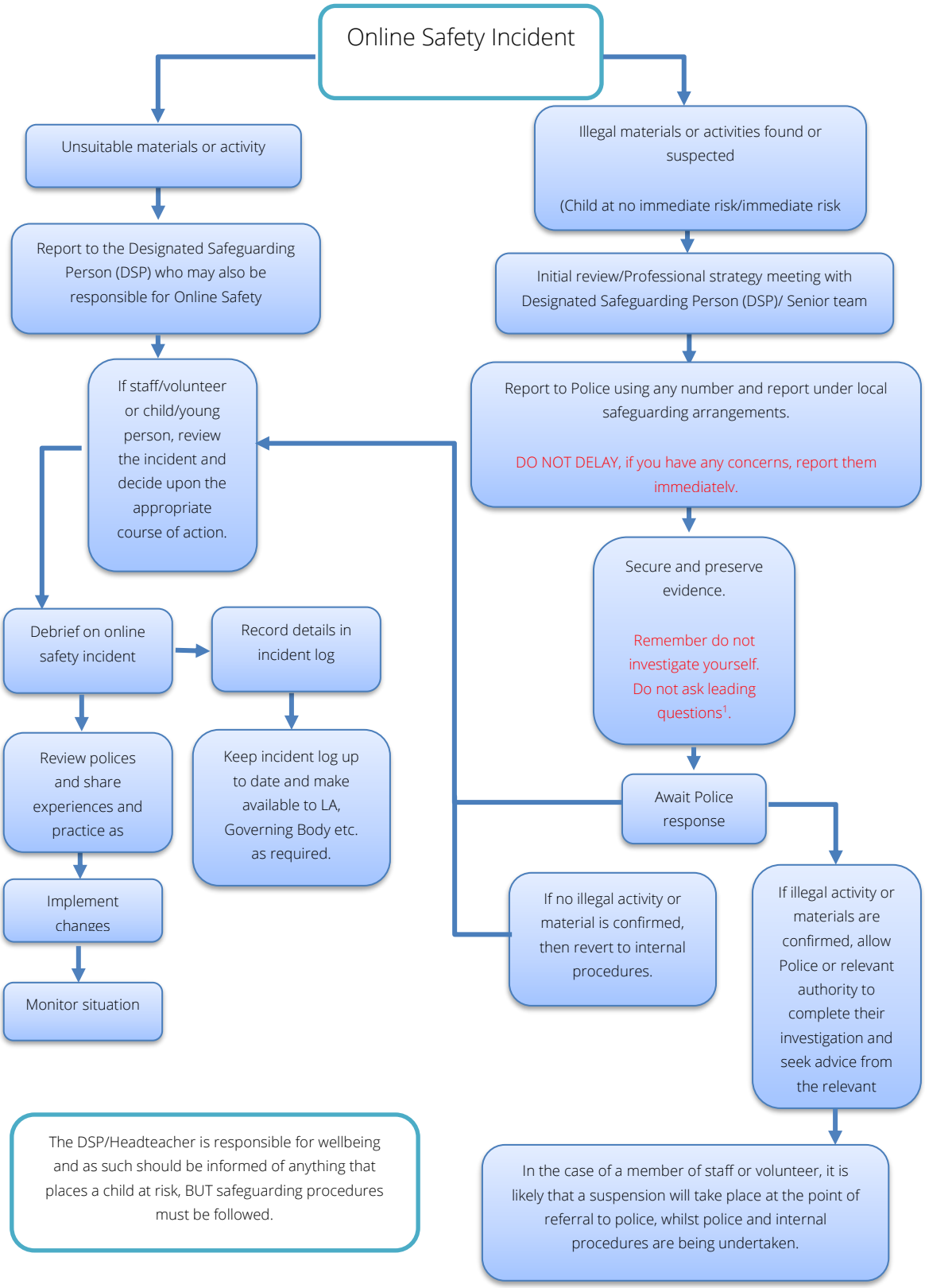
We ensure that every member of staff and every governor knows that they have an individual responsibility for reporting and that they are aware of the need to be alert to signs of abuse and neglect, and know how to respond to a learner who may disclose such issues.

The school will take all reasonable precautions to ensure online safety for all school users, but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- **there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.**
- **all members of the school community will be made aware of the need to immediately report online safety issues/incidents**
- **reports will be dealt with as soon as is practically possible once they are received**
- **the Designated Safeguarding Person, Online Safety Lead and other responsible staff have appropriate skills and training to deal with the various risks related to online safety**
- **if there is any suspicion that the incident involves child abuse images, any other illegal activity or the potential for serious harm** (see flowchart and user actions chart in the appendix), **the incident must be escalated through the normal school safeguarding procedures and the police informed. In these circumstances any device involved should be isolated to support a potential police investigation. In addition to child abuse images such incidents would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials.
- any concern about staff misuse will be reported immediately to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- as long as there is no suspected illegal activity devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated computer that will not be used by learners and if necessary can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same computer for the duration of the procedure.
    - it is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (**except in the case of images of child sexual abuse – see above).**
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority (as relevant)
        - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g. peer support for those reporting or affected by an online safety incident
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP; Keeping safe online on Hwb
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - *local authority/external agencies, as relevant*

