Ysgol Cybi

Polisi E-bost Staff Ysgolion / *School Staff E-mail Policy*

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

Ynglŷn â'r polisi hwn

Mae'r polisi hwn yn amlinellu'r hyn y mae'n rhaid i'r ysgol ei wneud er mwyn sicrhau defnydd effeithiol ac effeithlon o e-bost gan staff yr ysgol.

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

About this policy

This policy outlines what the school needs to do to ensure the effective and appropriate use of e-mail by school staff.

This policy is supported by resources on the Data Protection page on the Learning Service Microsite.

Fersiwn / *Version*	**Dyddiad / *Date***	**Crynodeb o newidiadau / *Summary of changes***	**Dyddiad a Dderbyniwyd gan Fwrdd o Lywodraethwyr / *Date Accepted by Board of Governors***
F1/*V1*	Rhagfyr 2022 / *December 2022*	Polisi newydd / *New policy*	

Dyddiad yr adolygiad nesaf / *Date of next review*	
Bydd y polisi hwn yn cael ei adolygu yn: / *This policy will be reviewed in:*	Rhagfyr 2025 / *December 2025*
Yr unigolyn a fydd yn ymgymryd â'r adolygiad fydd: / *The review will be undertaken by:*	Swyddog Diogelu Data Ysgolion / *Schools Data Protection Officer*

Manylion Cyswllt:

Swyddog Diogelu Data Ysgolion

E-bost:
dpoysgolionmon@ynysmon.llyw.cymru

Rhif ffôn: 01248 751833

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

Contact Details:

Schools Data Protection Officer

E-mail:
dpoysgolionmon@ynysmon.llyw.cymru

Telephone: 01248 751833

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

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

Dogfen:	Templed polisi ar y defnydd effeithiol a phriodol o e-bost gan staff ysgolion.
Document:	*Policy template on the effective and appropriate use of e-mail by school staff.*
Cyfrifoldeb:	Cyfrifoldeb y llywodraethwyr ysgol yw sicrhau bod gweithdrefnau ar waith i sicrhau bod yr ysgol yn cydymffurfio â'r polisi hwn. Cyfrifoldeb y Pennaeth yw sicrhau gweithrediad a chydymffurfiaeth gan holl staff yr ysgol.
Responsibility:	*It is the responsibility of the school governors to ensure procedures are in place to ensure that the school complies with this policy. It is the responsibility of the Headteacher to ensure implementation and compliance by all school staff.*

Cynnwys **Tudalen**

1. Datganiad Polisi 4
2. Sgôp 4
3. Deddfwriaeth, Canllawiau a Pholisïau 5
4. Diffiniadau 5
5. Cyfrifoldebau 7
   5.1. Corff Llywodraethu'r Ysgol 7
   5.2. Y Pennaeth (ac/neu'r Person sy'n Gyfrifol am Ddiogelu Data yn yr Ysgol) 7
   5.3. Holl Staff yr Ysgol 8
   5.4. Swyddog Diogelu Data Ysgolion 8
6. Anfon E-byst 9
   6.1. Gwybodaeth Bersonol a Sensitif mewn E-byst 9
   6.2. Gweithgareddau a Chynnwys E-bost 10
   6.3. Cyfathrebu â Disgyblion dros E-bost 11
7. Llofnod E-bost 11
8. Dosbarthiad Gwybodaeth Bersonol mewn E-byst 11
9. Dargadw E-byst a'u Gwaredu'n Ddiogel 12
10. Cwotâu a Chyfyngiadau E-bost 13
11. E-byst a Dolenni Cyswllt Amheus 13
12. Gwirio am Firysau 14
13. Monitro 14
14. Mynd yn Erbyn y Polisi 14
15. Adolygu'r Polisi a Threfniadau Arolygiaeth 15

ATODIAD A – Polisi E-byst Staff Ysgolion – Rhestr Wirio'r Pennaeth 29

English Version **16**

1. Datganiad Polisi

Mae'r polisi hwn yn amlinellu beth mae'r ysgol angen ei wneud i sicrhau defnydd effeithiol ac effeithlon o e-bost gan staff ysgolion. Bydd y polisi hwn yn darparu arweiniad ar sut i reoli ac felly lleihau'r risgiau sydd ynghlwm ag e-bost ar gyfer y defnyddiwr a'r ysgol.

Mae rhannu gwybodaeth bersonol neu sensitif ynglŷn ag unigolion adnabyddedig dros e-bost yn cynnwys prosesu gwybodaeth bersonol ac felly mae angen iddo gydymffurfio â'r egwyddorion diogelu data dan *Reoliadau Diogelu Data Cyffredinol y DU (UK GDPR)* a *Deddf Diogelu Data 2018.*

Prif bwrpas yr ysgol mewn darparu cyfleusterau e-bost yw cynorthwyo staff ysgolion ym mherfformiad eu rôl; i ddarparu gweithgareddau dysgu ac addysgu a chynorthwyo mewn darparu gweithgareddau busnes cymeradwy'r ysgol.

Dim ond defnyddwyr awdurdodedig systemau cyfrifiadur yr ysgol sydd â hawl i ddefnyddio cyfleusterau e-bost ac ni fydd cyfleusterau TG a ddarperir gan yr ysgol ar gyfer e-bost yn cael eu camddefnyddio.

Mae gan bob defnyddiwr o systemau e-bost yr ysgol ddyletswydd i sicrhau eu bod yn ymarfer defnydd addas a phriodol ac mae'n rhaid iddynt ddeall eu cyfrifoldebau yn hyn o beth. Mae cyfrifoldeb unigol ar holl staff ysgolion i sicrhau eu bod yn rheoli eu cyfrif e-bost yn gywir.

Mae hefyd yn hanfodol sicrhau bod yr wybodaeth a gadwir yn y systemau e-bost yn cael ei rheoli'n gywir. Os na chaiff ei rheoli'n gywir, mae'n bosibl y bydd yn arwain at arferion gwaith aneffeithlon, gorlwytho gwybodaeth neu golled gwybodaeth y gall arwain at ddigwyddiad diogelwch data.

Bydd y polisi hwn yn helpu i gyfrannu at:

- sicrhau bod yr ysgol yn cydymffurfio â'i gofynion dan ddeddfwriaeth diogelu data megis *UK GDPR*; *Deddf Diogelu Data 2018* a *Deddf Rhyddid Gwybodaeth 2000*;
- sicrhau nad yw'r system e-byst wedi ei gorlwytho â llwyth gwaith dianghenraid;
- lleihau gorlwytho gwybodaeth mewn perthynas ag eitemau e-bost diangen y mae angen eu hadolygu.

2. Sgôp

Mae'r polisi hwn yn berthnasol ar gyfer holl aelodau o staff ysgolion, gan gynnwys gweithwyr dros dro, contractwyr eraill, gwirfoddolwyr, llywodraethwyr ac unrhyw drydydd partïon gyda chyfrif e-bost ysgol.

Mae hyn yn cymhwyso at gyfrifon e-bost Hwb (Llywodraeth Cymru) ac unrhyw gyfrifon e-bost swyddogol ysgol eraill.

Mae'r polisi hwn yn cymhwyso at ddefnydd, at ddibenion anfon neu dderbyn negeseuon ac atodiadau e-bost, o unrhyw gyfleusterau TG, gan gynnwys caledwedd, meddalwedd a rhwydweithiau a ddarperir gan yr ysgol.

Bydd risgiau i'r defnyddiwr a'r ysgol yn cael eu rheoli drwy sicrhau defnydd priodol o e-byst drwy wneud defnyddwyr yn ymwybodol o beth sy'n dderbyniol ac yn annerbyniol. Mae'r rhain yn seiliedig ar ofynion deddfwriaethol a pholisïau mewnol ac mae'n rhaid i bob unigolyn sydd â chyfrif e-bost ysgol eu dilyn.

