



Mae'r polisi hwn yn rhan o Bolisi Diogelu Statudol yr Ysgol. Rhaid i unrhyw faterion a phryderon ynghylch diogelwch ar-lein ddilyn prosesau diogelu ac amddiffyn plant yr ysgol.

Cyflwyniad

Prif nodau ein polisi e-ddiogelwch yw:

Nodi'r egwyddorion allweddol a ddisgwylir gan bob aelod o gymuned Ysgol Gymraeg Melin Gruffydd ynghylch defnyddio technolegau TGCh.

Diogelu ac amddiffyn plant a staff Ysgol Gymraeg Melin Gruffydd.

Cynorthwyo staff ysgol sy'n gweithio gyda phlant i weithio'n ddiogel ac yn gyfrifol gyda'r rhyngrwyd a thechnolegau cyfathrebu eraill ac i fonitro eu safonau a'u harfer eu hunain.

Pennu disgwyliadau clir o ran ymddygiad a/neu godau ymarfer sy'n berthnasol i ddefnydd cyfrifol o'r rhyngrwyd at ddefnydd addysgol, personol neu hamdden.

Sicrhau bod pob aelod o gymuned yr ysgol yn ymwybodol bod ymddygiad anghyreithlon neu annio gel yn annerbyniol ac, lle bo hynny'n briodol, y cymerir camau disgyblu neu gyfreithiol yn eu herbyn.

Lleihau'r risg o honiadau camarweiniol neu faleisus a wneir yn erbyn oedolion sy'n gweithio gyda disgyblion.

Gellir crynhoi'r prif feysydd risg ar gyfer cymuned ein hysgol fel a ganlyn:

Cynnwys

- Dod i gysylltiad â chynnwys amhriodol
- Gwefannau ffordd o fyw sy'n hyrwyddo ymddygiadau niweidiol
- Cynnwys sy'n ymwneud â chasineb
- Dilysu cynnwys: sut i wirio dilysrwydd a chywirdeb cynnwys ar-lein

Cysylltiad

- Gwastrodi (camfanteisio rhywiol, radicaleiddio ac ati)
- Bwllo ar-lein o bob math
- Lladrad hunaniaeth gymdeithasol neu fasnachol, gan gynnwys cyfrineiriau

Ymddygiad

- Ymddygiadau ymosodol (bwlio)
- Materion preifatrwydd, gan gynnwys datgelu gwybodaeth bersonol
- Ôl-troed digidol ac enw da ar-lein
- Iechyd a lles (faint o amser a dreulir ar-lein, gamblu, delwedd y corff)
- Secstio
- Hawlfraint (ychydig o ofal neu ystyriaeth i eiddo a pherchnogaeth ddeallusol)

Ehangder

Mae'r polisi hwn yn berthnasol i gymuned yr ysgol gyfan gan gynnwys Uwch Dîm Arweinyddiaeth Ysgol Gymraeg Melin Gruffydd, bwrdd Llywodraethwyr yr ysgol, yr holl staff a gyflogir yn uniongyrchol neu'n anuniongyrchol gan yr ysgol a'r holl ddisgyblion.

Bydd Uwch Dîm Arweinyddiaeth Ysgol Gymraeg Melin Gruffydd a Bwrdd Llywodraethwyr ysgolion yn sicrhau bod unrhyw ddeddfwriaeth berthnasol neu newydd a allai effeithio ar y ddarpariaeth ar gyfer e-Ddiogelwch yn yr ysgol yn cael ei hadlewyrchu yn y polisi hwn.

Mae Deddf Addysg ac Arolygiadau 2006 yn grymuso penaethiaid, i raddau rhesymol, i reoleiddio ymddygiad myfyrwyr neu ddisgyblion pan fyddant oddi ar safle'r ysgol ac yn grymuso aelodau staff i orfodi cosbau disgynnu am ymddygiad amhriodol.

Mae hyn yn berthnasol i ddigwyddiadau seiberfwlio, neu ddigwyddiadau e-ddiogelwch y mae'r polisi hwn yn ymdrin â hwy, a all ddigwydd y tu allan i'r ysgol, ond sy'n gysylltiedig ag aelodaeth o'r ysgol.

Bydd yr ysgol yn nodi'n glir ei rheolaeth ar ddigwyddiadau o fewn y polisi hwn, ymddygiad cysylltiedig a pholisiau gwrth-fwlio a bydd, lle y gwyddys, yn hysbysu rhieni a gofalwyr am ddigwyddiadau o ymddygiad e-Ddiogelwch amhriodol y tu allan i'r ysgol.

Adolygiad/Perchnogaeth

Cyfeirir at y polisi diogelwch ar-lein o fewn polisiau ysgolion eraill (e.e. polisi Diogelu ac Amddiffyn Plant, polisi Gwrth-fwlio, ABCh).

Mae'r ysgol wedi penodi cydlynnydd e-Ddiogelwch a fydd yn gyfrifol am berchnogaeth dogfennau, eu hadolygu a'u diweddu.

Ysgrifennwyd y polisi e-Ddiogelwch gan Gydlynnydd e-Ddiogelwch yr ysgol ac mae'n gyfredol ac yn briodol ar gyfer ei gynulleidfa a'i bwrpas arfaethedig.

Bydd y polisi diogelwch ar-lein yn cael ei adolygu'n flynyddol neu pan wneir unrhyw newidiadau sylweddol o ran y technolegau a ddefnyddir yn yr ysgol

Mae perchnogaeth eang ar y polisi ac mae'r UDA wedi cytuno arno ac mae'r Llywodraethwyr wedi'i gymeradwyo. Bydd yr holl newidiadau i'r polisi diogelwch ar-lein yr ysgol yn cael eu rhannu i bob aelod o staff a disgblion.

Polisi Cyfathrebu

Credwn mai cyfrifoldeb cymuned gyfan yr ysgol yw e-Ddiogelwch, ac mae gan bawb gyfrifoldeb i sicrhau bod pob aelod o'r gymuned yn gallu elwa o'r cyfleoedd y mae technoleg yn eu darparu ar gyfer dysgu ac addysgu. Mae'r cyfrifoldebau canlynol yn dangos sut y bydd pob aelod o'r gymuned yn cyfrannu.

Bydd y staff/disgblion/y cymuned yn cael eu hysbysu o'r polisi yn y ffyrdd canlynol:

Polisi i'w bostio ar wefan/ystafell athrawon/ystafelloedd dosbarth yr ysgol.

- Polisi i fod yn rhan o'r pecyn sefydlu ysgol ar gyfer staff newydd.
- Diweddariadau a hyfforddiant rheolaidd ar ddiogelwch ar-lein i'r holl staff.
- Trafodir cytundebau defnydd derbyniool gyda'r staff a'r disgblion ar ddechrau pob blwyddyn.
- Cyhoeddi cytundebau defnydd derbyniool i gymuned gyfan yr ysgol, wrth ddod i mewn i'r ysgol.

Rolau a Chyfrifoldebau

Uwch Dîm Arweinyddiaeth

- Y pennath sy'n gyfrifol yn y pen draw am ddarpariaeth e-Ddiogelwch ar gyfer pob aelod o gymuned yr ysgol, er y bydd y cyfrifoldeb o ddydd i ddydd am e-Ddiogelwch yn cael ei ddirprwyo i'r cydlynnydd e-Ddiogelwch.
- Mae'r pennath a'r uwch dîm arweinyddiaeth yn gyfrifol am sicrhau bod y Cydlynnydd e-Ddiogelwch a staff perthnasol eraill yn derbyn hyfforddiant addas i'w galluogi i gyflawni eu rolau diogelwch ar-lein ac i hyfforddi cydweithwyr eraill pan fo angen.
- Bydd y pennath a'r uwch dîm arweinyddiaeth yn sicrhau bod trefniadau yn eu lle sy'n caniatáu monitro a chefnogi'r rhai yn yr ysgol sy'n cyflawni'r rôl monitro

e-Ddiogelwch yn fewnol. Mae'r ddarpariaeth hon yn darparu rhwyd ddiogelwch a hefyd yn cefnogi'r cydweithwyr hynny sy'n ymgymryd â rolau monitro pwysig.

- Bydd yr uwch dîm arweinyddiaeth yn derbyn adroddiadau monitro gan y Cydlynnydd e-Ddiogelwch.
- Dylai'r pennath a'r uwch dîm arweinyddiaeth sicrhau eu bod yn ymwybodol o'r gweithdrefnau i'w dilyn os bydd digwyddiad e-Ddiogelwch difrifol.
- Dylai'r pennath a'r uwch dîm arweinyddiaeth dderbyn adroddiad diweddar u gan y tîm rheoli digwyddiadau

Cyfrifoldebau'r Cydlynnydd e-Ddiogelwch

- Hyrwyddo ymwybyddiaeth ac ymrwymiad i e-Ddiogelwch ledled yr ysgol
- I fod y pwynt cyswllt cyntaf yn yr ysgol ar holl faterion e-Ddiogelwch
- Bod yn gyfrifol o ddydd i ddydd am e-Ddiogelwch yn yr ysgol a chwarae rhan flaenllaw wrth sefydlu ac adolygu polisiau a gweithdrefnau e-Ddiogelwch yr ysgol
- Arwain grŵp neu bwyllgor e-Ddiogelwch yr ysgol
- Cael cyswllt rheolaidd â phwyllgorau e-Ddiogelwch eraill, e.e. yr Awdurdod Lleol, yr Adran Diogelu Lleol
- Cyfathrebu'n rheolaidd â staff technegol yr ysgol (iTeach)
- Cyfathrebu'n rheolaidd â'r llywodraethwr e-Ddiogelwch dynodedig, Mr Denis Pugh
- Cyfathrebu'n rheolaidd â'r uwch dîm arweinyddiaeth
- Creu a chynnal polisiau a gweithdrefnau e-Ddiogelwch
- Datblygu dealltwriaeth o faterion e-Ddiogelwch cyfredol, arweiniad a deddfwriaeth briodol
- Sicrhau bod pob aelod o staff yn derbyn lefel briodol o hyfforddiant mewn materion e-Ddiogelwch
- Sicrhau bod addysg e-Ddiogelwch wedi'i hymgorffori ar draws y cwricwlwm
- Sicrhau bod e-Ddiogelwch yn cael ei hyrwyddo i rieni a gofalwyr
- Monitro ac adrodd ar faterion e-Ddiogelwch i'r uwch dîm arweinyddiaeth fel sy'n briodol
- Sicrhau bod yr holl staff yn ymwybodol o'r gweithdrefnau y mae'n rhaid eu dilyn os bydd digwyddiad e-Ddiogelwch
- Sicrhau bod y cofnod digwyddiadau e-Ddiogelwch yn cael ei ddiweddar u
- Sicrhau bod polisi e-Ddiogelwch yr ysgol yn gyfredol ac yn berthnasol
- Sicrhau bod polisi e-Ddiogelwch yr ysgol yn cael ei adolygu ar amseroedd a drefnir ymlaen llaw
- Sicrhau bod Polisiau Defnydd Derbyniol yr ysgol yn briodol ar gyfer y gynulleidfa a fwriadwyd
- Hyrwyddo i bob aelod o gymuned yr ysgol ddefnydd diogel o'r rhyngrwyd ac unrhyw dechnolegau a ddefnyddir yn yr ysgol

Cyfrifoldebau athrawon a staff cymorth

- Darllen, deall a helpu i hyrwyddo polisiau ac arweiniad e-Ddiogelwch yr ysgol
- Darllen, deall a chadw at Bolisi Defnydd Derbyniol staff yr ysgol
- Rhoi gwybod i'r cydlynnydd e-Ddiogelwch am unrhyw gamddefnydd neu broblem a amheur
- Datblygu a chynnal ymwybyddiaeth o faterion ac arweiniad e-Ddiogelwch cyfredol
- Modelu ymddygiadau diogel a chyfrifol yn y ffordd y maen nhw'n defnyddio technoleg eu hunain
- Sicrhau bod unrhyw gyfathrebu digidol a wneir gyda'r disgyblion yn cael ei wneud yn broffesiynol a dim ond trwy systemau'r ysgol yn unig, BYTH trwy fecanweithiau personol, e.e. e-bost, neges destun, ffonau symudol ac ati.
- Ymgorffori negeseuon e-Ddiogelwch mewn gweithgareddau dysgu ar draws pob maes o'r cwricwlwm.
- Goruchwyliau ac arwain disgyblion yn ofalus wrth gymryd rhan mewn gweithgareddau dysgu sy'n cynnwys technoleg
- Sicrhau bod disgyblion yn gwbl ymwybodol o sgiliau ymchwil ac yn gwbl ymwybodol o faterion cyfreithiol sy'n ymwneud â chynnwys electronig fel deddfau hawlfraint
- Bod yn ymwybodol o faterion e-Ddiogelwch sy'n gysylltiedig â defnyddio ffonau symudol, camerâu a dyfeisiau symudol
- Deall a bod yn ymwybodol o fecanweithiau riportio digwyddiadau sy'n bodoli yn yr ysgol
- Cynnal lefel broffesiynol o ymddygiad wrth ddefnyddio technoleg at ddibenion personol bob amser

Cyfrifoldebau staff technegol (iTeach)

- Darllen, deall, cyfrannu at a helpu i hyrwyddo polisiau a chanllawiau e-Ddiogelwch yr ysgol
- Darllen, deall a chadw at bolisi Defnydd Derbyniol staff yr ysgol · Rhoi gwybod i'r cydgysylltydd e-Ddiogelwch am unrhyw faterion sy'n ymwneud ag e-Ddiogelwch.
- Datblygu a chynnal ymwybyddiaeth o faterion, deddfwriaeth ac arweiniad e-Ddiogelwch cyfredol sy'n berthnasol i'w gwaith
- Cynnal lefel broffesiynol o ymddygiad yn eich defnydd personol o dechnoleg bob amser
- Cefnogi'r ysgol i ddarparu seilwaith technegol diogel i gefnogi dysgu ac addysgu

- Sicrhau bod y fynediad a geir i'r rhwydwaith ysgolion yn un sydd trwy fecanwaith cyfyngedig, awdurdodedig yn unig
- Sicrhau bod darpariaeth yn bodoli ar gyfer canfod camddefnydd ac ymosodiadau maleisus
- Cymryd cyfrifoldeb am ddiogelwch system TGCh yr ysgol
- Cysylltu â'r awdurdod lleol neu'r ymddiriedolaeth a phobl a sefydliadau priodol eraill ar faterion technegol
- Dogfennu'r holl weithdrefnau technegol a'u hadolygu i sicrhau cywirdeb ar gyfnodau priodol
- Cyfyngu pob cyfrif lefel gweinyddwr yn briodol
- Sicrhau bod rheolaethau mynediad yn bodoli i amddiffyn gwybodaeth bersonol a sensitif a gedwir ar ddyfeisiau sy'n eiddo i'r ysgol
- Sicrhau bod rheolaethau mynediad ffisegol priodol yn bodoli i reoli mynediad i systemau gwybodaeth ac offer telathrebu yn yr ysgol
- Sicrhau bod gweithdrefnau wrth gefn priodol yn bodoli fel y gellir adfer gwybodaeth a systemau beirniadol os bydd trychineb
- Sicrhau bod rheolaethau a gweithdrefnau'n bodoli fel bod mynediad at asedau meddalwedd sy'n eiddo i'r ysgol yn gyfyngedig
- Bod yn aelod o'r tîm rheoli digwyddiadau sy'n cyfarfod pob tymor i adolygu digwyddiadau e-Ddiogelwch sydd wedi digwydd yn yr ysgol

Cyfrifoldebau disgylion

- Darllen, deall a chadw at Bolisi Defnydd Derbyniol disgylion yr ysgol
- Helpu a chefnogi'r ysgol i greu polisiau ac arferion e-Ddiogelwch a chadw at unrhyw bolisiau ac arferion y mae'r ysgol yn eu creu
- Gwybod a deall polisiau yr ysgol ar ddefnyddio ffonau symudol, camerâu digidol a dyfeisiau symudol
- Gwybod a deall polisiau'r ysgol o ran seiberfwlio
- Cymryd cyfrifoldeb am ddysgu am fanteision a risgau defnyddio'r rhyngrwyd a thechnolegau eraill yn ddiogel yn yr ysgol ac yn y cartref
- Bod yn gwbl ymwybodol o sgiliau ymchwil ac o faterion cyfreithiol sy'n ymwneud â chynnwys electronig fel deddfau hawlfraint
- Cymryd cyfrifoldeb am ddefnydd diogel a chyfrifol ei gilydd o dechnoleg yn yr ysgol ac yn y cartref, gan gynnwys barnu'r risgau a berir gan y dechnoleg bersonol sy'n eiddo i'r ysgol ac sy'n cael ei defnyddio y tu allan i'r ysgol.
- Sicrhau eu bod yn parchu teimladau, hawliau, gwerthoedd ac eiddo deallusol eraill wrth iddynt ddefnyddio technoleg yn yr ysgol ac yn y cartref
- Deall pa gamau y dylent eu cymryd os ydynt yn teimlo'n bryderus, yn anghyfforddus, yn agored i niwed neu mewn perygl wrth ddefnyddio technoleg yn yr ysgol a gartref, neu os ydynt yn ymwybodol bod hyn yn effeithio ar rywun arall

- Deall pwysigrwydd riportio cam-drin, camddefnyddio neu fynediad at ddeunyddiau amhriodol a bod yn gwbl ymwybodol o drefniadau riportio digwyddiad yr ysgol
- Trafod materion e-Ddiogelwch gyda theulu a ffrindiau mewn ffordd agored a gonest

Cyfrifoldebau rhieni a gofalwyr

- Helpu a chefnogi'r ysgol i hyrwyddo e-Ddiogelwch
- Darllen, deall a hyrwyddo Polisi Defnydd Derbyniol disgylion yr ysgol gyda'u plant
- Cymryd cyfrifoldeb am ddysgu am fanteision a risgau defnyddio'r rhyngrwyd a thechnolegau eraill y mae eu plant yn eu defnyddio yn yr ysgol ac yn y cartref
- Cymryd cyfrifoldeb am eu hymwybyddiaeth a'u dysgu eu hunain mewn perthynas â'r cyfleoedd a'r risgau a berir gan dechnolegau newydd a rhai sy'n dod i'r amlwg
- Trafod pryderon e-Ddiogelwch â'u plant, dangos diddordeb yn y modd y maent yn defnyddio technoleg a'u hannog i ymddwyn yn ddiogel ac yn gyfrifol wrth ddefnyddio technoleg
- Modelu ymddygiadau diogel a chyfrifol yn eu defnydd eu hunain o dechnoleg
- Ymgynghori â'r ysgol os oes ganddynt unrhyw bryderon ynghylch defnydd eu plant o dechnoleg.
- Cytuno i arwyddo cytundeb cartref-ysgol i gefnogi dull yr ysgol o ymdrin â diogelwch ar-lein a pheidio â lanlwytho nac ychwanegu unrhyw ddelweddau, fideos, synau neu destunau a allai beri gofid neu bechu unrhyw aelod o gymuned yr ysgol.
- Cefnogi safbwyt yr ysgol ar ddefnyddio systemau ac offer TGCh.
- Os yw rhiant yn ychwanegu ffotograff o'u plentyn ar gyfryngau cymdeithasol rydym yn argymhell nad oes arwyddluniau'r ysgol yn weladwy i ddiogelu eu plentyn.
- Gofynnir i rieni a gofalwyr ddarllen a llofnodi cytundebau defnydd derbyniol ar ran eu plant wrth gael eu derbyn i'r ysgol.
- Mae'n ofynnol i rieni a gofalwyr roi caniatâd ysgrifenedig i ddefnyddio unrhyw ddelweddau o'u plant mewn amrywiaeth o wahanol amgylchiadau.

Cyfrifoldebau'r corff llywodraethu

- Darllen, deall, cyfrannu at a helpu i hyrwyddo polisiau ac chanllaw e-Ddiogelwch yr ysgol

- Datblygu trosolwg o fuddion a risgiau'r rhyngrywd a thechnolegau cyffredin a ddefnyddir gan ddisgyblion
- Datblygu trosolwg o sut mae seilwaith TGCh ysgolion yn darparu mynediad diogel i'r rhyngrywd
- Datblygu trosolwg o sut mae'r ysgol yn annog disgyblion i fabwysiadu ymddygiadau diogel a chyfrifol wrth ddefnyddio technoleg yn yr ysgol a'r tu allan iddi
- Cefnogi'r gwaith e-Ddiogelwch wrth hyrwyddo a sicrhau defnydd diogel a chyfrifol o dechnoleg yn yr ysgol a'r tu allan iddi, gan gynnwys annog rhieni i gymryd rhan mewn gweithgareddau e-Ddiogelwch.
- Sicrhau bod cyllid ac adnoddau priodol ar gael i'r ysgol weithredu ei strategaeth e-Ddiogelwch

Cyfrifoldebau'r Swyddog Amddiffyn Plant/Swyddog Diogelu

- Deall y materion sy'n ymwneud â rhannu gwybodaeth bersonol neu sensitif
- Deall y peryglon o ran mynediad i gyswilt amhriodol ar-lein gydag oedolion a dieithriaid
- Bod yn ymwybodol o ddigwyddiadau posibl neu wirioneddol yn ymwneud â meithrin perthynas amhriodol â phlant ifanc
- Bod yn ymwybodol o seiberfwlio a'r defnydd o gyfryngau cymdeithasol at y diben hwnnw

Cyfrifoldebau grwpiau allanol eraill

- Bydd yr ysgol yn cysylltu â sefydliadau lleol i sefydlu dull cyffredin o ymdrin ag e-Ddiogelwch a defnyddio technolegau yn ddiogel
- Bydd yr ysgol yn sensitif ac yn dangos empathi i faterion yn ymwneud â'r rhyngrywd y mae disgyblion y tu allan i'r ysgol yn cael profiad ohonynt, e.e. gwefannau rhwydweithio cymdeithasol, ac yn cynnig cyngor priodol lle bo hynny'n briodol
- Bydd unrhyw sefydliadau allanol yn llofnodi Polisi Defnydd Derbyniol cyn defnyddio unrhyw offer neu ryngrywd yr ysgol
- Bydd yr ysgol yn darparu Polisi Defnydd Derbyniol ar gyfer unrhyw westai sydd angen defnyddio system gyfrifiadurol yr ysgol neu'r rhyngrywd ar dir yr ysgol · Bydd yr ysgol yn sicrhau bod lefelau goruchwyliaeth priodol yn bodoli pan fydd sefydliadau allanol yn defnyddio'r rhyngrywd ac offer TGCh yn yr ysgol.

Rheoli Systemau Cynnwys Digidol a Chyfathrebu

Ceir caniatâd ysgrifenedig gan rieni neu ofalwyr ar gyfer y lleoliadau a ganlyn cyn cyhoeddi ffotograffau o ddisgyblion. Gwneir hyn wrth gael eu derbyn i'r ysgol.

- Ar wefan yr ysgol - www.ygmg.cymru
 - Ar gyfrif cyfryngau cymdeithasol yr ysgol - Instagram, Twitter a facebook
 - Ar lwyfannau dysgu'r ysgol - Seesaw (FPh) a Google Classroom (CA2)
 - Ar ap yr ysgol - MySchoolApp
 - Ym mhrosbectws yr ysgol a deunydd hyrwyddo argraffedig arall, e.e. papurau newydd
 - Mewn deunydd arddangos y gellir ei ddefnyddio oddi ar y safle
 - Wedi'i recordio neu ei drosglwyddo ar fideo neu drwy we-gamera mewn cynhadledd addysgol
-
- Gall rhieni a gofalwyr wrthod rhoi caniatâd, yn ysgrifenedig, ar unrhyw adeg.
 - Byddwn yn atgoffa disgyblion o ymddygiadau diogel a chyfrifol wrth greu, defnyddio a storio delweddau digidol, fideo a sain.
 - Byddwn yn atgoffa disgyblion o'r risgiau o ddefnyddio delweddau digidol, fideo a sain yn amhriodol yn eu gweithgareddau ar-lein yn yr ysgol ac yn y cartref.
 - Dim ond i greu delweddau digidol, fideo a sain y bydd disgyblion a staff yn defnyddio offer yr ysgol. Mewn amgylchiadau eithriadol, gellir defnyddio offer personol gyda chaniatâd y penneth ar yr amod bod unrhyw gyfryngau'n cael eu trosglwyddo i ddyfais yr ysgol yn unig a'u dileu o unrhyw ddyfeisiau personol. Yn benodol, ni chymerir delweddau digidol, fideo a sain heb ganiatâd cyfranogwyr; bydd delweddau a fideo o weithgareddau priodol a bydd y cyfranogwyr mewn gwisg briodol; ni fydd enwau llawn cyfranogwyr yn cael eu defnyddio naill ai o fewn yr adnodd ei hun, yn enw'r ffeil nac yn y testun cysylltiedig ar-lein; ni fydd adnoddau o'r fath yn cael eu cyhoeddi ar-lein heb ganiatâd y staff a'r disgyblion dan sylw.
 - Os yw disgyblion yn cymryd rhan, gofynnir am ganiatâd rhieni perthnasol hefyd cyn bod adnoddau cael eu cyhoeddi ar-lein.
 - Wrth chwilio am ddelweddau, clipiau fideo neu sain, bydd rheolau hawlfraint a chydabod perchnogaeth yn cael eu dysgu i'r disgyblion.

Storio delweddau

- Rhaid storio unrhyw ddelweddau, fideos neu glipiau sain o ddisgyblion ar rwydwaith yr ysgol a pheidio byth â'u trosglwyddo i offer personol.

- Bydd yr ysgol yn storio delweddau o ddisgyblion sydd wedi gadael yr ysgol am 2 flynedd ar ôl iddynt adael i'w defnyddio yng ngweithgareddau'r ysgol ac adnoddau hyrwyddo.
- Ni chaniateir i ddisgyblion na staff ddefnyddio cyfryngau cludadwy personol i storio unrhyw ddelweddau, fideos na chlipiau sain o ddisgyblion.

Polisi cyfrinair

Mae gan ddisgyblion y Cyfnod Sylfaen a Chyfnod Allweddol 2 gyfrinair mewngofnodi i holl offer TGCh yr ysgol. Mae'r ysgol yn ei gwneud yn glir bod yn rhaid i staff a disgyblion gadw eu cyfrineiriau'n breifat bob amser, rhaid iddynt beidio eu rhannu ag eraill; os yw cyfrinair yn cael ei gyfaddawdu dylid hysbysu'r pennath neu'r cydlynnydd ar unwaith.

- Mae gan yr holl staff eu henw defnyddiwr unigryw a'u cyfrineiriau preifat eu hunain i gael mynediad at systemau ysgolion. Mae'r staff yn gyfrifol am beidio â datgelu eu cyfrinair(au). Peidiwch a gwneud nodyn o chyfrineiriau'r systemau. Dim ond eu datgelu i staff cymorth TGCh awdurdodedig y dylech ddatgelu eich cyfrinair personol pan fo angen am hynny a nid i unrhyw un arall. Sicrhewch bod yr holl gyfrineiriau personol a ddatgelwyd yn cael eu newid cyn gynted â phosibl. Gwnewch yn siŵr eich bod chi'n nodi'ch cyfrineiriau personol pob tro y byddwch chi'n mewngofnodi . Peidiwch â chynnwys cyfrineiriau mewn unrhyw weithdrefnau mewngofnodi awtomatig. Mae'r ysgol yn cadw cofnod o'r holl fynediad gan ddefnyddwyr a'u gweithgareddau wrth ddefnyddio'r system.
- Rydym yn ei gwneud yn ofynnol i staff ddefnyddio cyfrineiriau CRYF. Dylai cyfrineiriau gynnwys o leiaf wyth nod a dylent fod yn anodd i'w dyfalu ac yn cynnwys rhifau, llythrennau a nodau arbennig. Po fwyaf ar hap yw'r cyfrinair, y mwyaf diogel ydyw. Dylai defnyddwyr greu cyfrineiriau gwahanol ar gyfer gwahanol gyfrifon a chymwysiadau.
- Dylai defnyddwyr newid eu cyfrineiriau pryd bynnag y bydd unrhyw arwydd bod y system neu'r cyfrinair wedi cael ei gyfaddawdu. Rydym yn ei gwneud yn ofynnol i staff newid eu cyfrineiriau ddwywaith y flwyddyn.
- Rydym yn ei gwneud yn ofynnol i staff sy'n defnyddio systemau critigol ddefnyddio dilysiad dau ffactor.

Technolegau Datblygol

Bydd pob technoleg newydd yn cael ei phrofi a'i hadolygu ar gyfer unrhyw wendidau diogelwch a allai fodoli. Bydd gwrthfesurau addas yn cael eu mabwysiadu yn yr ysgol i sicrhau bod unrhyw risgiau'n cael eu rheoli i lefel dderbynol. Cyn defnyddio unrhyw dechnolegau newydd yn yr ysgol, bydd staff a disgyblion yn cael hyfforddiant priodol. Gallai defnyddio systemau cyfrifiadurol heb ganiatâd neu at ddibenion amhriodol fod yn drosedd o dan Ddeddf Camdefnyddio Cyfrifiaduron 1990 a bydd

manylion o dorri'r rheolau yn cael eu hanfon at yr awdurdodau priodol. Bydd dulliau o nodi, asesu a lleihau risgiau yn cael eu hadolygu'n rheolaidd.

Hidlo Mynediad i'r Rhyngrywyd

Mae'r ysgol yn defnyddio gwasanaeth rhyngrywyd wedi'i hidlo. Darperir y system hidlo gan Gyngor Caerdydd gan ddefnyddio Smoothwall ac mae'n cynnwys hidlo sy'n briodol i oedran ac aeddfedrwydd y disgyblion. Os yw defnyddwyr yn darganfod gwefan sydd â chynnwys amhriodol, dylid rhoi gwybod i aelod o staff a fydd yn hysbysu'r Cydlynydd e-Ddiogelu. Bydd pob digwyddiad yn cael ei gofnodi yn y log eSafeguarding. Os yw defnyddwyr yn darganfod gwefan sydd â chynnwys a allai fod yn anghyfreithlon, dylid rhoi gwybod am hyn ar unwaith i'r Cydlynydd e-Ddiogelu. Bydd yr ysgol yn riportio digwyddiadau o'r fath i'r darparwr hidlo - Cyngor Caerdydd. Addysgir disgyblion i asesu cynnwys wrth i'w sgiliau defnyddio'r rhyngrywyd ddatblygu. Bydd y disgyblion yn defnyddio offer sy'n briodol i'w hoedran i ymchwilio i gynnwys rhyngrywyd. Mae gwerthuso deunyddiau cynnwys ar-lein yn rhan o addysgu a dysgu ym mhob pwnc a bydd yn cael ei ystyried yn ofyniad ysgol gyfan ar draws y cwricwlwm.

Awdurdodi Mynediad i'r Rhyngrywyd

Bydd yr holl staff a disgyblion yn cael yr hyfforddiant ymwybyddiaeth priodol ac yn llofnodi'r Polisi Defnydd Derbyniol disgyblion ynghylch mynediad i ryngrywyd yr ysgol. Hysbysir rhieni y bydd disgyblion yn cael mynediad i'r we dan oruchwyliaeth sy'n briodol i'w hoedran a'u gallu. Wrth ystyried mynediad i'r rhyngrywyd i aelodau agored i niwed cymuned yr ysgol (plant sy'n derbyn gofal) bydd yr ysgol yn gwneud penderfyniadau ar sail gwybodaeth flaenorol. Bydd mynediad cyfrifol i ddisgyblion y Cyfnod Sylfaen yn cael ei oruchwyliau'n uniongyrchol gan oedolyn cyfrifol. Bydd disgyblion Cyfnod Allweddol 2 yn cael eu goruchwyliau a'u monitro'n agos yn ystod yr amser y maent yn defnyddio'r rhyngrywyd. Bydd disgyblion yn aml yn cael eu hatgoffa o faterion diogelwch rhyngrywyd a defnydd diogel.

E-bost

- Mae'r ysgol hon yn darparu cyfrif e-bost i staff ar gyfer eu defnydd proffesiynol a dylent fod yn ymwybodol y bydd unrhyw ddefnydd o system e-bost yr ysgol yn cael ei fonitro a'i wirio.
- Rydym yn defnyddio cyfeiriadau e-bost anhysbys neu grŵp, er enghraifft ygmg@ygmg.co.uk

- Byddwn yn cysylltu â'r Heddlu os bydd un o'n staff neu ddisgyblion yn derbyn e-bost yr ydym ni'n ystyried ei fod yn arbennig o annymunol neu sy'n torri'r gyfraith.
- Byddwn yn sicrhau bod cyfrifon e-bost yn cael eu cynnal a'u diweddu
- Ni ddylai staff ddefnyddio cyfrifon e-bost personol yn ystod oriau ysgol nac at ddibenion proffesiynol, yn enwedig i gyfnewid unrhyw wybodaeth neu ddogfennau sy'n gysylltiedig â'r ysgol.
- Er diogelwch defnyddwyr a derbynwyr, caiff pob e-bost ei hidlo a'i logio. Gellir sicrhau bod llwybr olrhain llawn ar gael pe bai angen.
- Dim ond i gyfathrebu â disgyblion a rhieni a gofalwyr y bydd staff yn ddefnyddio cyfrifon e-bost swyddogol a ddarperir gan ysgolion. Ni ddylai staff, o dan unrhyw amgylchiadau, gysylltu â disgyblion, rhieni na chynnal unrhyw fusnes ysgol gan ddefnyddio cyfeiriadau e-bost personol.

Defnyddio e-bost

Dim ond ar y system ysgolion y gall disgyblion ddefnyddio cyfrifon a gymeradwyir gan ysgolion a dim ond dan oruchwyliaeth uniongyrchol athrawon at ddibenion addysgol. Pan yn defnyddio e-bost, atgoffir disgyblion a staff i anfon negeseuon cwrtais a chyfrifol. Rhaid i ddisgyblion beidio â datgelu manylion personol amdanyst eu hunain nac eraill mewn negeseuon e-bost. Dylai'r cyfathrebu rhwng staff a disgyblion neu aelodau o gymuned ehangach yr ysgol fod yn broffesiynol ac yn gysylltiedig â materion ysgol yn unig. Dylid gwirio cyfrifon e-bost staff yn rheolaidd am ohebiaeth newydd. Bydd disgyblion a staff yn cael eu hysbysu o beryglon agor e-bost gan anfonwr neu ffynhonnell anhysbys neu wyliau ac agor atodiadau. Ni ddylai disgyblion a staff byth agor atodiadau o ffynhonnell na ellir ymddiried ynddynt. Dylid rhoi gwybod i aelod o staff ar unwaith os defnyddir system e-bost yr ysgol yn amhriodol neu derbynir negeseuon amhriodol gan ddefnyddiwr arall. Rhaid i ddisgyblion ddweud ar unwaith wrth athro neu oedolyn dibynadwy os ydyn nhw'n derbyn unrhyw e-bost amhriodol neu ymosodol.

Gwefan yr ysgol

Pennaeth yr ysgol sydd gan y cyfrifoldeb cyffredinol am sicrhau bod cynnwys y wefan yn gywir a bod ansawdd y cyflwyniad yn cael ei gynnal. Gwaith yr ysgol ei hun yw'r rhan fwyaf o'r deunydd; lle mae gwaith rhywun arall yn cael ei gyhoeddi neu ei gysylltu ag ef, rydym yn credydu'r ffynonellau a ddefnyddir ac yn nodi hunaniaeth neu statws yr awdur yn glir. Nid oes enwau llawn ynglwm wrth ffotograffau a gyhoeddir ar y we. Nid ydym yn defnyddio enwau disgyblion wrth arbed delweddau yn enwau'r ffeiliau nac yn y tagiau os yn cyhoeddi ar wefan yr ysgol.

Defnyddio blogiau, wicis, podlediadau, rhwydweithiau cymdeithasol a ffyrdd eraill i ddisgyblion gyhoeddi cynnwys ar-lein

Bydd blogio, podledu a chyhoeddi cynnwys ar-lein arall gan ddisgyblion yn digwydd yn yr ysgol a gellir eu cyhoeddi ar wefan yr ysgol. Ni chaniateir i ddisgyblion bostio na chreu cynnwys ar wefannau oni bai bod y wefan wedi'i chymeradwyo gan un o'r

athrawon. Ni fydd disgyblion yn defnyddio eu henw go iawn wrth greu adnoddau sy'n hygrych i'r cyhoedd. Fe'u hanogir i greu llysenw priodol. Addysgir cyhoeddi personol trwy wefannau sy'n briodol i'w hoedran ac sy'n addas at ddibenion addysgol. Anogir staff a disgyblion i fabwysiadu ymddygiadau diogel a chyfrifol tebyg yn eu defnydd personol o flogiau, wicis, gwefannau rhwydweithio cymdeithasol a chyhoeddi ar-lein eraill y tu allan i'r ysgol.

Rhwydweithio cymdeithasol

Staff, Gwirfoddolwyr a Chontractwyr

- Cyfarwyddir staff i gadw cyfathrebu proffesiynol a phreifat ar wahân bob amser.
- Gofynnir i'r athrawon beidio â chynnal mannau rhwydwaith cymdeithasol ar gyfer y disgyblion ar sail bersonol nag i ddefnyddio eu mannau eu hunain ar gyfer eu myfyrwyr, ond yn hytrach, ddefnyddio system ddewisol yr ysgol ar gyfer cyfathrebiadau o'r fath at ddefnydd unrhyw rwydweithio cymdeithasol a gymeradwyir gan yr ysgol ac sy'n glynw at bolisi cyfathrebu'r ysgol.

O ran defnydd preifat, bydd staff yr ysgol yn sicrhau:

- Ni ddylid cyfeirio yn y cyfryngau cymdeithasol at fyfyrwyr/disgyblion, rhieni/gofalwyr na staff yr ysgol;
- Ni ddylai staff ysgol fod yn ffrindiau ar-lein gydag unrhyw ddisgybl/myfyriwr.
- Nid ydynt i gymryd rhan mewn trafodaeth ar-lein ar faterion personol sy'n ymwneud ag aelodau o gymuned yr ysgol;
- Ni ddylid priodoli barn bersonol i'r ysgol na'r awdurdod lleol ac ni ddylai barn bersonol gyfaddawdu ar rôl broffesiynol yr aelod staff, na dwyn anfri ar yr ysgol;
- Mae gosodiadau diogelwch ar broffiliau cyfryngau cymdeithasol personol yn cael eu gwirio'n rheolaidd i leihau'r risg o golli gwybodaeth bersonol.

Disgyblion:

- Yn cael eu dysgu am rwydweithio cymdeithasol, ymddygiadau derbyniol a sut i riportio camddefnydd, bygwth neu gam-drin trwy ein gwaith cwricwlwm diogelwch ar-lein.
- Mae'n ofynnol i fyfyrwyr lofnodi a dilyn ein Cytundeb Defnydd Derbyniol sy'n briodol i'w hoedran.

Rhieni:

- Atgoffir rhieni am risgiau a phrotocolau rhwydweithio cymdeithasol trwy ein Cytundeb Defnydd Derbyniol i rieni a deunyddiau cyfathrebu ychwanegol pan fo angen.

- Rydym yn atgoffa rheini bod angen iddynt ofyn caniatâd cyn lanlwytho ffotograffau, fideos neu unrhyw wybodaeth arall am bobl eraill.

Defnyddio Ffonau Symudol yn yr Ysgol

Defnydd Staff o Ddyfeisiau Personol

Ni fydd ffonau symudol na dyfeisiau personol yn cael eu defnyddio mewn unrhyw ffordd yn ystod gwersi nac yn ystod amser ysgol ffurfiol. Dylent gael eu diffodd neu dro'i'r sŵn i ffwrdd bob amser. Cyfrifoldeb perchenog y ddyfais yw ffonau symudol a dyfeisiau symudol dan berchnogaeth bersonol a ddygir i'r ysgol. Nid yw'r ysgol yn derbyn unrhyw gyfrifoldeb am golli, dwyn neu ddifrodi ffonau symudol neu ddyfeisiau symudol personol. Dylid diffodd swyddogaeth Bluetooth ffôn symudol bob amser ac ni ddylid ei defnyddio i anfon delweddau neu ffeiliau i ffonau symudol eraill. Dim ond yn ystod gwersi y bydd ffonau symudol personol yn cael eu defnyddio gyda chaniatâd ymlaen llaw gan y pennath. Ni ddylid cymryd unrhyw ddelweddau na fideos ar ffonau symudol na dyfeisiau symudol sy'n eiddo personol oni bai bod y pennath yn cael caniatâd ymlaen llaw mewn amgylchiadau eithriadol. Dylid lanlwytho delweddau i weinydd yr ysgol a'u dileu ar unwaith o'r ddyfais bersonol.

Defnydd Disgyblion o Ddyfeisiau Personol

Cynghorir disgyblion (ac eithrio Blwyddyn 6) i beidio â dod â'i ffôn symudol neu ddyfais personol i'r ysgol. Nid yw'r ysgol yn derbyn unrhyw gyfrifoldeb am golli, dwyn neu ddifrodi ffonau symudol neu ddyfeisiau symudol disgyblion. Bydd disgyblion yn cael eu cyfarwyddo i ddefnyddio ffonau symudol a dyfeisiau personol yn ddiogel ac yn briodol a byddant yn ymwybodol o'r rheolau a'r canlyniadau. Os yw disgybl yn torri rheol yr ysgol yna bydd y ffôn neu'r ddyfais yn cael ei atafaelu ac yn cael ei gadw mewn man diogel. Yna bydd ffonau symudol a dyfeisiau yn cael eu trosglwyddo i rieni neu ofalwyr. Os oes angen i ddisgybl gysylltu â'i rieni neu ofalwyr, caniateir iddo ddefnyddio ffôn yr ysgol. Cynghorir rhieni blwyddyn 6 i beidio â chysylltu â'u plentyn trwy eu ffôn symudol yn ystod y diwrnod ysgol, ond i gysylltu â swyddfa'r ysgol.

Defnyddio Gliniaduron/iPads

Mae'r defnydd o liniaduron ac iPads gan yr holl staff wedi'i gyfyngu gan gytundeb defnydd derbyniol sydd wedi'i lofnodi gan staff perthnasol. Rhaid rhoi gliniaduron ac iPads a adewir yn yr ysgol dros nos dan glo. Rhaid peidio â chysylltu iPads â chyfrifon iTunes unigol a rhaid i geisiadau am apiau gael eu gwneud yn ysgrifenedig

i'r cydlynnydd TGCh. Os na all staff fynychu'r gwaith am gyfnod estynedig (dros 2 wythnos) dylid dychwelyd gliniaduron ac iPads i'r ysgol.

Dysgu ac Addysgu

Credwn mai'r ffordd orau i ddatblygu ymddygiadau diogel a chyfrifol ar-lein, nid yn unig i ddisgyblion ond pawb yng nghymuned ein hysgol, yw trwy addysg effeithiol. Rydym yn gwybod bod y rhyngrwyd a thechnolegau eraill wedi'u hymgorffori ym mywydau ein disgyblion, nid yn unig yn yr ysgol ond y tu allan hefyd, a chredwn fod dyletswydd arnom i helpu i baratoi ein disgyblion i elwa'n ddiogel o'r cyfleoedd a ddaw yn sgil y rhyngrwyd.

- Byddwn yn darparu cyfres o wersi penodol sy'n gysylltiedig ag eSafeguarding ym mhob grŵp blwyddyn fel rhan o'r cwricwlwm TGCh/cwricwlwm ABCh/gwersi eraill gan sicrhau y cyflawnir yr amcanion canlynol:

Dosbarthiadau Meithrin/Derbyn

- Defnyddio caledwedd TGCh i ryngweithio â meddalwedd gyfrifiadurol sy'n briodol i'w hoedran.

Blynnyddoedd 1 a 2

- Defnyddio technoleg yn ddiogel ac yn barchus, gan gadw gwybodaeth bersonol yn breifat; nodi ble i fynd am gymorth a chefnogaeth pan fydd ganddynt bryderon am gynnwys neu gyswilt ar y rhyngrwyd neu dechnolegau ar-lein eraill.

CA2

- Defnyddio technolegau chwilio yn effeithiol, dysgu sut mae canlyniadau'n cael eu dewis a'u rhestru a byddwch yn ddetholgar wrth werthuso cynnwys digidol
- Defnyddio technoleg yn ddiogel, yn barchus ac yn gyfrifol; deall ymddygiad derbyniol/annerbyniol; nodi ystod o ffyrdd i riportio pryderon am gynnwys a chyswilt.
- Cymryd rhan mewn Diwrnod Rhyngrwyd Mwy Diogel blynnyddol.
- Byddwn yn trafod, atgoffa neu godi negeseuon e-Ddiogelu perthnasol gyda disgyblion fel mater o drefn lle bynnag y mae cyfleoedd addas yn codi yn ystod pob gwers; gan gynnwys yr angen i amddiffyn gwybodaeth bersonol, ystyried y canlyniadau y gallai eu gweithredoedd eu cael ar eraill, yr angen i wirio cywirdeb a dilysrwydd yr wybodaeth y maent yn ei defnyddio a'r angen i barchu a chyd nabod perchnogaeth deunyddiau digidol.
- Bydd unrhyw ddefnydd o'r rhyngrwyd yn cael ei gynllunio'n ofalus i sicrhau ei fod yn briodol i'w hoedran ac yn cefnogi'r amcanion dysgu ar gyfer meysydd cwricwlwm penodol.
- Bydd disgyblion yn cael eu dysgu sut i ddefnyddio ystod o offer ar-lein sy'n briodol i'w hoedran mewn ffordd ddiogel ac effeithiol.

- Byddwn yn atgoffa disgyblion am eu cyfrifoldebau trwy Bolisi Defnydd Derbyniol defnyddiwr terfynol a fydd yn cael ei rannu gyda phob disgybl a bydd polisi defnyddiwr ar y cyd yn cael ei arddangos pan fydd disgybl yn mewngofnodi i rwydwaith yr ysgol.
- Bydd staff yn dangos ymddygiad diogel a chyfrifol pan yn defnyddio technoleg eu hunain yn ystod gwersi.
- Byddwn yn dysgu disgyblion sut i chwilio am wybodaeth ac i werthuso cynnwys gwefannau am gywirdeb wrth eu defnyddio mewn unrhyw faes cwricwlwm.
- Wrth chwilio'r rhyngrwyd am wybodaeth, bydd disgyblion yn cael eu tywys i ddefnyddio peiriannau chwilio sy'n briodol i'w hoedran. Bydd pob defnydd yn cael ei fonitro a bydd disgyblion yn cael eu hatgoffa o beth i'w wneud os dônt ar draws gynnwys anaddas.
- Bydd pob disgybl yn cael ei ddysgu mewn ffordd sy'n briodol i'w oedran am hawlfraint mewn perthynas ag adnoddau ar-lein ac fe'u dysgir i ddeall am berchnogaeth a phwysigrwydd parchu a chyd nabod hawlfraint deunyddiau a geir ar y rhyngrwyd.
- Bydd disgyblion yn cael eu dysgu am effaith seiberfwlio ac yn gwybod sut i ofyn am gymorth os cânt eu heffeithio gan unrhyw fath o fwlio ar-lein.
- Bydd disgyblion yn ymwybodol o ble i ofyn am gyngor neu help os ydynt yn cael problemau wrth ddefnyddio'r rhyngrwyd a thechnolegau cysylltiedig; h.y. rhiant neu ofalwr, athro neu aelod staff dibynadwy, neu sefydliad fel Childline

Dysgu o Bell

Os bydd rhaid sefydlu swigen ynysu neu gau'r ysgol a bydd angen dysgu o bell, byddwn yn darparu'r canlynol:

- Amrywiaeth eang o fewnbwn/gwersi fyw a ddarperir gan athrawon ac a gefnogir gan Gynorthwywyr Dosbarth trwy Google Meet. Bydd y sesiynau hyn yn cael eu recordio.
- Gosodwch dasgau yn Seesaw neu Google Classroom i'r plant gwblhau ac yna eu cyflwyno er mwyn iddynt gael eu marcio a chael adborth.
- Pan ystyri eu bod yn briodol, bydd plant hefyd yn cyrchu fideos wedi'u recordio ymlaen llaw i arddangos y tasgau penodol a chefnogi eu dysgu.
- Mae mynediad e-ddysgu i e.e. Ed Shed, IDL, Sumdog, CLPA yn darparu gwersi ar-lein ychwanegol
- Darparu deunyddiau ar-lein ychwanegol trwy'r wefan a twitter.
- Sicrhewch fod gennych dudalen ddiogelwch ar y wefan fel arwyddost i ddiogelwch ar-lein.
- Os mai dim ond yr athrawon sy'n hunanynysu ond eu bod yn iach, yna byddant yn trefnu gwersi ar-lein er mwyn cyflwyno mewnbwn gwersi i'w Dosbarth a chynnal cyswllt trwy gydol eu hamser yn hunanynysu.

Hyfforddiant Staff

- Mae ein staff yn derbyn gwybodaeth a hyfforddiant rheolaidd ar faterion e-Ddiogelwch ar ffurf diweddaradau blynnyddol/cyfarfodydd staff pob tymor, DPP ac e-byst gan y cydlynnydd e Diogelwch, fel sy'n briodol.
- Fel rhan o'r broses sefydlu mae'r holl staff newydd yn derbyn gwybodaeth ac arweiniad ar y polisi e-Ddiogelwch a Pholisïau Defnydd Derbyniol yr ysgol.
- Bydd yr holl staff yn cael gwybod am gyfrifoldebau unigol sy'n ymwneud â diogelu plant yng nghyd-destun e-Ddiogelwch ac yn gwybod beth i'w wneud os bydd unrhyw aelod o gymuned yr ysgol yn camddefnyddio technoleg.

Digwyddiadau

- Bydd yr ysgol yn cymryd pob rhagofal rhesymol i sicrhau diogelwch ar-lein.
- Rhoddir gwybodaeth i staff a disgyblion am droseddau defnydd a'r cosbau possibl.
- Y Cydlynnydd E-Ddiogelwch a'r pennath yw'r prif bwyntiau cyswllt ar gyfer unrhyw ddigwyddiad.
- Mae'r pennath a'r Cydlynnydd e-Ddiogelwch yn cael gwybod am unrhyw risg neu dorri rheol ar-lein a amheur
- Cyfeirir unrhyw bryder yngylch staff yn camddefnyddio'r offer yn uniongyrchol i'r pennath bob tro , oni bai bod y pryder yn ymwneud â'r pennath ac os felly cyfeirir y gwyn at Gadeirydd y Llywodraethwyr

Diogelu Data a Diogelwch Gwybodaeth

Bydd data personol yn cael ei gofnodi, ei brosesu, ei drosglwyddo ac ar gael yn unol â Deddf Diogelu Data 2018. Mae'r ysgol wedi defnyddio rheolaethau technegol priodol i leihau'r risg o golli data neu dorri rheolau. Dylai defnyddwyr fod yn wyliadwrus wrth gyrchu gwybodaeth sensitif neu bersonol ar y sgrin i sicrhau na all unrhyw un arall, a allai fod yn anawdurdodedig, ddarllen yr wybodaeth. Dylid rheoli pob mynediad at systemau gwybodaeth trwy gyfrinair cymhleth addas. Ni fydd staff a disgyblion yn gadael dogfennau printiedig personol a sensitif ar argraffwyr o fewn mannau cyhoeddus yr ysgol. Bydd yr holl wybodaeth ffisegol yn cael ei storio mewn ardaloedd mynediad rheoledig. Dylid sicrhau pob cyfathrebiad sy'n cynnwys gwybodaeth bersonol neu sensitif (e-bost, ffacs neu bost) yn briodol. Sicrheir yr holl wybodaeth bersonol a sensitif a gymerir oddi ar y safle trwy reolaethau technegol priodol.

e.e. gliniaduron wedi'u hamgryptio neu yriannau caled wedi'u hamgryptio. Sicrheir dyfeisiau a gymerir oddi ar y safle, e.e. gliniaduron, llechi, ac ati, yn unol â gweithdrefnau trin gwybodaeth yr ysgol ac, er enghraifft, ni chânt eu gadael mewn ceir na lleoliadau nad ydynt yn ddiogel.

Rheoli Asedau

Bydd manylion yr holl galedwedd sy'n eiddo i'r ysgol yn cael eu cofnodi mewn rhestr caledwedd. Bydd yr holl offer TGCh diangen yn cael ei waredu trwy asiantaeth awdurdodedig a bydd y storfa ar offer TGCh sydd o bosibl â data personol arno yn cael ei ddinistrio'n heb unrhyw fodd o'i adfer.



This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Introduction

The main aims of our e-safety police are:

To set out the key principles expected of all members of the school community at Ysgol Gymraeg Melin Gruffydd with respect to the use of ICT-based technologies.

To safeguard and protect the children and staff of Ysgol Gymraeg Melin Gruffydd.

To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.

To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to the whole school community including Ysgol Gymraeg Melin Gruffydd's Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all pupils.

Ysgol Gymraeg Melin Gruffydd's Senior Leadership Team and school Board of Governors will ensure that any relevant or new legislation that may impact upon the provision for e-Safety within school will be reflected within this policy.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students or pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyberbullying, or other e-Safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate e-Safety behaviour that takes place out of school.

Review/Ownership

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSE).

The school has appointed an e-Safety coordinator who will be responsible for document ownership, review and updates.

The e-Safety policy has been written by the school e-Safety Coordinator and is current and appropriate for its intended audience and purpose.

The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school

There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Communication Policy

We believe that e-Safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The policy will be communicated to staff/pupils/community in the following ways:

Policy to be posted on the school website/ staffroom/ classrooms.

- Policy to be part of the school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year.
- Acceptable use agreements to be issued to the whole school community, on entry to the school.

Roles & Responsibilities

Senior Leadership Team

- The headteacher is ultimately responsible for e-Safety provision for all members of the school community, though the day-to-day responsibility for e-Safety will be delegated to the e-Safety coordinator.
- The headteacher and senior leadership team are responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues when necessary.
- The headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role. This provision provides a

safety net and also supports those colleagues who take on important monitoring roles.

- The senior leadership team will receive monitoring reports from the e-Safety Coordinator.
- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious e-Safety incident.
- The headteacher and senior leadership team should receive update report from the incident management team

Responsibilities of the e-Safety Coordinator

- To promote an awareness and commitment to e-Safety throughout the school
- To be the first point of contact in school on all e-Safety matters
- To take day-to-day responsibility for e-Safety within school and to have a leading role in establishing and reviewing the school e-Safety policies and procedures
- To lead the school e-Safety group or committee
- To have regular contact with other e-Safety committees, e.g. the Local Authority, Local Safeguarding Department
- To communicate regularly with school technical staff (iTeach)
- To communicate regularly with the designated e-Safety governor, Mr Denis Pugh
- To communicate regularly with the senior leadership team
- To create and maintain e-Safety policies and procedures
- To develop an understanding of current e-Safety issues, guidance and appropriate legislation
- To ensure that all members of staff receive an appropriate level of training in e-Safety issues
- To ensure that e-Safety education is embedded across the curriculum
- To ensure that e-Safety is promoted to parents and carers
- To monitor and report on e-Safety issues to the senior leadership team as appropriate
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
- To ensure that an e-Safety incident log is kept up to date
- To ensure that the school e-Safety policy is current and pertinent
- To ensure that the school e-Safety policy is reviewed at prearranged time intervals
- To ensure that school Acceptable Use Policies are appropriate for the intended audience
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school

Responsibilities of teachers and support staff

- To read, understand and help promote the school's e-Safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the e-Safety coordinator
- To develop and maintain an awareness of current e-Safety issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed e-Safety messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of e-Safety issues related to the use of mobile phones, cameras and mobile devices
- To understand and be aware of incident-reporting mechanisms that exist within the school
- To maintain a professional level of conduct in personal use of technology at all times

Responsibilities of technical staff (iTeach)

- To read, understand, contribute to and help promote the school's e-Safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any e-Safety related issues that come to your attention to the e Safety coordinator.
- To develop and maintain an awareness of current e-Safety issues, legislation and guidance relevant to their work
- To maintain a professional level of conduct in your personal use of technology at all times
- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the school ICT system

- To liaise with the local authority or trust and other appropriate people and organisations on technical issues
- To document all technical procedures and review them for accuracy at appropriate intervals
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school

- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted
- To be a member of the incident-management team that meets termly to review e-Safety incidents that have occurred within school

Responsibilities of pupils

- To read, understand and adhere to the school pupil Acceptable Use Policy
- To help and support the school in the creation of e-Safety policies and practices and to adhere to any policies and practices the school creates
- To know and understand school policies on the use of mobile phones, digital cameras and mobile devices
- To know and understand school policies regarding cyberbullying
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school
- To discuss e-Safety issues with family and friends in an open and honest way

Responsibilities of parents and carers

- To help and support the school in promoting e-Safety
- To read, understand and promote the school pupil Acceptable Use Policy with their children
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- To discuss e-Safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology.
- To agree to sign a home-school agreement to support the school approach to online safety and not deliberately upload or add any images, videos, sounds or texts that could upset or offend any member of the school community.
- To support the school's stance on the use of ICT and ICT equipment.
- If a parent adds a photograph of their child onto social media we recommend that they do not have the school emblems visible to safeguard their child.
- Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school.
- Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances.

Responsibilities of the governing body

- To read, understand, contribute to and help promote the school's e-Safety policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- To support the e-Safety work in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-Safety activities
- To ensure appropriate funding and resources are available for the school to implement its e-Safety strategy

Responsibilities of the Child Protection Officer/Safeguarding Officer

- To understand the issues surrounding the sharing of personal or sensitive information
- To understand the dangers regarding access to inappropriate online contact with adults and strangers
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyberbullying and the use of social media for this purpose

Responsibilities of other external groups

- The school will liaise with local organisations to establish a common approach to e-Safety and the safe use of technologies
- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice where appropriate
- Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds · The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school

Managing Digital Content and Communication Systems

Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done on entry to the school.

- On the school website - www.ygmg.cymru
- On the school social media account - Instagram, Twitter and facebook
- On the school's learning platforms - Seesaw (FPh) and Google Classroom (KS2)
- On the school app - MySchoolApp
- In the school prospectus and other printed promotional material, e.g. newspapers
- In display material that may be used off site
- Recorded or transmitted on a video or via webcam in an educational conference

- Parents and carers may withdraw permission, in writing, at any time.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- The school will store images of pupils that have left the school for 2 years following their departure for use in school activities and promotional resources.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.

Password policy

Foundation Phase and KS2 pupils have a class logon to all school ICT equipment. The school makes it clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised the headteacher or coordinator should be notified immediately.

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private. • Do not write down system passwords. Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible. Make sure you enter your personal passwords each time

you login. Do not include passwords in any automated logon procedures. The school maintains a log of all accesses by users and of their activities while using the system.

- We require staff to use STRONG passwords. Passwords should contain a minimum of eight characters and be difficult to guess with numbers, letters and special characters in their passwords. The more randomly they are placed, the more secure they are. Users should create different passwords for different accounts and applications.
- Users should change their passwords whenever there is any indication of possible system or password compromise. We require staff to change their passwords twice a year.
- We require staff using critical systems to use two factor authentication.

Emerging Technologies

All new technologies will be tested and reviewed for any security vulnerabilities that may exist. Suitable countermeasures will be adopted within school to ensure that any risks are managed to an acceptable level. Prior to deploying any new technologies within school, staff and pupils will have appropriate training. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities. Methods to identify, assess and minimise risks will be reviewed regularly.

Filtering Internet Access

The school uses a filtered internet service. The filtering system is provided through Cardiff Council using Smoothwall and includes filtering appropriate to the age and maturity of the pupils. If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the e-Safeguarding Coordinator. All incidents will be documented in the eSafeguarding log. If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding Coordinator. The school will report such incidents to the filtering provider - Cardiff Council. Pupils will be taught to assess content as their internet usage skills develop. Pupils will use age-appropriate tools to research internet content. The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Internet Access Authorisations

All staff and pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy regarding internet access within school. Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability. When considering internet access for vulnerable members of the school community (looked after children) the school will make decisions based on prior knowledge. Foundation Phase pupils' internet access will be directly supervised by a responsible adult. Key Stage 2 pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

E-mail

- This school provides staff with an email account for their professional use and should be aware that any use of the school email system will be monitored and checked.
- We use anonymous or group e-mail addresses, for example ygmg@ygmg.co.uk
- We will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- We will ensure that email accounts are maintained and up to date
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.
- Staff will only use official school-provided email accounts to communicate with pupils and parents and carers. Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

Email usage

Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes. Pupils and staff will be reminded when using email about the need to send polite and responsible messages. Pupils must not reveal personal details of themselves or others in email communications. Communication between staff and pupils or members of the wider school community should be professional and related to school matters only. Staff email accounts should be checked regularly for new correspondence. Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments. Pupils and staff should never open attachments from an untrusted source. Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately. Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.

School website

The headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status. Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Using blogs, wikis, podcasts, social networking and other ways for pupils to publish content online

Blogging, podcasting and other publishing of online content by pupils will take place within school and may be published on the school's website. Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff. Pupils will not use their real name when creating publicly-accessible resources. They will be encouraged to create an appropriate nickname. Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications for the use of any school approved social networking will adhere to school's communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student.
- 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 and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our age appropriate pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

Mobile Phone Usage in School

Staff Use of Personal Devices

Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or on silent at all times. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices. The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones. Personal mobile phones will only be used during lessons with prior permission from the headteacher in exceptional circumstances. No images or videos should be taken on mobile phones or personally-owned mobile devices unless a prior permission is given from the headteacher in exceptional circumstances. Images should be uploaded to the school server and deleted instantly from the personal device.

Pupils' Use of Personal Devices

Pupils (except Year 6) are advised not to bring his or her mobile phone or personally-owned device into school. The school accepts no responsibility for the loss, theft or damage of pupils' mobile phones or mobile devices. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences. If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will then be released to parents or carers. If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Year 6 parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Use of Laptops/iPads

The use of laptops and iPads by all staff is restricted by an acceptable use agreement which is signed by relevant staff. Laptops and iPads left in school overnight must be locked away. iPads must not be connected to individual iTunes accounts and requests for apps must be in writing to the ICT coordinator. If staff are unable to attend work for an extended period (over 2 weeks) laptops and iPads should be returned to school.

Teaching & Learning

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide a series of specific eSafeguarding-related lessons in every year group as part of the ICT curriculum / PSE curriculum / other lessons ensuring the following objectives are met:

Nursery/Reception classes

- Use ICT hardware to interact with age-appropriate computer software.

Years 1 and 2

- Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

KS2

- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- Use technology safely, respectfully and responsibly; recognize acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.
- Take part in Safer Internet Day each year.
- We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.

- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which will be shared with every pupil and a collective user policy will be displayed when a pupil logs on to the school network.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline

Remote Learning

In the event of a bubble isolation or school closure, where remote learning will be required, we will provide the following:

- A wide range of live input/lesson delivered by teachers and supported by TAs via Google Meet. These sessions will be recorded.
- Set tasks via Seesaw or Google Classroom for the children to complete and submit for marking and feedback.
- Where deemed appropriate, children will also access pre-recorded videos to demonstrate the set tasks and support their learning.
- E-learning access to e.g. Ed Shed, IDL, Sumdog, CLPA provide additional online lessons
- Provide additional online materials via the website and twitter.
- Have a safety page on the website to signpost online safety.
- If the teachers are just isolating but are well, then they will arrange online lessons to deliver the input of a lesson to their Class and maintain contact throughout their isolation time.

Staff Training

- Our staff receive regular information and training on e-Safety issues in the form of annual updates/ termly staff meetings, CPD and emails from the e Safety coordinator, as appropriate.
- As part of the induction process all new staff receive information and guidance on the e-Safety policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

Incidents

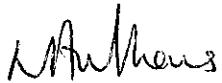
- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- E-Safety Coordinator and headteacher act as the first point of contact for any incident.
- Any suspected online risk or infringement is reported to the headteacher and e-Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the headteacher, unless the concern is about the headteacher in which case the complaint is referred to the Chair of Governors

Data Protection and Information Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. The school has deployed appropriate technical controls to minimise the risk of data loss or breaches. Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information. All access to information systems should be controlled via a suitably complex password. Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school. All physical information will be stored in controlled access areas. All communications involving personal or sensitive information (email, fax or post) should be appropriately secured. All personal and sensitive information taken off site will be secured through appropriate technical controls, e.g. encrypted laptops or encrypted hard-drives. Devices taken off site, e.g. laptops, tablets, etc, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Management of Assets

Details of all school-owned hardware will be recorded in a hardware inventory. All redundant ICT equipment will be disposed of through an authorised agency and ICT equipment that may have held personal data will have the storage media irretrievably destroyed.

Chair of governors: 

Date: 10 May 2021