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident
Unsuitable materials or activity
Report to the Designated Safeguarding Person (DSP) who may also be responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as
Keep incident log up to date and make available to LA, Governing Body etc. as required.
Implement changes
Monitor situation
Illegal materials or activities found or suspected
(Child at no immediate risk/immediate risk
Initial review/Professional strategy meeting with Designated Safeguarding Person (DSP)/ Senior team
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediatelv.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSP/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Principal Teacher / Deputy Head	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X	X							
Corrupting or destroying the data of other users.		X				X			
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X			
Unauthorised downloading or uploading of files or use of file sharing.	X								
Using proxy sites or other means to subvert the school's filtering system.	X	X	X			X			
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X			X			
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X			X			

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.									
Unauthorised use of digital devices (including taking images)									
Unauthorised use of online services									
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.									
Continued infringements of the above, following previous warnings or sanctions.									

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X				
Deliberate actions to breach data protection or network security rules.								
Deliberately accessing or trying to access offensive or pornographic material.								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.								
Using proxy sites or other means to subvert the school's filtering system.								
Unauthorised downloading or uploading of files or file sharing.								
Breaching copyright or licensing regulations.								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.								
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.								
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers								

Inappropriate personal use of the digital technologies e.g. social media / personal e-mail.								
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner.								
Actions which could compromise the staff member's professional standing.								
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.								
Failing to report incidents whether caused by deliberate or accidental actions.								
Continued infringements of the above, following previous warnings or sanctions.								

Education

Online Safety Education Programme

While regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's safeguarding provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways

- **a planned online safety curriculum across all year groups and a range of subjects, (e.g. DCF/PSE/RSE/Health and Well-being) and topic areas and should be regularly revisited**
- **key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities**
- **it incorporates/makes use of relevant national initiatives and opportunities e.g.** Safer Internet Day **and** Anti-bullying week
- **the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language. Learners considered to be at increased risk online (e.g. children in care, SEND learners, learners experiencing loss or trauma or mental health issues) are provided with targeted or differentiated online safety education**
- **learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information**

- **learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- *learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school*
- *staff should act as good role models in their use of digital technologies the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- *where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit*
- *it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need*
- the online safety education programme will be regularly audited and evaluated to ensure the quality of learning and outcomes.

Contribution of Learners

The school acknowledges, learns from and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of digital leaders*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **a planned programme of formal online safety, cyber security and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.** *It is*

expected that some staff will identify online safety as a training need within the performance management process

- **the training will be an integral part of the school's annual safeguarding and data protection training for all staff**
- **all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours**
- *the Online Safety Lead and Designated Safeguarding Person (or other nominated person) will receive regular updates through attendance at external training events, (e.g. Hwb Keeping safe online training events, from the Regional Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*
- *the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways such as:

- Hwb training – Online safety for governors
- attendance at training provided by the local authority or other relevant organisation (e.g. SWGfL)
- participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor.

Schools should consider providing all governors with a Hwb account in order to use the secure tools and services available e.g. Microsoft Outlook, Teams etc as well as appropriate application training. This would negate the need for governors to use personal email accounts, thereby reducing the risk to data.

Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will seek to provide information and awareness to parents and carers through:

- *regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes*

- *regular opportunities for engagement with parents/carers on online safety issues through awareness workshops/parent/carer evenings etc*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website, learning platform, Hwb*
- *high profile events/campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/publications, e.g. Hwb Keeping safe online, The UK Safer Internet Centre, Childnet International (see Appendix for further links/resources).*
- *Sharing good practice with other schools in clusters and or the local authority*

Adults and Agencies

Drawing on this intelligence, the school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- providing family learning courses in use of new digital technologies and online safety
- online safety messages targeted towards families and relatives.
- the school will provide online safety information via their learning platform, website, and social media for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision (for early years settings please refer to the Online Safety Toolkit for early years practitioners)

The school recognises the support and advice that may be provided by external groups and agencies and values their contribution to school programmes and events.

Filtering

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the Welsh Government Recommended web filtering standards for schools and the UK Safer Internet Centre Appropriate filtering. (The school will need to decide on the merits of external/internal provision of the filtering service – see Appendix).
- internet access is filtered for all users
- illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes (see Appendix for more details).

- there is an appropriate and balanced approach to providing access to online content according to role and/or need
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.

If necessary, the school will seek advice from, and report issues to, the Report Harmful Content site.

Monitoring

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*

Users are made aware, through the acceptable use agreements, that monitoring takes place.
(schools may wish to add details of the monitoring programmes that are used).