Disgwylir i staff ysgolion gynnal y safonau uchaf o ran ymddygiad ac ymarfer proffesiynol a disgwylir iddynt gadw at egwyddorion allweddol ymddygiad da ac ymarfer proffesiynol yn unol â *Chod Ymddygiad ac Ymarfer Proffesiynol Cyngor y Gweithlu Addysg (CGA).*

3. Deddfwriaeth, Canllawiau a Pholisïau

Y brif ddeddfwriaeth diogelu data y mae'r polisi hwn yn cydymffurfio â hi yw *Rheoliad Diogelu Data Cyffredinol y DU (UK GDPR)*; *Deddf Diogelu Data 2018* a *Deddf Rhyddid Gwybodaeth 2000.*

Dylid darllen y polisi hwn hefyd ar y cyd â'r *Polisi Diogelu Data Ysgolion*, *Polisi Diogelwch Gwybodaeth Ysgolion; Polisi Cyfryngau Cymdeithasol Staff Ysgolion; Polisi Ceisiadau gan Wrthrych y Data Ysgolion; Polisi Digwyddiadau Diogelwch Data Ysgolion* a'r *Cyfnodau Cadw Ysgolion.*

Mae'r polisi hwn hefyd yn seiliedig ar egwyddorion y *'Cod Ymddygiad ac Ymarfer Proffesiynol ar gyfer cofrestryddion gyda Chyngor y Gweithlu Addysg (CGA)*' a *'Chyngor y Gweithlu Addysg (CGA) Cynnal Ffiniau Proffesiynol gyda Dysgwyr Canllaw Arfer Dda'.*

4. Diffiniadau

Data personol	Unrhyw wybodaeth ynglŷn ag unigolyn naturiol yr adnabyddir neu y gellir ei adnabod yn uniongyrchol neu'n anuniongyrchol drwy'r wybodaeth honno. Gellir ei storio'n ddigidol, ar gyfrifiadur, neu mewn systemau ffeilio ar bapur.
Data categori arbennig	Gwybodaeth ynglŷn â hil, tarddiad ethnig, barn wleidyddol, credoau crefyddol neu athronyddol, aelodaeth undeb llafur (neu ddiffyg aelodaeth), gwybodaeth enetig, gwybodaeth fiometreg (i adnabod unigolyn) unigolyn, a gwybodaeth ynglŷn ag iechyd, bywyd rhywiol neu ogwydd rhywiol unigolyn. Data categori arbennig yw data personol sydd angen amddiffyniad bellach oherwydd ei fod yn sensitif.

Prosesu gwybodaeth	Casglu, meddiannu, cofnodi, trefnu, strwythuro, storio, dargadw, diwygio, addasu, altro, adennill, ymgynghori, lledaenu, cyfyngu, datgelu, dinistrio, dileu gwybodaeth neu ei defnyddio neu wneud unrhyw beth â hi.
Digwyddiad Diogelwch Data	Toriad diogelwch sy'n arwain at ddinistrio, colli, addasu, datgelu neu fynediad anawdurdodedig at ddata personol a drosglwyddir, a storir neu a brosesir mewn unrhyw ddull arall, yn ddamweiniol neu'n anghyfreithlon.
E-bost	Negeseuon a ddosberthir drwy ddulliau electronig o un defnyddiwr cyfrifiadur i un neu fwy o dderbynwyr drwy rwydwaith. Yn ogystal â chynnwys testunol, mae e-bost yn caniatáu i'r anfonwr anfon ffotograffau, fideo neu glipiau sain ar ffurf neu ffeiliau digidol.
Blwch Post	Y gyrchfan y cyflwynir negeseuon post electronig iddi. Mae'n cyfateb i flwch llythyrau yn y system bost.
Anawdurdodedig	Heb hawl cyfreithlon.
Seiberddiogelwch	Mae seiberddiogelwch yn cyfeirio at y corff o dechnolegau, prosesau ac arferion a ddylunnir i amddiffyn rhwydweithiau, dyfeisiau, rhaglenni a data rhag ymosodiad, difrod neu fynediad anawdurdodedig.
Hacwyr	Mae haciwr yn unigolyn sy'n defnyddio cyfrifiadur, rhwydweithio neu sgiliau eraill i oresgyn problem dechnegol ac sy'n cael mynediad anghyfreithlon i wybodaeth mewn system gyfrifiadurol ac weithiau'n ymyrryd â hi.
Ymosodiad Seiber	Mae ymosodiad seiber yn ymosodiad a gychwynnwyd o gyfrifiadur yn erbyn gwefan, system gyfrifiadurol neu gyfrifiadur unigol (gyda'i gilydd, cyfrifiadur) sy'n peryglu cyfrinachedd, uniondeb neu argaeledd y cyfrifiadur neu'r wybodaeth a gedwir arno.
Bygythiad	Achos posibl digwyddiad dieisiau, y gall arwain at niwed i system neu sefydliad.
Risg	Effaith ansicrwydd ar amcanion. Risgiau i unigolion: y potensial ar gyfer difrod neu ofid. Nodweddir risg yn aml drwy gyfeirio at "ddigwyddiadau" a "chanlyniadau" posibl, neu gyfuniad o'r rhain.
Asesiad Risg	Adnabyddiaeth a dadansoddiad risgiau i amcanion busnes y sefydliad.
Effaith	Beth yw canlyniadau'r risg pe bai'n digwydd?
Tebygolrwydd	Pa mor debygol ydyw bod y risg am ddigwydd – annhebygolrwydd, siawns neu debygolrwydd.
Mesur Rheoli	Mesur sy'n addasu risg.
Phishing	Mae sgamwyr yn anfon e-byst ffug at filoedd o bobl yn gofyn am wybodaeth sensitif (fel manylion banc) neu'n cynnwys dolenni i wefannau drwg. Maent yn gwneud hyn i ddwyn manylion i'w gwerthu neu efallai i gael gafael ar wybodaeth a gedwir gan sefydliadau.

Drwgwedd	Meddalwedd sydd wedi'i gynllunio'n benodol i darfu, difrodi, neu gael mynediad heb awdurdod i system gyfrifiadurol.
Fflamio	Term rhithwir ar gyfer mentro neu anfon negeseuon ymfflamychol mewn e-bost.
Sothach	Negeseuon amherthnasol neu ddigymell a anfonir dros y rhyngrwyd/e-bost, fel arfer i nifer fawr o ddefnyddwyr, at ddibenion hysbysebu, *phishing*, lledaenu meddalwedd maleisus, ac ati.
Firws Cyfrifiadur	Mae firws cyfrifiadurol yn fath o raglen gyfrifiadurol faleisus, sydd, pan gaiff ei gweithredu, yn dyblygu ei hun ac yn mewnosod ei chod ei hun. Pan wneir y dyblygu, mae'r cod hwn yn heintio'r ffeiliau a'r rhaglenni arall sy'n bresennol ar y system.
Spyware	Meddalwedd sy'n galluogi defnyddiwr i gael gwybodaeth gudd am weithgareddau cyfrifiadurol rhywun arall drwy drosglwyddo data'n gudd o'u gyriant caled.
Trojan horses	Rhaglen a gynlluniwyd i dorri diogelwch system gyfrifiadurol tra'n cyflawni rhywfaint o swyddogaeth ddiniwed yn ôl pob golwg.
Seiber-fwlio	Unrhyw ddefnydd o gyfryngau cymdeithasol neu dechnoleg cyfathrebu i fwlio unigolyn neu grŵp.
Amgryptio	Mae amgryptio data yn ddull diogelwch lle mae gwybodaeth yn cael ei hamgodio a dim ond defnyddiwr sydd â'r allwedd amgryptio gywir y gellir ei gyrchu neu ei ddadgryptio. Mae data wedi'i amgryptio yn ymddangos wedi'i sgramblo neu'n annarllenadwy i berson neu endid sy'n cyrchu heb ganiatâd.
Dilysiad	Dilysu yw'r broses o benderfynu a yw rhywun (neu rywbeth) yn pwy (neu beth) y mae'n honni i fod.
Dilysiad aml-ffactor	Mae dilysu aml-ffactor, wedi'i dalfyrio fel 2FA, yn broses ddilysu sy'n gofyn am ddau ffactor dilysu gwahanol i sefydlu hunaniaeth - mae'n golygu ei gwneud yn ofynnol i ddefnyddiwr brofi ei hunaniaeth mewn dwy ffordd wahanol cyn rhoi mynediad iddynt i system.
Dienwi	Cael gwared ar wybodaeth adnabod o rywbeth (fel data cyfrifiadurol) fel na ellir adnabod na nodi'r ffynhonnell wreiddiol.

5. Cyfrifoldebau

5.1. Corff Llywodraethu'r Ysgol

Mae corff llywodraethu'r ysgol yn gyfrifol am:

- fonitro cydymffurfiad ac atebolrwydd cyffredinol yr ysgol mewn perthynas â'r polisi hwn;
- sicrhau y gall yr ysgol dystiolaethu cydymffurfiaeth â deddfwriaeth diogelu data.

5.2. Y Pennaeth (ac/neu'r Person sy'n Gyfrifol am Ddiogelu Data yn yr Ysgol)

Mae'r Pennaeth ac/neu'r person sy'n gyfrifol am ddiogelu data yn yr ysgol yn gyfrifol am:

- sicrhau bod y polisi hwn yn cael ei weithredu a hyrwyddo dealltwriaeth a chydymffurfiaeth â'r polisi hwn;
- monitro'r broses o weithredu'r polisi hwn a chydymffurfio ag ef;
- sicrhau bod gwybodaeth bersonol mewn negeseuon e-bost yn cael ei chadw a'i phrosesu yn unol â *UK GDPR*; *Deddf Diogelu Data 2018* a *Deddf Rhyddid Gwybodaeth 2000*;
- sicrhau bod yr holl staff yn cydymffurfio â'r *Cyfnodau Cadw Ysgolion* a bod yr ysgol yn cynnal gweithgareddau cadw tŷ rheolaidd sy'n ymwneud ag e-byst;
- sicrhau bod lefelau dosbarthu'n cael eu defnyddio'n briodol;
- sicrhau bod staff yn cael hyfforddiant priodol ar gyfer defnyddio negeseuon e-bost;
- monitro bod staff yr ysgol yn glynu wrth egwyddorion y *Cod Ymddygiad ac Ymarfer Proffesiynol ar gyfer cofrestryddion gyda Chyngor y Gweithlu Addysg (CGA);*
- yn ei wneud yn fandadol i ddefnyddio dilysiad aml-ffactor yng nghyfrifon HWB staff er mwyn diogelu cyfrifon Office 365.

5.3. Holl Staff yr Ysgol

Mae'r holl staff a gyflogir gan yr ysgol neu sy'n gwirfoddoli yn yr ysgol, gan gynnwys athrawon, cymorthyddion dosbarth, staff cefnogi busnes a llywodraethwyr yn gyfrifol am:

- sicrhau dealltwriaeth a chydymffurfiaeth â'r polisi hwn;
- sicrhau'r arfer o ddefnyddio e-bost yn briodol ac yn addas;
- rheoli cyfrifon e-bost ysgolion unigol yn gywir;
- peidio â defnyddio cyfrifon e-bost personol neu anawdurdodedig i rannu data personol neu sensitif sy'n ymwneud â'r ysgol;
- sicrhau bod gwybodaeth bersonol mewn negeseuon e-bost yn cael ei chadw a'i phrosesu yn unol â *UK GDPR*; *Deddf Diogelu Data 2018* a *Deddf Rhyddid Gwybodaeth 2000*;
- glynu wrth egwyddorion y *Cod Ymddygiad ac Ymarfer Proffesiynol ar gyfer cofrestryddion gyda Chyngor y Gweithlu Addysg (CGA)*;
- defnyddio lefelau dosbarthu yn briodol mewn perthynas ag e-byst;
- cydymffurfio'n llawn â'r *Cyfnodau Cadw Ysgolion*;
- cadw o fewn cwota'r cyfrif e-bost;
- bod yn ofalus o negeseuon e-bost a dolenni cyswllt amheus;
- ymgymryd â'r holl hyfforddiant a gynhigir ar ddefnyddio negeseuon e-bost.

5.4. Swyddog Diogelu Data Ysgolion

Mae'r Swyddog Diogelu Data Ysgolion yn gyfrifol am:

- ddarparu cyngor ac arweiniad i'r ysgol mewn perthynas ag amddiffyn a diogelwch gwybodaeth yn ymwneud â defnydd e-bost.
- monitro gweithrediad a chydymffurfiaeth â'r polisi hwn gan yr ysgol;
- darparu cyngor a chefnogaeth ac arwain ar adrodd am ddigwyddiadau diogelwch data mewn perthynas â gwybodaeth bersonol a sensitif a gynhwysir mewn e-byst.

6. Anfon E-byst

Dylai staff ysgolion ystyried a yw e-bost yn wirioneddol angenrheidiol cyn ei anfon.

Nid yw e-bost safonol yn ffurf ddiogel o gyfathrebu. Gall y negeseuon a anfonir fod dros rwydweithiau a berchnogir gan bobl eraill. Bydd dull mwy diogel o gyfathrebu'n cael ei ddefnyddio, os yw cynnwys e-bost yn sensitif neu'n gritigol megis os datgelwyd neu addaswyd y cynnwys gan berson anawdurdodedig y gall achosi embaras, trallod neu golled ariannol. Mae angen cymryd gofal bod canlyniadau potensial o yrru negeseuon yn cael eu gwerthfawrogi.

Ystyrir mai'r unigolyn sydd wedi mewngofnodi ar gyfrifiadur fydd awdur unrhyw negeseuon a anfonir o'r cyfrif cyfrifiadur hwnnw. Bydd holl staff yr ysgol yn allgofnodi neu'n cloi eu cyfrifiaduron pan fyddant i ffwrdd o'u desgiau; ni ddylai defnyddiwr anfon neges o gyfrif rhywun arall o dan unrhyw amgylchiadau.

Wrth anfon e-bost, rhaid i'r anfonwr wirio bod cyfeiriad e-bost y derbynnydd yn gywir ac nad oes unrhyw un arall na ddylai dderbyn yr e-bost yn cael ei gopïo fel derbynnydd. Mae'n hawdd iawn anfon e-bost at y derbynnydd anghywir.

Os yn anfon unrhyw e-bost lle mae angen cuddio cyfeiriadau e-bost unigol, dylid defnyddio'r cyfleuster copïo dall (bcc). Dylid defnyddio'r cyfleuster copïo dall wrth anfon at nifer fawr o dderbynwyr (yn enwedig yn allanol).

Mae angen ystyried cyn ymateb i e-bost grŵp neu gopïo eraill yn yr e-bost, a oes angen i'r holl dderbynwyr dderbyn yr wybodaeth. Ni ddylai staff yr ysgol anfon negeseuon e-bost at yr holl staff oni bai ei bod yn angenrheidiol ac yn briodol i'r holl staff dderbyn yr wybodaeth.

6.1. Gwybodaeth Bersonol a Sensitif mewn E-byst

Ni fydd staff yr ysgol yn defnyddio eu cyfrif e-bost personol neu anawdurdodedig i rannu data personol neu sensitif sy'n ymwneud â'r ysgol nag ei staff a disgyblion.

Ni ddylid defnyddio e-bost i anfon gwybodaeth bersonol sensitif heb ddefnyddio lefel o ddiogelwch cyfrinair sy'n briodol i sensitifrwydd y data yn gyntaf.

Yn ddiofyn, mae system e-bost HWB wedi'i ffurfweddu i amgryptio ei sgwrs â systemau e-bost eraill wrth anfon a derbyn negeseuon. Gweler y canllaw- 'Amgryptio e-bost a anfonir o gyfeiriadau HWB' ar y Porth TG i gael arweiniad ar hyn-

https://desggymorth.ynysmon.gov.uk/support/solutions/articles/50000102041-encrypting-email-sent-from-hwb-addresses-

Os oes rhaid rhannu gwybodaeth bersonol sensitif drwy e-bost, dylid cadw'r wybodaeth berthnasol mewn dogfen Microsoft Word neu Excel. Yna dylid diogelu'r ddogfen a'i hanfon fel atodiad e-bost. Dylid rhannu'r cyfrinair ar wahân ac yn ddiogel gyda'r derbynnydd arfaethedig. Fel arall, bydd angen dadbersonoli gwybodaeth bersonol.

Gall fod yn briodol defnyddio blaenlythrennau yn lle enwau llawn mewn e-byst neu ddefnyddio dynodwr unigryw lle mai dim ond staff yr ysgol sy'n gallu adnabod yr unigolyn.

Efallai y byddai'n briodol gofyn i'r derbynnydd gadarnhau ei fod wedi derbyn yr e-bost os yw'n cynnwys gwybodaeth bersonol.

Os caiff neges e-bost sy'n cynnwys gwybodaeth bersonol neu sensitif ei rhannu â derbynnydd anfwriadol neu os yw'n cael ei cholli neu ei chyrchu gan ddefnyddiwr anawdurdodedig, efallai y bydd angen rhoi gwybod i'r Swyddog Diogelu Data Ysgolion ar unwaith am ddigwyddiad diogelwch data. Bydd yr ysgol yn cydymffurfio â'r *Polisi Digwyddiadau Diogelwch Data Ysgolion.*

6.2. Gweithgareddau a Chynnwys E-bost

Mae'r canlynol yn enghreifftiau o weithgareddau a defnydd a waherddir gan staff yr ysgol ar gyfrifon e-bost swyddogol yr ysgol:

- gweithgareddau sy'n gwastraffu ymdrech staff yn afresymol neu adnoddau wedi'u rhwydweithio, neu weithgareddau sy'n afresymol yn gwadu gwasanaeth i ddefnyddwyr eraill;
- gweithgareddau sy'n llygru neu'n dinistrio data defnyddwyr eraill neu'n amharu ar waith defnyddwyr eraill;
- defnydd personol afresymol neu ormodol;
- gweithgareddau sy'n cyfaddawdu preifatrwydd eraill neu'n beirniadu neu'n camliwio eraill yn annheg; mae hyn yn cynnwys copïo dosbarthiad i unigolion eraill;
- galluogi trydydd partïon i ddarparu mynediad heb awdurdod i wasanaethau a chyfleusterau ysgolion.

Ni fydd unrhyw staff ysgol yn anfon nac yn anfon ymlaen negeseuon e-bost y gellir eu dehongli mewn unrhyw ffordd fel rhai sarhaus, aflonyddgar neu ymosodol gan unrhyw berson neu gwmni arall. Mae enghreifftiau o ddeunydd gwaharddedig yn cynnwys ond heb fod yn gyfyngedig i:

- deunydd anghyfreithlon;
- deunydd cyfrinachol sy'n ymwneud â gweithgareddau'r ysgol i drydydd parti;

- negeseuon, delweddau, cartwnau, jôcs neu ffeiliau fideo sy'n benodol yn rhywiol;
- delweddau, data neu ddeunydd arall sy'n anweddus;
- afradlonedd, anlladrwydd, slander neu enllib;
- unrhyw negeseuon sydd yn gallu cael eu dehongli fel trosedd casineb ar sail hil, crefydd, anabledd, tueddfryd rhywiol, hunaniaeth trawsryweddol;
- credoau neu sylwebaeth wleidyddol;
- unrhyw neges y gellid ei hystyried yn sarhaus, yn fygythiol, yn ymosodol neu'n aflonyddu, yn fwlio, yn wahaniaethu neu'n amharu ar eraill yn seiliedig ar eu rhyw, hil, ethnigrwydd, cyfeiriadedd rhywiol, oedran, statws priodasol, tarddiad cenedlaethol, anabledd neu gredoau crefyddol neu wleidyddol;
- deunydd difenwol neu ddeunydd sy'n cynnwys hawliadau o natur dwyllodrus;
- negeseuon dienw neu ffugio negeseuon neu wybodaeth pennawd e-bost yn fwriadol (h.y. heb adnabod yr anfonwr yn glir) neu ar gyfer 'fflamio';
- deunydd sydd wedi'i gynllunio neu sy'n debygol o achosi annifyrrwch, anghyfleustra neu bryder;
- cynigion annymunol;
- deunydd masnachol neu hysbysebu digymell, llythyrau cadwyn, datganiadau i'r wasg neu e-bost sothach arall o unrhyw fath.

6.3. Cyfathrebu â Disgyblion dros E-bost

Bydd staff yr ysgol ond yn defnyddio cyfrif e-bost awdurdodedig i gyfathrebu mewn perthynas â busnes yr ysgol.

Ni fydd staff yr ysgol yn defnyddio eu cyfrif e-bost personol i gyfathrebu â disgyblion na'u teulu/gofalwyr.

7. Llofnod E-bost

Mae'n arfer dda sefydlu llofnod dwyieithog ar gyfrifon e-bost. Bydd y llofnod yn ymddangos ar ddiwedd negeseuon e-bost. Dylai hyn gynnwys enw a manylion cyswllt staff yr ysgol. Dylid diweddaru'r manylion hyn.

Mae sefydlu llofnod dwyieithog yn sicrhau bod yr ysgol yn cyflwyno delwedd broffesiynol ac yn rhoi gwybod i'r derbynnydd pwy yw'r anfonwr a ffyrdd o gysylltu.

8. Dosbarthiad Gwybodaeth Bersonol mewn E-byst

Rhaid adnabod negeseuon e-bost sy'n cynnwys data personol a data categori arbennig gan ddefnyddio termau dosbarthu data (SWYDDOGOL neu SWYDDOGOL-SENSITIF) ym maes pwnc yr e-bost.

Pennir y categori dosbarthu gwybodaeth ar y **niwed** a allai ddeillio o golli neu ddatgelu'r wybodaeth heb awdurdod. Categori dosbarthu gwybodaeth sy'n pennu sut y mae'n rhaid diogelu/ymdrin â gwybodaeth.

Categori Dosbarthu	**Yr effaith os caiff yr wybodaeth ei cholli neu ei datgelu i unigolion anawdurdodedig**	**Enghreifftiau o wybodaeth**
SWYDDOGOL	Bydd bron i holl yr wybodaeth y mae'r ysgol yn dod i gysylltiad â hi yn ystod y diwrnod gwaith yn wybodaeth SWYDDOGOL. Fodd bynnag, mae gwybodaeth swyddogol hefyd yn cynnwys data personol sydd eisoes ar gael i'r cyhoedd na fyddai, pe bai'n cael ei ddatgelu heb ganiatâd neu golled, yn achosi niwed neu ofid i unrhyw unigolyn.	Adroddiadau rheolaidd, adroddiadau blynyddol cyhoeddedig, data alldro ar gyfer dangosyddion perfformiad allweddol, gwybodaeth sydd ar gael am ddim e.e. gwybodaeth ar wefan yr ysgol; enwau cyflogeion a theitlau swyddi a gwybodaeth nad yw'n fasnachol sensitif.
SWYDDOGOL-SENSITIF	• Achosi niwed neu ofid i unigolion; • Torri cyfyngiadau statudol ar ddatgelu gwybodaeth; • Byddai'n arwain at dorri hyder i drydydd partïon (lle nad yw'r wybodaeth ar gael i'r cyhoedd); • Achosi niwed neu ofid sylweddol i unigolion neu grwpiau; • Rhagfarnu'r ymchwiliad neu hwyluso'r gwaith o gomisiynu troseddau.	Gwybodaeth am ddisgyblion neu staff y mae gan yr ysgol ddyletswydd gofal drosti, e.e. enwau, cyfeiriadau, cofnod disgyblion.

Ni ddylid cynnwys gwybodaeth bersonol ym maes pwnc yr e-bost.

9. Dargadw E-byst a'u Gwaredu'n Ddiogel

Bydd cyfrifon e-bost ysgolion hefyd yn amodol ar reoliadau diogelu data ac mae'n rhaid dilyn y *Cyfnodau Cadw Ysgolion* mewn perthynas ag e-byst.

Ni fydd staff yr ysgol yn defnyddio eu cyfrif e-bost swyddogol yn yr ysgol i storio gwybodaeth ac fel system ffeilio neu reoli achosion. Dylid ystyried systemau e-bost fel ffordd o ddanfon a derbyn negeseuon - nid ydynt wedi'u bwriadu ar gyfer storio ac adalw negeseuon a ffeiliau atodol yn y tymor hir.

Bydd negeseuon e-bost yn cael eu dileu neu eu ffeilio fel y bo'n briodol. Bydd negeseuon e-bost y mae angen eu dileu yn cael eu dileu a bydd angen trosglwyddo negeseuon e-bost y mae angen eu cadw yn unol â'r *Cyfnodau Cadw Ysgolion* i ffolder rhwydwaith priodol. Dylid cymhwyso'r *Cyfnodau Cadw Ysgolion* o fewn y system ffeilio berthnasol er mwyn cydymffurfio â *UK GDPR*. Dylai staff yr ysgol lanhau eu blwch post e-bost yn rheolaidd.

Gellir darparu gwybodaeth bersonol mewn negeseuon e-bost i unigolion fel rhan o Geisiadau gan Wrthrych y Data. Bydd yr ysgol yn dilyn y *Polisi Ceisiadau gan Wrthrych y Data Ysgolion.*

Os oes unrhyw ansicrwydd, dylai'r ysgol ymgynghori â'r Swyddog Diogelu Data Ysgolion i gael arweiniad ar ba mor hir i gadw negeseuon e-bost.

Bydd negeseuon e-bost nad oes eu hangen mwyach yn unol â'r *Cyfnodau Cadw Ysgolion* yn cael eu dileu'n barhaol o systemau gwybodaeth yr ysgol.

Bydd unrhyw gopïau caled o wybodaeth bersonol a gynhwysir mewn e-bost yn cael eu dinistrio mewn modd diogel.

Mae'r *Cyfnodau Cadw Ysgolion* i'w gweld ar y dudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

10. Cwotâu a Chyfyngiadau E-bost

Mae gan bob cyfrif derfynau cwota wedi'u gosod arnynt.

Bydd defnyddwyr yn derbyn hysbysiad e-bost wrth agosáu at eu terfyn cwota ac fe'u hanogir i ddilyn canllawiau yn yr e-bost hwn i reoli eu cyfrif. Unwaith y byddant dros gwota, ni ellir anfon unrhyw negeseuon e-bost pellach i fewnflwch unigolyn nes eu bod wedi lleihau eu storfeydd o dan eu terfyn.

Mae e-bost sy'n methu â chael ei ddanfon oherwydd bod defnyddiwr dros gwota yn cael ei gadw yn y ciwiau post lleol am bedwar diwrnod a bydd y system yn rhoi cynnig arall arni o bryd i'w gilydd. Ar ôl pedwar diwrnod, dychwelir yr e-bost i'r anfonwr.

Bydd ffolderi e-bost yn cael eu hadolygu'n rheolaidd gan y defnyddiwr a bydd unrhyw negeseuon nad ydynt yn hanfodol yn cael eu dileu neu eu cadw mewn ffolderi. Mae sawl ffordd o leihau maint y blwch post:

- canfod a dileu/trosglwyddo negeseuon e-bost mawr i ffolder rhwydwaith priodol;
- dod o hyd i hen negeseuon e-bost a'u dileu/trosglwyddo i ffolder rhwydwaith priodol;
- glanhau negeseuon e-bost dyblyg o sgyrsiau parhaus.

Ni ddylid cynnwys atodiadau mawr neu niferus heb fod angen.

11. E-byst a Dolenni Cyswllt Amheus

Dylai staff ysgol fod yn wyliadwrus o negeseuon e-bost, atodiadau a dolenni cyswllt annisgwyl. Ni fydd negeseuon e-bost, atodiadau a dolenni cyswllt yn cael eu hagor oni bai eu bod yn dod o ffynhonnell hysbys. Mae gan ffeiliau neu ddolenni maleisus a anfonir drwy e-bost y potensial i ddal cyfrineiriau, dwyn data ysgol a gwneud gweithfannau neu hyd yn oed rwydwaith yr ysgol yn segur.

Os bydd defnyddwyr yn derbyn negeseuon e-bost sy'n ymddangos yn amheus (er enghraifft, negeseuon e-bost gyda llinellau pwnc amheus) fe'u cynghorir i beidio ag

agor yr e-bost nac unrhyw atodiadau sydd wedi'u cynnwys. Yn hytrach, dylid dileu'r e-bost a gwagio'r 'eitemau wedi'u dileu'.

Dylid bod yn ofalus cyn i atodiadau a dolenni cyswllt a dderbynnir mewn negeseuon e-bost gael eu hagor. Bydd hyn yn wir hyd yn oed os yw'r e-bost yn dod o ffynhonnell hysbys.

Dylid rhoi gwybod i Ddesg Gwasanaeth TGCh Cyngor Sir Ynys Môn am unrhyw negeseuon e-bost amheus fel y gellir nodi unrhyw batrwm o broblem neu ymosodiad ehangach cyn gynted â phosibl a chymryd camau ataliol.

12. Gwirio am Firysau

Gelwir firysau cyfrifiadurol, *trojan horses* a *worms* gyda'i gilydd yn ddrwgwedd. Un dull cyffredin o ddosbarthu meddalwedd maleisus yw drwy e-bost. Mae'r holl gyfathrebu e-bost drwy'r pyrth e-bost yn cael ei wirio am ddrwgwedd.

Mae strategaethau gwirio yn cynnwys: gwrthod negeseuon sy'n cynnwys atodiadau gweithredadwy, sganio negeseuon ar gyfer drwgwedd hysbys neu gyfuniad o'r ddwy dechneg.

Bydd yr holl negeseuon e-bost a dderbynnir gan yr ysgol yn cael eu trosglwyddo drwy hidlydd cyn cyrraedd blychau post defnyddwyr; os yw'r e-bost yn cael ei nodi fel e-bost sothach, bydd yn cael ei roi mewn cwarantin gan y system. Ni ddylai staff yr ysgol newid gosodiad nodweddion diogelwch ar eu dyfeisiau.

Dylai dilysiad aml-ffactor gael ei actifadu ar gyfrifon HWB staff er mwyn diogelu cyfrifon Office 365.

13. Monitro

Yr ysgol/Cyngor Sir Ynys Môn sy'n berchen ar y system e-bost, sy'n golygu y bydd yr holl draffig e-bost, yr anfonir ac a dderbynnir, gan gynnwys atodiadau, yn cael eu monitro a'u hadolygu a bydd unrhyw gamau gweithredu priodol yn cael eu cymryd.

Mae hyn yn golygu na ddylid cymryd bod unrhyw beth yn breifat, hyd yn oed os yw wedi'i farcio'n "breifat" a/neu'n "gyfrinachol" neu gydag unrhyw eiriad tebyg.

Bydd y monitro hwn yn sicrhau bod y polisi hwn yn effeithiol a bod defnyddwyr y system e-bost yn cadw at ei chynnwys. Mae'r monitro hefyd i sicrhau bod systemau e-bost yr ysgol yn gweithio'n iawn.

14. Mynd yn Erbyn y Polisi

Gallai peidio â chydymffurfio â'r polisi hwn gan aelodau o staff yr ysgol arwain at ganlyniadau difrifol- gallai hyn sbarduno proses disgyblu o dan polisi disgyblu mae'r ysgol wedi ei fabwysiadu.

Gall hyn arwain at roi'r unigolion y mae eu gwybodaeth bersonol yn cael ei phrosesu a'r ysgol mewn perygl.

Os bydd person nad yw'n gyflogai (h.y. gweithwyr dros dro, contractwyr eraill, gwirfoddolwyr, llywodraethwyr ac unrhyw drydydd partïon sydd efo cyfrif e-bost ysgol) yn mynd yn erbyn y polisi hwn, efallai y bydd ei gontract neu trefniant yn cael ei derfynu ar unwaith.

15. Adolygu'r Polisi a Threfniadau Arolygiaeth

Bydd y polisi hwn yn cael ei adolygu gan y Swyddog Diogelu Data Ysgolion bob tair blynedd, oni bai bod newidiadau i ddeddfwriaeth, codau ymarfer, polisi neu arweiniad yn gofyn i'r polisi gael ei ddiweddaru ynghynt.

Bydd y polisi hwn yn cael ei gymeradwyo gan Uwch Dîm Reolaeth y Gwasanaeth Dysgu gyda mewnbwn gan y Grŵp Gweithredol Diogelu Data Ysgolion a bydd yn cael ei fabwysiadu gan gorff llywodraethu'r ysgol. Bydd cydymffurfiaeth â'r polisi hwn a gweithdrefnau cysylltiedig yn cael ei fonitro gan Dîm Arweinyddiaeth a chorff llywodraethu'r ysgol.

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

E-bost: dpoysgolionmon@ynysmon.llyw.cymru

Ffôn: 01248 751833

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

Gellir cael rhagor o wybodaeth ynglŷn â diogelu data ar wefan yr ICO:
https://ico.org.uk/

Content **Page**

1. Policy Statement 17
2. Scope 17
3. Legislation, Guidance and Policies 18
4. Definitions 18
5. Responsibilities 20
5.1. School Governing Body 20
5.2. Headteacher (and/or Person Responsible for Data Protection within the School) 20
5.3. All Staff within the School 21
5.4. Schools Data Protection Officer 21
6. Sending E-mails 21
6.1. Personal and Sensitive Information within E-mails 22
6.2. E-mail Activities and Content 23
6.3. Communicating with Pupils via E-mail 24
7. E-mail Signature 24
8. Classification of Personal Information within E-mails 24
9. Retention and Secure Disposal of E-mails 25
10. E-mail Quotas and Limits 25
11. Suspicious E-mails and Links 26
12. Virus Checking 26
13. Monitoring 27
14. Breach of the Policy 27
15. Review of Policy and Oversight Arrangements 27
APPENDIX A- School Staff E-mail Policy- Headteacher's Checklist 31

1. Policy Statement

This policy outlines what the school needs to do to ensure the effective and appropriate use of e-mail by school staff. This policy will provide guidance on how to manage and thereby reduce the risks associated with e-mail for both the user and the school.

Sharing personal or sensitive information of identifiable individuals via e-mail constitutes processing personal information and therefore needs to comply with the data protection principles under the *UK General Data Protection Regulations (UK GDPR)* and the *Data Protection Act 2018*.

The school's main purpose in providing e-mail facilities is to assist school staff in the performance of their role; to provide teaching and learning activities and to assist in delivering approved business activities of the school.

Only authorised users of the school computer systems are entitled to use e-mail facilities and IT facilities provided by the school for e-mail will not be misused.

Every user of the school's e-mail systems has a duty to ensure they practice appropriate and proper use and must understand their responsibilities in this regard. There is an individual responsibility on all school staff to ensure that they manage their e-mail account correctly.

It is also critical to ensure that the information held within the e-mail systems is managed correctly. If not managed correctly, it is possible to result in inefficient work practices, information overload or loss of information that could result in a data breach.

This policy will help contribute to:

- ensuring that the school is compliant with its requirements under data protection legislation such as the *UK GDPR;* the *Data Protection Act 2018* and the *Freedom of Information Act 2000;*
- ensuring that the e-mail system is not overloaded with unnecessary workload;
- reducing information overload of unnecessary e-mail items which need to be reviewed.

2. Scope

This policy applies to all members of school staff, including temporary workers, other contractors, volunteers, governors and any and third parties with a school e-mail account.

This applies to Hwb (Welsh Government) e-mail accounts and any other official school e-mail accounts.

This policy applies to the use, for the purpose of sending or receiving e-mail messages and attachments, of any IT facilities, including hardware, software and networks, provided by the school.

Risks to both the user and the school will be managed by ensuring the proper use of e-mails by making users aware of what is acceptable and unacceptable. These are based upon both legislative requirements and internal policies and must be followed by all individuals with a school e-mail account.

School staff are expected to maintain the highest standards of professional conduct and practice and are expected to adhere to the key principles of good conduct and professional practice according to the *Education Workforce Council (EWC) Code of Professional Conduct and Practice.*

3. Legislation, Guidance and Policies

The main data protection legislation that this policy complies with is that of the *UK General Data Protection Regulation (UK GDPR)*; *Data Protection Act 2018* and the *Freedom of Information Act 2000.*

This policy should also be read in conjunction with the *Schools Data Protection Policy, Schools Information Security Policy; School Staff Social Media Policy; Schools Data Subject Access Request Policy; Schools Data Breach Policy* and *Schools Retention Schedule.*

This policy is also based on the principles of the '*Code of Professional Conduct and Practice for registrants with the Education Workforce Council (EWC)'* and the *'Education Workforce Council (EWC) Maintaining Professional Boundaries with Learners Guide to Good Practice'.*

4. Definitions

Personal data	Any information relating to an identified or identifiable natural person that can be identified either directly or indirectly from that information. This can be stored electronically, on a computer, or in paper-based filing systems.
Special category data	Information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation. Special category data is personal data that needs more protection because it is sensitive.
Processing information	Collecting, obtaining, recording, organising, structuring, storing, retaining, amending, adapting, altering, retrieving, consulting, disseminating, restricting, disclosing, destroying, erasing information or using or doing anything with it.

Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed information.
E-mail	Messages distributed by electronic means from one computer user to one or more recipients via a network. In addition to textual content, e-mail allows the sender to send photographs, video or sound clips in digital form or files.
Mailbox	The destination to which electronic mail messages are delivered. It is the equivalent of a letter box in the postal system.
Unauthorised	Without a legitimate right.
Cyber security	Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorised access.
Hackers	A hacker is an individual who uses a computer, networking or other skills to overcome a technical problem and who illegally gains access to and sometimes tampers with information in a computer system.
Cyber attack	A cyber-attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.
Threat	Potential cause of an unwanted incident, which can result in harm to a system or organisation.
Risk	Effect of uncertainty on objectives. Risks to individuals: the potential for damage or distress. Risk is often characterised by reference to potential “events” and “consequences”, or a combination of these.
Risk Assessment	The identification and analysis of risks to the organisation’s business objectives.
Impact	What are the consequences of the risk were it to occur. Impact is considered as having either an immediate effect or a future effect.
Likelihood	How likely is it that the risk will occur- uncertainty, chance and probability.
Control	Measure that is modifying risk.
Phishing	Scammers send fake emails to thousands of people asking for sensitive information (such as bank details) or containing links to bad websites. They do this to steal details to sell or perhaps to access information held by organisations.
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
Flaming	A virtual term for venting or sending inflammatory messages in an e-mail.

Spam	Irrelevant or unsolicited messages sent over the internet/e-mail, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.
Computer Virus	A computer virus is a kind of malicious computer program, which when executed, replicates itself and inserts its own code. When the replication is done, this code infects the other files and program present on the system.
Spyware	Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.
Trojan horses	A program designed to breach the security of a computer system while ostensibly performing some innocuous function.
Cyber bullying	Any use of social media or communication technology to bully an individual or group.
Encryption	Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data appears scrambled or unreadable to a person or entity accessing without permission.
Authentication	Authentication is the process of determining if someone (or something is who (or what) it claims to be.
Two-factor authentication (2FA)	Two-factor authentication, abbreviated as 2FA, is an authentication process that requires two different authentication factors to establish identity- it means requiring a user to prove their identity in two different ways before granting them access to a system.
Anonymised	To remove identifying information from something (such as computer data) so that the original source cannot be known or identified.

5. Responsibilities

5.1. School Governing Body

The school governing body has the responsibility for:

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

5.2. Headteacher (and/or Person Responsible for Data Protection within the School)

The Headteacher and/or the person who is responsible for data protection within the school is responsible for:

- ensuring the implementation of this policy and promoting understanding and compliance with this policy;
- monitoring the implementation and compliance with this policy;

- ensuring personal information within e-mails are kept and processed in line with *UK GDPR*; *Data Protection Act 2018* and the *Freedom of Information Act 2000*;
- ensuring that all staff comply with the *Schools Retention Schedule* and that the school carries out regular housekeeping activities relating to e-mails;
- ensuring that classification levels are used appropriately;
- ensuring staff have appropriate training for using e-mails;
- monitoring that school staff adhere to the principles of the *Code of Professional Conduct and Practice for registrants with the Education Workforce Council (EWC);*
- mandating the use of Multi Factor Authentication in staff HWB accounts in order to protect Office 365 accounts.

5.3. All Staff within the School

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

- ensuring understanding and compliance with this policy;
- ensuring the practice of appropriate and proper use of e-mail;
- managing individual school e-mail accounts correctly;
- not using personal or unauthorised e-mail accounts to share personal or sensitive data relating to the school;
- ensuring personal information within e-mails are kept and processed in line with *UK GDPR*; the *Data Protection Act 2018* and the *Freedom of Information Act 2000;*
- adhering to the principles of the *Code of Professional Conduct and Practice for registrants with the Education Workforce Council (EWC);*
- appropriately using classification levels in relation to e-mails;
- fully complying with the *Schools Retention Schedule*;
- keeping within the e-mail account quota;
- being cautious of suspicious e-mails and links;
- undertaking all training offered on using e-mails.

5.4. Schools Data Protection Officer

The Schools Data Protection Officer is responsible for:

- providing advice and guidance to the school regarding information protection and security regarding e-mail use;
- monitoring the implementation and compliance of this policy by the school;
- providing advice and support and leading on the reporting of data breaches relating to personal and sensitive information contained within e-mails.

6. Sending E-mails

School staff should consider whether an e-mail is really required before sending an e-mail.

Standard e-mail is not a secure form of communication. The messages that are sent may be over networks owned by other people. A more secure method of communication will be used, if the content of an e-mail is sensitive or critical such that if the contents were disclosed or modified by an unauthorised person it could cause embarrassment, distress or financial loss. Care needs to be taken that the potential consequences of sending messages are appreciated.

The individual logged in at a computer will be considered to be the author of any messages sent from that computer account. All school staff will log off or lock their computers when away from their desks; under no circumstances should a user send a message from somebody else's account.

When sending an e-mail, the sender must check that the recipient e-mail address is correct and that no-one else that should not receive the e-mail is copied in as a recipient. It is very easy to send an e-mail to the wrong recipient.

If sending any e-mail where there is a need to conceal individual e-mail addresses, the blind copy facility (bcc) should be used. The blind copy facility should be used when sending to a large number of recipients (particularly external).

Consideration needs to be given before responding to a group e-mail or copying others in the e-mail, if all the recipients need to receive the information. School staff should not send e-mails to all staff unless it is necessary and appropriate for all staff to receive the information.

6.1. Personal and Sensitive Information within E-mails

School staff will not use their personal or an unauthorised e-mail account to send or receive any personal or sensitive data relating to the school or its staff or pupils.

E-mail should not be used to send sensitive personal information without first applying a level of password protection appropriate to the sensitivity of the data.

By default, HWB's e-mail system is configured to encrypt its conversation with other e-mail systems while sending and receiving messages. Please see guide- 'Encrypting e-mail sent from HWB addresses' on the IT Portal for guidance on this- https://desggymorth.ynysmon.gov.uk/support/solutions/articles/50000102041-encrypting-email-sent-from-hwb-addresses-

If sensitive personal information has to be shared via e-mail, the relevant information should be saved in to a Microsoft Word or Excel document. The document should then be password protected and sent as an e-mail attachment. The password should be separately and securely shared with the intended recipient. Otherwise, personal information will need to be de-personalised.

It may be appropriate to use initials instead of full names within e-mails or use a unique identifier where only school staff are able to recognise the individual.

It may be appropriate to ask the recipient to confirm that they have received the e-mail if it contains personal information.

If e-mails containing personal or sensitive information is shared with an unintended recipient or is lost or accessed by an unauthorised user, there may be a data breach that will need to be reported immediately to the Schools Data Protection Officer. The school will comply with the *Schools Data Breach Policy.*

6.2. E-mail Activities and Content

The following are examples of activities and usage that is prohibited by school staff on official school e-mail accounts:

- activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users;
- activities that corrupt or destroy other users' data or disrupt the work of other users;
- unreasonable or excessive personal use;
- activities that violate the privacy of others or unfairly criticise or misrepresent others; this includes copying distribution to other individuals;
- enabling the unauthorised provision of access to school services and facilities by third parties.

No school staff will send or forward e-mails that in any way may be interpreted as insulting, disruptive or offensive by any other person, or company. Examples of prohibited material include but are not limited to:

- illegal material;
- confidential material concerning the activities of the school to a third party;
- sexually explicit messages, images, cartoons, jokes or movie files;
- indecent images, data or other material;
- profanity, obscenity, slander or libel;
- any message which could be viewed as demonstrating hate crime on the basis of race, religion, disability, sexual orientation, transgender identity;
- political beliefs or commentary;
- any message which could be viewed as abusive, threatening, offensive or as harassment, bullying, discrimination or disparagement of others based on their gender, race, ethnicity, sexual orientation, age, marital status, national origin, disability or religious or political beliefs;
- defamatory material or material that includes claims of a deceptive nature;
- anonymous messages or deliberately forging messages or e-mail header information (i.e. without clear identification of the sender) or for 'flaming';
- material which is designed or likely to cause annoyance, inconvenience or anxiety;

- unwelcome propositions;
- unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind.

6.3. Communicating with Pupils via E-mail

School staff will only use an authorised e-mail account to communicate in respect of school business.

School staff will not use their personal e-mail account to communicate with pupils or their family/carers.

7. E-mail Signature

It is good practice to set-up a bilingual signature on e-mail accounts. The signature will appear at the end of e-mail messages. This should contain the school staff's name and contact details. These details should be kept up-to-date.

Setting up a bilingual signature ensures the school presents a professional image and informs the recipient of who the sender is and ways to get in touch.

8. Classification of Personal Information within E-mails

E-mails containing personal and special categories data must be identified using data classification terms (OFFICIAL or OFFICAL-SENSITIVE) within the subject field of the e-mail.

The information classification category is determined on the **harm** that could result from loss or unauthorised disclosure of the information. Information classification category determines how information must be protected/handled.

Classification Category	Impact if the information is lost or disclosed to unauthorised people	Examples of Information
OFFICIAL	Almost all the information the school comes into contact with during the course of the working day will be OFFICIAL information. However, OFFICIAL information also includes personal data that is already in the public domain that if disclosed without consent or loss, would not cause harm or distress to any individual.	Routine reports, published annual reports, out-turn data for key performance indicators, information that is freely available e.g. information on the school website; employees' names and job titles and information that is not commercially sensitive.
OFFICIAL-SENSITIVE	• Cause harm or distress to individuals; • Breach statutory restrictions on the disclosure of information; • Would lead to a breach of confidence to third parties (where	Pupil or staff information for which the school has a duty of care e.g. names, addresses, pupil record.

	information is not in the public domain); • Cause substantial harm or distress to individuals or groups; • Prejudice the investigation or facilitate the commission of crime.	

Personal information should not be included in the subject field of the e-mail.

9. Retention and Secure Disposal of E-mails

School e-mail accounts will also be subject to the data protection regulations and the *Schools Retention Schedule* must be followed regarding e-mails.

School staff will not use their official school e-mail account to store information and as a filing or case management system. E-mail systems should be thought of as a way of delivering and receiving messages- they are not intended for the long term storage and retrieval of messages and attachment files.

E-mails will be deleted or filed as appropriate. E-mails that need to be deleted will be deleted and e-mails that need to be kept in line with the *Schools Retention Schedule* will need to be transferred to an appropriate network folder. The *Schools Retention Schedule* should be applied within the relevant filing system in order to comply with *UK GDPR.* School staff should clean up their e-mail mailbox on a regular basis.

Personal information within e-mails may be provided to individuals as part of Data Subject Access Requests. The school will follow the *Schools Data Subject Access Request Policy.*

Where there is any uncertainty, the school should consult with the Schools Data Protection Officer for guidance on how long to retain e-mails.

E-mails that are no longer required according to the *Schools Retention Schedule* will be deleted permanently from the school's information systems.

Any hard copies of personal information contained within an e-mail will be destroyed in a secure manner.

The *Schools Retention Schedule* can be found on the Data Protection page on the Learning Service Microsite.

10. E-mail Quotas and Limits

All accounts have quota limits placed on them.

Users will receive e-mail notification when approaching their quota limit and are encouraged to follow guidance in this e-mail to manage their account. Once over quota no further e-mails can be delivered to an individual's inbox until they have reduced their storage below their limit.

E-mail that fails to be delivered because a user is over quota is held in the local mail queues for four days and the system will retry periodically to deliver. After four days the e-mail is returned to sender.

E-mail folders will be reviewed regularly by the user and any non-essential messages will be deleted or saved within folders. There are several ways to reduce the mailbox size:

- finding and deleting/transferring large e-mails to an appropriate network folder;
- finding and deleting/transferring old e-mails to an appropriate network folder;
- cleaning up duplicate e-mails from ongoing conversations.

E-mails containing large or multiple attachments should not be sent unnecessarily.

11. Suspicious E-mails and Links

School staff should be wary of unexpected e-mails, attachments and links. E-mails, attachments and links will not be opened unless they are from a known source. Malicious files or links sent via e-mail have the potential to capture passwords, steal school data and render workstations or even the school's network unusable.

Should users receive e-mails which appear suspicious (for example, e-mails with suspect subjects lines) they are advised not to open the e-mail or any included attachments. Instead the e-mail should be deleted and the 'deleted items' emptied.

Caution will be exercised before attachments and links received within e-mails are opened. This will be the case even if the e-mail is from a known source.

The Isle of Anglesey County Council's ICT Service Desk should be notified of any suspicious e-mails so that any pattern of a wider problem or attack can be identified at the earliest opportunity and preventative action taken.

12. Virus Checking

Computer viruses, trojan horses and worms are collectively known as malware. One common method of distributing malware is via e-mail. All e-mail communication through the e-mail gateway is checked for malware.

Checking strategies include: refusing messages containing executable attachments, scanning messages for known malware or a combination of both techniques.

All e-mail received by the school will be passed through a filter before reaching users mailboxes; if the e-mail is identified as Spam, it will be quarantined by the system. School staff should not change the setting of security features on their devices.

Multi Factor Authentication should be activated within staff HWB accounts in order to protect Office 365 accounts.

13. Monitoring

The school/Isle of Anglesey County Council owns the e-mail system which means that all e-mail traffic, both sent and received, including attachments, will be monitored and reviewed and any action deemed appropriate will be taken.

This means that nothing should be taken to be private, even if marked as “private” and/or “confidential” or with any similar wording.

This monitoring will make sure that this policy is effective and that users of the e-mail system are abiding by its content. The monitoring is also to ensure that the school’s e-mail systems are working properly.

14. Breach of the Policy

Non-compliance with this policy by members of school staff could lead to serious consequences- this could trigger a disciplinary process under the school’s adopted disciplinary policy.

This can lead to putting both the individuals whose personal information is being processed and the school at risk.

If a non-employee breaches this policy (i.e. temporary workers, other contractors, volunteers, governors and any and third parties with a school e-mail account), they may have their contract or arrangement terminated with immediate effect.

15. Review of Policy and Oversight Arrangements

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

This policy will be approved by the Learning Service Senior Management Team with the input of the Schools Data Protection Operational Group and will be adopted by the school governing body. Compliance with this policy and related procedures will be monitored by the School Leadership Team and the governing body.

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

E-mail: dpoysgolionmon@ynysmon.llyw.cymru

Telephone: 01248 751833

Address:
Learning Service
Isle of Anglesey County Council
Council Offices

Llangefni
Anglesey
LL77 7TW

Further information regarding data protection can be obtained from the ICO website: https://ico.org.uk/

ATODIAD A

Polisi E-bost Staff Ysgolion

Rhestr Wirio'r Pennaeth

Rhif	Camau Gweithredu	A oes gan yr ysgol hyn ar waith (Oes/Nac oes)/ (Sylwadau/Dyddiadau etc.)
1	Mae'r fersiwn cyfredol o'r *Polisi E-bost Staff Ysgolion* wedi ei fabwysiadu'n ffurfiol gan gorff llywodraethu'r ysgol.	
2	Mae proses ar waith i fonitro cydymffurfiad yr ysgol â'r polisi hwn yn barhaus.	
3	Mae gwybodaeth bersonol mewn e-byst yn cael ei chadw a'i phrosesu yn unol â *UK GDPR*; *Deddf Diogelu Data 2018* a *Deddf Rhyddid Gwybodaeth 2000.*	
4	Mae'r holl staff yn cydymffurfio â'r *Cyfnodau Cadw Ysgolion* ac mae'r ysgol yn cynnal gweithgareddau cadw tŷ rheolaidd mewn perthynas ag e-byst.	
5	Defnyddir lefelau dosbarthu yn briodol – SWYDDOGOL a SWYDDOGOL-SENSITIF.	
6	Mae staff wedi derbyn hyfforddiant priodol ar gyfer defnyddio e-byst.	
7	Nid yw staff yn defnyddio cyfrifon e-bost personol neu anawdurdodedig i rannu data personol neu sensitif yn ymwneud â'r ysgol.	
8	Mae staff yn ymwybodol i fod yn wyliadwrus o e-byst a dolenni cyswllt amheus a bob amser yn wyliadwrus a byddant yn adrodd ar y rhain i Ddesg Gymorth TGCh Cyngor Sir Ynys Môn.	
9	Mae staff yn defnyddio'r cyfleuster copïo dall (bcc) wrth anfon e-byst lle mae angen cuddio cyfeiriadau e-bost unigol.	
10	Mae staff yn defnyddio'r swyddogaeth amgryptio ar eu cyfrif HWB neu ddogfen wedi'i diogelu â chyfrinair mewn e-byst wrth anfon gwybodaeth bersonol sensitif.	
11	Mae staff yn defnyddio blaenlythrennau yn hytrach nag enwau llawn mewn e-byst neu'n defnyddio dynodwr unigryw lle mai dim ond staff yr ysgol a all adnabod yr unigolyn.	

12	Mae staff yr ysgol bob amser yn hysbysu'r Pennaeth os rhennir e-byst sy'n cynnwys gwybodaeth bersonol neu sensitif gyda derbynnydd na fwriadwyd neu os caiff ei cholli neu ei chyrchu gan ddefnyddiwr anawdurdodedig.	
13	Mae staff yn adolygu eu ffolderi e-bost yn gyson ac mae unrhyw negeseuon nad ydynt yn hanfodol un ai'n cael eu dileu neu eu harbed mewn ffolderi.	
14	Mae'r ysgol yn dilyn y *Polisi Ceisiadau gan Wrthrych y Data* ac mae e-byst yn ffurfio rhan o'r chwiliad am wybodaeth bersonol fel rhan o Geisiadau gan Wrthrych y Data.	
15	Mae gan staff lofnod dwyieithog ar eu cyfrifon e-bost.	
16	Nid yw staff yn defnyddio eu cyfrif e-bost ysgol yn afresymol neu'n ormodol at ddefnydd personol.	
17	Mae dilysiad aml-ffactor wedi ei alluogi yn HWB ar gyfer holl staff.	

APPENDIX A

School Staff E-mail Policy

Headteacher's Checklist

No	Actions to be Taken	Has the school got this in place (Yes/No)/ Comments/Dates etc.)
1	The current version of the *School Staff E-mail Policy* has been formally adopted by the School Governing Body.	
2	There is a process in place to continually monitor the school's compliance with this policy.	
3	Personal information within e-mails are kept and processed in line with *UK GDPR*; *Data Protection Act 2018* and the *Freedom of Information Act 2000.*	
4	All staff comply with the *Schools Retention Schedule* and the school carries out regular housekeeping activities relating to e-mails.	
5	Classification levels are used appropriately- OFFICIAL and OFFICIAL-SENSITIVE.	
6	Staff have received appropriate training for using e-mails.	
7	Staff do not use personal or unauthorised e-mail accounts to share personal or sensitive data relating to the school.	
8	Staff are aware to be cautious of suspicious e-mails and links and are always cautious and will report these to the Isle of Anglesey County Council's ICT Service Desk.	
9	Staff use the blind copy facility (bcc) when sending e-mails where there is a need to conceal individual e-mail addresses.	
10	Staff use the encryption function on their HWB account or password protect documents within e-mails if sending sensitive personal information.	
11	Staff use initials instead of full names within e-mails or use a unique identifier where only school staff are able to recognise the individual.	

12	School staff always inform the Headteacher if e-mails containing personal or sensitive information is shared with an unintended recipient or is lost or accessed by an unauthorised user.	
13	Staff regularly review their e-mail folders and any non-essential messages are either deleted or saved within folders.	
14	The school follows the *Schools Data Subject Access Request Policy* and e-mails form part of the search for personal information as part of Data Subject Access Requests.	
15	Staff have a bilingual signature on their e-mail accounts.	
16	Staff do not unreasonably or excessively use their school e-mail account for personal use.	
17	Multi Factor Authentication has been enabled in HWB on all staff accounts.	