Polisi E-diolgelwch

Mabwysiadwyd gan y Corff Llywodraethol :

Llofnod y Cadeirydd: …… Dyddiad: ……

Llofnod y Pennaeth: …….…….. Dyddiad: ……

Dyddiad Adolygu: ……

Polisi E-ddiogelwch

1 Cefndir

Mae technolegau newydd wedi dod yn rhan hanfodol o fywydau plant a phobl ifanc yng nghymdeithas heddiw, o fewn ysgolion ac yn eu bywydau y tu allan i'r ysgol.

Mae'r rhyngrwyd a thechnoleg digidol a gwybodaeth arall yn arfau grymus, sy'n cynnig cyfleoedd newydd i bawb. Mae cyfathrebu electronaidd yn helpu athrawon a disgyblion ddysgu oddi wrth ei gilydd. Gall y technolegau hyn gychwyn trafodaeth, hyrwyddo creadigrwydd a chynyddu ymwybyddiaeth o gyd-destun hyrwyddo dysgu effeithiol. Dylai plant a phobl ifanc gael yr hawl i ryngrwyd diogel bob amser.

Mae'r anghenraid i blant a phobl ifanc allu defnyddio'r rhyngrwyd a thechnoleg cyfathrebu cysylltiedig yn briodol a diogel ac yn cael ei drin fel rhan o ddyletswydd gofal ehangach ac mae pawb sy'n gweithio mewn ysgolion wedi'i rwymo iddo.

Fel gyda risg arall, mae'n amhosibl cael gwared llwyr o risg. Felly mae'n hanfodol trwy, ddarpariaeth addysgol dda, i ddatblygu gwytnwch disgyblion i'r peryglon y gallant eu hwynebu, fel bod ganddynt yr hyder a'r sgiliau i wynebu a thrin y risg.

2 Sgôp y Polisi

Mae'r polisi yn berthnasol i bob aelod o gymdeithas yr ysgol (gan gynnwys staff, disgyblion, gwirfoddolwyr, rhieni / gofalwyr, ymwelwyr, defnyddwyr o'r ardal) sy'n cael mynediad i ac yn ddefnyddwyr systemau TGCh yr ysgol, y tu mewn a'r tu allan i'r ysgol.

3 Swyddogaethau a Chyfrifoldebau

3.1 Corff Llywodraethol

Mae **llywodraethwyr** yn gyfrifol am gymeradwyo'r polisi e-ddiogelwch ac adolygu effeithioldeb y polisi.

3.2 Pennaeth

Mae'r **Pennaeth** yn gyfrifol am sicrhau diogelwch (gan gynnwys e-ddiogelwch) aelodau'r ysgol, bydd cyfrifoldeb dyddiol am e-ddiogelwch yn cael ei ddatganoli i'r cydlynydd/swyddog e-ddiogelwch.

3.3 Cydlynydd e-ddiogelwch:

Mae'r cydlynydd e-ddiogelwch yn:

- cymryd cyfrifoldeb dyddiol am faterion e-ddiogelwch gyda rhan flaenllaw mewn sefydlu ac adolygu polisïau / dogfennau e-ddiogelwch yr ysgol
- sicrhau bod yr holl staff yn ymwybodol o'r drefn sydd angen ei dilyn os bydd digwyddiad e-ddiogelwch
- darparu/trefnu hyfforddiant a chyngor i staff
- derbyn adroddiadau ar ddigwyddiadau e-ddiogelwch a chreu log o ddigwyddiadau er cyfrannu i ddatblygiadau e-ddiogelwch y dyfodol, *(ceir esiamplau o daflenni log addas ar y rhyngrwyd addysg)*
- rhoi adroddiad rheolaidd i'r tîm arwain uwch/llywodraethwyr

3.4. Athrawon a Staff Cefnogi

Mae athrawon a staff cefnogi yn gyfrifol am sicrhau:

- **bod ganddynt ymwybyddiaeth gyfredol o faterion e-ddiogelwch a pholisi ac ymarfer e-ddiogelwch cyfredol yr ysgol**
- **wedi darllen, deall a llofnodi Cytundeb Defnydd Derbyniol Staff yr ysgol (CDD)**
- **eu bod yn hysbysu'r Cydlynydd E-ddiogelwch o unrhyw gam ddefnydd a amheuir neu broblem**
- bod materion e-ddiogelwch wedi'u gwreiddio ymhob agwedd o'r cwricwlwm a gweithgareddau ysgol eraill
- bod disgyblion yn deall a dilyn y polisi e-ddiogelwch a defnydd derbyniol
- eu bod yn cadw golwg ar weithgaredd TGC mewn gwersi, gweithgareddau ysgol, allgwricwlaidd ac estynedig
- eu bod yn ymwybodol o faterion e-ddiogelwch yn ymwneud â defnyddio ffôn symudol, camerâu a dyfeisiadau sy'n cael eu dal yn y llaw a'u bod yn cadw golwg ar eu defnydd ac yn gweithredu polisiau ysgol cyfredol parthed y dyfeisiadau hyn
- mewn gwersi ble mae defnydd o'r rhyngrwyd wedi'i rag gynllunio bydd disgyblion yn cael eu harwain i safleoedd a archwiliwyd yn addas i'w defnyddio a bod prosesau yn eu lle i drin unrhyw ddeunydd anaddas a ganfyddir wrth chwilio'r rhyngrwyd.

3.5 Disgyblion

Mae disgyblion yn gyfrifol am ddefnyddio systemau TGCh yn unol â Chytundeb Defnydd Derbyniol ar gyfer disgyblion, a disgwylir i rieni/gofalwyr drafod y cytundeb gyda'i plant a'i lofnodi cyn cael defnyddio systemau'r ysgol.

4 Addysg a Hyfforddiant

4.1 Disgyblion

Mae addysg disgyblion mewn e-ddiogelwch yn rhan hanfodol o ddarpariaeth e-ddiogelwch yr ysgol. Bydd gan ddisgyblion angen help a chefnogaeth yr ysgol i adnabod ac osgoi risg e-ddiogelwch ac adeiladu eu gwytnwch. Bydd addysg e-ddiogelwch yn cael ei ddarparu yn y ffyrdd canlynol: *(addasu ar gyfer eich sefyllfa)*

- **Bydd rhaglen e-ddiogelwch gael ei darparu fel rhan o TGCh / ABCh / gwersi eraill a dylid ail edrych arno'n rheolaidd - bydd hyn yn cynnwys y defnydd o TGCh a thechnoleg newydd yn a thu allan i'r ysgol**
- **Bydd negeseuon allweddol e-ddiogelwch yn cael eu hatgyfnerthu fel rhan o raglen wedi'i chynllunio o wasanaethau, tiwtorial / gweithgareddau bugeiliol**
- **Dylid addysgu disgyblion i fod ymwybodol ymhob gwers o'r deunydd / cynnwys maent yn ei weld ar lein a chael eu harwain at ddilysu cywirdeb yr wybodaeth**
- Dylid helpu disgyblion ddeall y CDD disgyblion a'u hannog i fabwysiadu defnydd diogel a chyfrifol o TGCh, y rhyngrwyd a dyfeisiadau symudol o fewn a thu allan i'r ysgol
- Dylid addysgu disgyblion i gydnabod ffynhonnell yr wybodaeth a defnyddir a pharchu hawlfraint wrth ddefnyddio deunydd a gafwyd ar y rhyngrwyd
- Bydd rheolau ar ddefnyddio systemau TGCh /rhyngrwyd yn cael eu harddangos ymhob ystafell
- Dylai staff weithredu fel esiamplau da wrth ddefnyddio TGCh, y rhyngrwyd a dyfeisiadau symudol

4.2 Rhieni/gofalwyr

Nid oes gan lawer o rieni a gofalwyr ond dealltwriaeth gyfyng o beryglon a phroblemau e-ddiogelwch, ond maent yn chwarae rhan hanfodol yn addysg eu plant wrth gadw golwg / rheoli profiad ar lein eu plant. Yn aml nid yw rhieni yn llawn sylweddoli pa mor aml mae plant a phobl ifanc yn dod ar draws deunydd niweidiol posibl ac amhriodol ar y rhyngrwyd ac yn aml yn ansicr beth i wneud yn ei gylch. "Mae rhaniad digidol rhwng y cenedlaethau". (Adroddiad Byron).

Felly bydd yr ysgol yn ceisio darparu gwybodaeth ac ymwybyddiaeth i rieni a gofalwyr trwy: *(dethol / dileu fel bo'n briodol)*

- *Lythyrau, cylchlythyrau, gwefan, ADRh*
- *Nosweithiau rhieni*

4.3 Staff

Mae'n hanfodol bod yr holl staff yn cael hyfforddiant e-ddiogelwch ac yn deall eu cyfrifoldebau, fel y nodwyd yn y polisi. Cynigir hyfforddiant fel a ganlyn: *(dethol / dileu fel bo'n briodol)*

- **Bydd rhaglen wedi'i gynllunio o hyfforddiant e-ddiogelwch ar gael i staff. Bydd archwiliad o anghenion hyfforddiant e-ddiogelwch yr holl staff yn cael ei gynnal yn rheolaidd.**
- **Dylai'r holl staff newydd gael hyfforddiant e-ddiogelwch fel rhan o'u rhaglen anwytho, i sicrhau eu bod yn deall yn iawn y polisi e-ddiogelwch a Chytundebau Defnydd Derbyniol**
- Bydd y cydlynydd e-ddiogelwch (neu rywun arall a enwebwyd) yn cael ei ddiweddaru'n rheolaidd trwy fynychu amrywiol gynadleddau/hyfforddiant a gynhaliwyd gan yr awdurdod lleol.
- Bydd y polisi e-ddiogelwch hwn a'i ddiweddariadau yn cael eu cyflwyno i a'u trafod gan staff mewn cyfarfodydd staff / tîm / ar ddyddiau HMS.
- Bydd y cydlynydd e-ddiogelwch (neu rywun arall a enwebwyd) yn darparu cyngor / arweiniad / hyfforddiant fel bo'r angen i unigolion

4.4 Llywodraethwyr

Dylai llywodraethwyr gymryd rhan mewn hyfforddiant / sesiynau ymwybyddiaeth e-ddiogelwch. Gellir cynnig hyn mewn nifer o ffyrdd:

- Mynychu hyfforddiant a drefnwyd gan yr awdurdod lleol neu sefydliad perthnasol arall.
- Cymryd rhan mewn hyfforddiant/sesiynau gwybodaeth ysgol i staff neu rieni.

5 Technegol –hidlo a chadw golwg

Mae gan yr ysgol (trwy'r awdurdod lleol) raglen hidlo uwch sef Smooth Wall. Mae YouTube gyda chwilio caeth wedi ei ganiatáu i ysgolion. Er hynny nid yw unrhyw system hidlydd yn 100% yn ddi-feth.

- Dylid hysbysu aelod o'r tîm TGCh Addysg ar unwaith am unrhyw broblemau hidlo.
- Ceisiadau gan staff i safleoedd i gael eu tynnu oddi ar y rhestr hidlo i'w hanfon at un o'r ymgynghorwyr TGCh.
- Mae staff technegol TGCh Conwy yn cadw golwg rheolaidd ac yn cofnodi gweithgaredd defnyddwyr ar systemau TGCh yr ysgol ac fe hysbysir defnyddwyr o hyn yn y Cytundeb Defnydd Derbyniol.
- Mae polisi cytunedig yn ei le parthed graddau defnydd personol (staff / disgyblion / defnyddwyr yn y gymdeithas) ac aelodau teuluol a ganiateir ar liniaduron a dyfeisiadau symudol y gellir eu defnyddio o fewn a thu allan i'r ysgol.

6 Cwricwlwm

Dylai e-ddiogelwch fod yn ffocws ymhob maes cwricwlwm a dylai staff atgyfnerthu neges e-ddiogelwch wrth ddefnyddio TGCh ar draws y cwricwlwm.

- mewn gwersi ble mae defnydd o'r rhyngrwyd wedi'i rag gynllunio, yr ymarfer gorau yw y dylai disgyblion gael eu harwain i safleoedd a gadarnhawyd yn addas iddynt i'w defnyddio a bod trefniadau yn eu lle i drin unrhyw ddeunydd anaddas a gafwyd mewn chwiliadau rhyngrwyd.
- Dylai staff gadw golwg ar gynnwys gwefannau mae pobl ifanc yn ymweld â hwy pan roddir rhyddid i ddisgyblion ddefnyddio'r rhyngrwyd e.e. wrth ddefnyddio peiriant chwilio.
- Dylid addysgu disgyblion ymhob gwers i fod yn feirniadol ymwybodol o'r deunydd / cynnwys maent yn edrych arno ar lein a'u harwain i ddilysu cywirdeb yr wybodaeth.
- Dylid addysgu disgyblion i gydnabod ffynhonnell yr wybodaeth a ddefnyddiwyd ac i barchu hawlfraint wrth ddefnyddio'r wybodaeth sydd ar y rhyngrwyd.

7. Defnyddio delweddau digidol a fideo – ffotograffig, fideo

Wrth ddefnyddio delweddau digidol, dylai staff ddweud wrth ac addysgu disgyblion am y peryglon a gysylltwyd â thynnu, rhannu, cyhoeddi a dosbarthu delweddau. Dylent yn arbennig gydnabod y peryglon a gysylltwyd â chyhoeddi eu delweddau eu hunain ar y rhyngrwyd e.e. ar safleoedd rhwydweithio cymdeithasol.

Caniateir i staff dynnu delweddau digidol / fideo i gefnogi nod addysgol, ond rhaid dilyn polisiau ysgol parthed rhannu, dosbarthu a chyhoeddi'r delweddau hyn. Dylai'r delweddau hyn gael eu tynnu ar offer yr ysgol, ni ddylid defnyddio offer personol staff at y fath bwrpas.

- Dylid cymryd gofal wrth dynnu delweddau digidol / fideo bod disgyblion wedi'u gwisgo'n briodol ac nid yn cymryd rhan mewn gweithgareddau a allai ddod ag enw drwg i'r ysgol.
- Ni ddylai disgyblion dynnu, defnyddio, rhannu, cyhoeddi na dosbarthu delweddau o eraill heb eu caniatâd

- Bydd lluniau a gyhoeddwyd ar wefan, neu rywle arall sy'n cynnwys disgyblion yn cael eu dethol yn ofalus ac yn cydymffurfio â chanllawiau ymarfer dda ar ddefnyddio'r fath ddelweddau.
- Ni fydd enwau llawn disgyblion yn cael eu defnyddio yn unlle ar wefan neu flog, yn arbennig mewn cysylltiad â llun.
- Ceisir caniatâd ysgrifenedig rhieni neu ofalwyr cyn cyhoeddi llun disgybl ar wefan yr ysgol
- Ni ellir cyhoeddi gwaith disgybl heb gael caniatâd y disgybl a rhieni neu ofalwyr.

8. Gwarchod Data

Dylai staff sicrhau eu bod yn:

- **Cymryd gofal bob amser i gadw data personol yn ddiogel, gan leihau'r perygl o'i golli neu gamddefnyddio.**
- **Defnyddio data personol yn unig ar gyfrifiaduron gyda chyfrinair a dyfeisiadau eraill, a sicrhau eu bod wedi'u "logio i ffwrdd" yn iawn ar ddiwedd unrhyw sesiwn pan ddefnyddir data personol.**
- **Trosglwyddo data gan ddefnyddio amgryptiad a dyfeisiadau wedi eu diogelu â chyfrinair.**
- **Peidio â defnyddio thechnolegau "cwmwl" e.e. DropBox, iCloud a Google Docs i storio data personol**

Pan fo data personol wedi'i storio ar unrhyw system cyfrifiadur symudol, cof bach neu unrhyw gyfrwng symudadwy arall:

- rhaid i'r data fod wedi'i amgryptio ag amddiffyniad cyfrinair
- rhaid amddiffyn â chyfrinair (ni ellir rhoi amddiffyniad cyfrinair ar lawer o gof bach / cardiau a dyfeisiadau symudol eraill)
- rhaid i'r ddyfais gynnig meddalwedd archwilio firws a malware a gymeradwywyd
- rhaid dileu'r data'n ddiogel oddi ar y ddyfais unwaith mae wedi'i drosglwyddo neu y gorffennwyd ei ddefnyddio.

9. Cyfathrebu

Wrth ddefnyddio technoleg cyfathrebu mae'r ysgol ystyried y canlynol fel ymarfer da:

- **Gellir ystyried gwasanaeth e-bost swyddogol yr ysgol yn ddiogel ac y cedwir golwg arno.** Felly, ni ddylai staff a disgyblion ond defnyddio gwasanaeth e-bost yr ysgol i gyfathrebu ag eraill yn yr ysgol, neu ar systemau'r ysgol (e.e. defnydd o bell).
- **Dylai defnyddwyr fod yn ymwybodol y cedwir golwg ar ddefnydd e-bost**
- **Rhaid i ddefnyddwyr hysbysu'r sawl a enwebwyd ar unwaith - yn unol â pholisi'r ysgol, y sawl sy'n cael unrhyw e-bost sy'n gwneud iddynt deimlo'n anghyfforddus, sydd o natur sarhaus, yn bygwth neu fwlio ac ni ddylent ymateb i'r e-bost.**
- **Rhaid i unrhyw gyfathrebu digidol rhwng staff a disgyblion neu rieni / gofalwyr (e-bost, sgwrs, ADRh ayb) fod yn broffesiynol ei don a chynnwys.** Ni all y cyfathrebu ond digwydd ar systemau ysgol swyddogol (cadw golwg). Ni ddylai cyfeiriadau e-bost personol, neges bawd destun neu siarad cyhoeddus / rhaglenni rhwydweithio cymdeithasol gael eu defnyddio ar gyfer cyfathrebu.

- Dylai disgyblion gael eu haddysgu am faterion diogelwch e-bost, megis y peryglon a gysylltir â defnyddio gwybodaeth bersonol. Hefyd, dylid addysgu strategau iddynt drin e-bost amhriodol a'u hatgoffa o'r angen i ddefnyddio e-bost yn glir a chywir a pheidio cynnwys unrhyw ddeunydd anaddas neu ddifrïol.
- Ni ddylid rhoi gwybodaeth bersonol ar wefan yr ysgol a dim ond cyfeiriadau e-bost swyddogol ddylid ei ddefnyddio i nodi aelodau o staff.

10. Gweithgareddau anaddas/amhriodol

Creda'r ysgol na fyddai'r gweithgareddau y cyfeiriwyd atynt isod yn briodol yng nghyd-destun yr ysgol ac na ddylai defnyddwyr, ymwneud â'r gweithgareddau hyn yn na thu allan i'r ysgol wrth ddefnyddio offer neu systemau'r ysgol. Mae polisi'r ysgol yn cyfyngu defnydd o'r rhyngrwyd fel a ganlyn: *(addasu/dileu yn ôl polisi'r ysgol)*

delweddau cam drin plant yn rhywiol

hyrwyddo neu gynnal gweithredoedd anghyfreithlon, e.e. o dan ddeddfwriaeth amddiffyn plant, anlladrwydd, camddefnyddio cyfrifiadur a thwyll

deunydd i oedolion sydd o bosibl yn torri Deddf Cyhoeddiadau Anllad ym Mhrydain
deunydd troseddol hiliol ym Mhrydain
pornograffi
hyrwyddo unrhyw fath o wahaniaethu
hyrwyddo casineb hiliol neu grefyddol
ymddygiad bygythiol, gan gynnwys hyrwyddo trais corfforol neu niwed meddyliol
defnyddio unrhyw wybodaeth arall a all fod yn sarhaus i gydweithiwr neu'n torri gonestrwydd ethos yr ysgol neu ddod ag enw drwg i'r ysgol
defnyddio systemau'r ysgol i redeg busnes preifat
defnyddio systemau, cymwysiadau, gwefannau neu fecanweithiau eraill sy'n osgoi hidlo neu amddiffyniad arall a ddefnyddir gan Gyngor Bwrdeistref Sirol Conwy
uwch lwytho, lawr lwytho neu drosglwyddo meddalwedd masnachol neu unrhyw ddeunydd hawlfraint sy'n perthyn i drydedd blaid, heb y caniatâd trwydded angenrheidiol
datgelu neu gyhoeddi gwybodaeth gyfrinachol neu berchnogol (e.e. ariannol / gwybodaeth bersonol, bas data, cod a chyfrineiriau cyfrifiadur / rhwydwaith)
creu neu ddatblygu firws cyfrifiadur neu ffeiliau niweidiol eraill
creu trafnidiaeth rhwydwaith trwm parhaus neu ddisymwth (lawr lwytho / uwch lwytho ffeiliau) sy'n achosi tagfa ar y rhwydwaith ac yn llesteirio eraill wrth ddefnyddio'r rhyngrwyd
chwarae ar lein (addysgol)
chwarae ar lein (anaddysgol)
hap chwarae ar lein
siopa / masnach ar lein
rhannu ffeil
defnyddio safleoedd rhwydweithio cymdeithasol

E-SAFETY POLICY

Policy adopted by Governing Body :

Signed by Chairperson: …….…… Date: ……

Signed by Headteacher: ……..…….. Date: ……

Review Date: ……

E-safety policy

1. Background

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

2. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

3. Roles and Responsibilities

3.1 The Governing Body

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

3.2 The Headteacher

The **Headteacher** is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the *E-Safety Co-ordinator / Officer*.

3.3 E-safety coordinator:

The e-safety coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides/arranges training and advice for staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, *(Examples of suitable log sheets may be found on the Education Intranet)*
- reports regularly to Senior Leadership Team/Governors

3.4 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices**
- **they have read, understood and signed the school Staff Acceptable Use Agreement (AUA)**
- **they report any suspected misuse or problem to the E-Safety Co-ordinator**
- e-safety issues are embedded in all aspects of the curriculum and other school activities

- students / pupils understand and follow the school e-safety and acceptable use policy
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils 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

3.5 Pupils

Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement, and parents/carers will be expected to discuss the agreement and sign it before being given access to school systems.

4 Education and Training

4.1 Pupils

The education of pupils in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-Safety education will be provided in the following ways: *(adapt to suit your situation)*

- **A planned e-safety programme will be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school**
- **Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information**
- Pupils should be helped to understand the need for the pupil AUA and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

4.2 Parents/carers

Many parents and carers have only a limited understanding of e-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 on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through: *(select / delete as appropriate)*

- *Letters, newsletters, web site, VLE*
- *Parents evenings*

4.3 Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.
Training will be offered as follows: *(select / delete as appropriate)*

- **A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.**
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements**
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at various conferences/training events held by the Local Authority
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required

4.4 Governors

Governors should take part in e-safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation.
- Participation in school training / information sessions for staff or parents

5. Technical –filtering and monitoring

The school (through the Local Authority) has an enhanced user-level filtering through the use of the Smooth Wall filtering program. YouTube, with strict filtering is available to schools now. However, no filtering system is 100% foolproof.

- Any filtering issues should be reported immediately to a member of the Education ICT team.
- Requests from staff for sites to be removed from the filtered list are to be sent to one of the ICT Advisors.
- Conwy ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Agreement.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used within and out of school.

6 Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that students / pupils 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 pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

7. Use of digital and video images – photographic, video

When using digital images, staff should inform and educate students / pupils 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.

Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' 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 pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers

8. Data Protection

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.**

- **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 and secure password protected devices.**
- **Do not store personal data on "cloud" storage technologies e.g. DropBox, iCloud, Google Docs**

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

9. Communication

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

- **The official school email service may be regarded as safe and secure and is monitored.** Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g.by remote access).
- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

10. Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows: *(amend/delete according to school policy)*

child sexual abuse images

promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation

adult material that potentially breaches the Obscene Publications Act in the UK

criminally racist material in UK

pornography

promotion of any kind of discrimination

promotion of racial or religious hatred

threatening behaviour, including promotion of physical violence or mental harm

any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Using school systems to run a private business

Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Conwy County Borough Council

Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions

Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
Creating or propagating computer viruses or other harmful files
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
On-line gaming (educational)
On-line gaming (non educational)
On-line gambling
On-line shopping / commerce
File sharing
Use of social networking sites