Technical Security

School technical systems will be managed in ways that ensures that the school meets recommended technical requirements:

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of copies off-site or in the cloud
- **all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Senior Management team.**
- **all users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details. Sharing of passwords or ID and passwords could lead to an offence under the Computer Misuse Act 1990. Users must immediately report any suspicion or evidence that there has been a breach of security**
- **all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password** by Elen H Powell who will keep an up to date record of users and their usernames.
- **the master account passwords for the school systems are kept in a secure place, e.g. school safe. It is recommended that these are secured using two factor authentication for such accounts** (further guidance is available in the 'Technical security policy template' in the Appendix)

- **passwords should be long. Good practice highlights that passwords over 12 characters in length are more difficult to crack. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length is more secure than any other special requirements such as uppercase/lowercase letters, number and special characters. Users should be encouraged to avoid using sequential or chronological numbers within their passwords. Passwords/passphrases should be easy to remember, but difficult to guess or crack. See the Family guide to cybersecurity for more information.**
- records of learner usernames and passwords for Foundation Phase learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. *Password complexity in foundation phase should be reduced (for example 6 character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged*
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- Elen H Powell is responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- appropriate security measures are in place (schools may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- an agreed policy is in place for the provision of temporary access of 'guests', (e.g. trainee teachers, supply teachers, visitors) onto the school systems
- an agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include:

- security risks in allowing connections to your school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

The school acceptable use agreements for staff, learners, parents and carers outline the expectations around the use of mobile technologies.

The school allows:

	School devices			**Personal devices**		
	School owned for individual use	School owned for multiple users	Authorised device[10]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No[11]	Yes	Yes/No[8]
Full network access	Yes	Yes	Yes			
Internet only						
No network access						

[10] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

[11] The school should add below any specific requirements about the use of mobile/personal devices in school.

School owned/provided devices:

- *to whom they will be allocated*
- *where, when and how their use is allowed – times/places/in/out of school*
- *if personal use is allowed*
- *levels of access to networks/internet (as above)*
- *management of devices/installation of apps/changing of settings/monitoring*
- *network/broadband capacity*
- *technical support*
- *filtering of devices*
- *access to cloud services*
- *use on trips/events away from school*
- *data protection*
- *taking/storage/use of images*
- *exit processes, what happens to devices/software/apps/stored data if user leaves the school*
- *liability for damage*
- *staff training.*

Personal devices

- *which users are allowed to use personal mobile devices in school (staff/learners/visitors)*
- *restrictions on where, when and how they may be used in school*
- *if used in support of learning, how staff will plan their lessons around the potential variety of device models and different operating systems*
- *storage*
- *whether staff will be allowed to use personal devices for school business*
- *data protection*
- *taking/storage/use of images*
- *liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility)*
- *identification/labelling of personal devices*
- *how visitors will be informed about school requirements*
- *how education about the safe and responsible use of mobile devices is included in the school online safety education programmes*
- *how misuse will be dealt with*

Social media

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online. The practitioner's guide to using social media on Hwb provides further information.

Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to follow the professional conduct set out by the General Teaching Council Wales (GTCW) and respect learners, their families, colleagues and the school.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- guidance for learners, parents/carers

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school or local authority
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

When official school social media accounts are established there should be:

- a process for approval by senior leaders
- clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it

must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *the school permits reasonable and appropriate access to private social media sites*

Monitoring of public social media

- As part of active social media engagement, the school will pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Group to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **should a maintained school or setting choose to use live-streaming or video-conferencing, governing bodies, headteachers and staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the live steaming policy.**
- **when using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites**
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own

personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images

- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images. Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes
- care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored on the school network in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters
- Other

The school website is managed/hosted by Elen H Powell and Eleri Waters. The school ensures that good practice has been observed in the use of online publishing e.g. use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is no risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected and full names are *not published.*

The school public online publishing provides information about online safety e.g. publishing the schools Online Safety Policy; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school:

- **has a Data Protection Policy.**
- **implements the data protection principles and is able to demonstrate that it does so**
- **has paid the appropriate fee to the Information Commissioner's Office (ICO)**
- **has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.**
- **has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it**
- **the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed**
- **has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it**
- **information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed**
- **will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this**
- **data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals**
- **provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice** (see Privacy Notice section in the appendix)
- **has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them**
- **carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier**

- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- **has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors**
- **understands how to share data lawfully and safely with other relevant data controllers. In Wales, schools should consider using the Wales Accord on Sharing Personal Information toolkit to support regular data sharing between data controllers**
- **has clear and understood policies and routines for the deletion and disposal of data**
- **reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this it has a policy for reporting, logging, managing, investigating and learning from information risk incidents**
- **As a maintained school, has a Freedom of Information Policy which sets out how it will deal with FOI requests**
- **provides protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff**

When personal data is stored on any mobile device or removable media the:

- **data will be encrypted and password protected.**
- **device will be password protected**. (be sure to select devices that can be protected in this way)
- **device will be protected by up to date virus and malware checking software**
- **data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.**

Staff must ensure that they:

- **at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse**
- **can recognise a possible breach, understand the need for urgency and know who to report it to within the school**
- **can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school**
- **only use encrypted mobile devices (including USBs) for personal data, particularly when it is about children**
- **will not transfer any school personal data to personal devices.** Procedures should be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).

- **use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data**
- **transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.**

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g. online safety education, awareness and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix