Arolygiaeth Ei Mawrhydi dros Addysg a Hyfforddiant yng Nghymru
Her Majesty's Inspectorate for Education and Training in Wales

Polisi Sicrhau Gwybodaeth

Taflen wybodaeth

Blwch gwybodaeth

I gael cyngor pellach, cysylltwch â'r: Grŵp Rheoli Gwybodaeth

Dyddiad cyhoeddi: Gorffennaf 2021

Fersiwn: 4.0

Rheoli fersiwn

Fersiwn o'r ddogfen	Awdur	Dyddiad cyhoeddi	Prif newidiadau a wnaed
1.0	Phil Sweeney	Mai 2012	
2.0	Grŵp Rheoli Gwybodaeth	Rhagfyr 2013	Diweddarwyd i adlewyrchu newidiadau i Gynllun Marcio Amddiffynnol y Llywodraeth
2.1	Grŵp Rheoli Gwybodaeth	Mawrth 2016	Mân ddiwygiadau yn dilyn archwiliad mewnol
3.0	Grŵp Rheoli Gwybodaeth	Mai 2018	Diweddarwyd i adlewyrchu cyflwyno'r Rheoliadau Cyffredinol ar Ddiogelu Data
4.0	Grŵp Rheoli Gwybodaeth	Gorffennaf 2021	Tôn llais. Ychwanegwyd canllaw ar 'gyfarwyddiadau trin. Dilëwyd yr atodiadau ('Marciau amddiffynnol' a 'Trefniadau ar gyfer anfon gwybodaeth trwy'r post a'r e-bost) – caiff y rhain eu cwmpasu gan gyfarwyddiadau desg lleol a gyhoeddwyd gan y PAG perthnasol.

Asesiad o'r Effaith ar Gydraddoldeb

Cynhaliwyd asesiad o resymwaith busnes ac mae'r polisi hwn yn cyfrannu at amcanion strategol ac egwyddorion cyflawni Estyn.

Yn unol ag Asesiad Estyn o Effaith ar Gydraddoldeb, cynhaliwyd asesiad cychwynnol o effaith sgrinio ac ystyrir nad yw'r polisi hwn yn cael effaith niweidiol ar sail y naw nodwedd warchodedig fel y'u diffinnir yn Neddf Cydraddoldeb 2010.

Cynnwys	Tudalen

Adran 1: Cyflwyniad

1 Mae gan Estyn ddyletswydd i gynnal diogeledd y wybodaeth y mae'n ei thrin – mae hyn yn golygu diogelu data rhag mynediad anawdurdodedig, sicrhau ei chywirdeb a'i huniondeb, a threfnu bod y wybodaeth ar gael i'r rhai sydd ei hangen.

2 Mae'r polisi hwn yn rhan o'n fframwaith o bolisïau a gweithdrefnau ar reoli gwybodaeth ac mae'n berthnasol i'r holl gyflogeion a phobl sy'n gweithio ar ein rhan. Rhaid i staff a phobl eraill sy'n gweithio i ni ddilyn y rheolau, polisïau a'r canllawiau a ddatblygwyd gennym. Hefyd, rhaid iddynt ddeall eu cyfrifoldebau personol wrth greu, rhannu a storio gwybodaeth mewn perthynas â'n gwaith.

3 Rheolwyr llinell sy'n gyfrifol am sicrhau bod staff asiantaethau yn cydymffurfio â'r polisi hwn. Ar gyfer arolygwyr allanol ac unigolion eraill sy'n gweithio i ni (e.e. drwy gontractau ar gyfer gwasanaethau a memoranda cyd-ddealltwriaeth), bydd cydymffurfio â'r polisi hwn wedi'i gynnwys yn y cytundebau, telerau ac amodau a'r arweiniad y byddwn yn eu cyhoeddi pan fyddant yn dechrau gweithio i ni.

Ein dull o reoli gwybodaeth

4 Mae'r pwyntiau canlynol yn disgrifio ein dull ar gyfer sicrhau gwybodaeth:

- Mae'r Grŵp Rheoli Gwybodaeth yn gyfrifol am oruchwylio ein polisïau sy'n gysylltiedig â gwybodaeth a rheoli risg. Mae'r grŵp hefyd yn gyfrifol am roi arweiniad a hyfforddiant i staff ar sut i drin gwybodaeth.
- Bydd unigolyn wedi'i enwi (Perchennog Asedau Gwybodaeth neu 'PAG') yn gyfrifol am y wybodaeth a gedwir ym mhob system neu faes gwaith. Bydd ef neu hi'n cael hyfforddiant ychwanegol.
- Bydd PAGau yn gyfrifol am nodi pob math o wybodaeth (asedau gwybodaeth) sy'n cael ei chadw, ei chynhyrchu neu'i derbyn gan eu maes busnes, a sicrhau y caiff ei storio mewn systemau priodol.
- Bydd asedau gwybodaeth yn cael eu dosbarthu gyda marciau amddiffynnol, yn ôl eu sensitifrwydd a pha mor ddifrifol y byddai'r niwed posibl o'u datgelu neu'u colli. Caiff y marciau amddiffynnol hyn eu diffinio gan ganllawiau'r llywodraeth. Mae PAGau yn gyfrifol am gyfleu a monitro'r defnydd o'r marciau hyn a'r cyfarwyddiadau ar gyfer eu trin yn eu maes busnes.
- Bydd y PAG yn gyfrifol am asesu'r risgiau sy'n gysylltiedig â dal pob ased gwybodaeth, ac am nodi'r ffyrdd i ddileu, lliniaru neu dderbyn y risgiau hyn.
- Gallai'r PAG gynyddu perchnogaeth a rheolaeth y risg i lefel briodol, yn unol â'n Polisi Rheoli Risg.
- Byddwn yn cynnal ac yn dilyn proses ar gyfer adrodd am achosion yn ymwneud â gwybodaeth a'u rheoli.

5 Caiff y rheolau cyffredinol ar gyfer trin gwybodaeth eu pennu gan PAGau ac uwch aelodau staff eraill. Ar gyfer darnau unigol o wybodaeth, y rhai sy'n derbyn, yn defnyddio ac yn dal y wybodaeth honno'n uniongyrchol fydd yn gyfrifol am ei chadw'n ddiogel. Bydd yr holl staff yn gyfrifol am ddefnyddio a thrin gwybodaeth o ddydd i ddydd, a byddwn yn eu cynorthwyo â hyfforddiant ac arweiniad.

Adran 2: Dosbarthu gwybodaeth: Marcio amddiffynnol a thrin gwybodaeth yn ddiogel

Marciau amddiffynnol

6 Mae Swyddfa'r Cabinet wedi gorchymyn defnyddio marciau amddiffynnol i helpu diogelu gwybodaeth y llywodraeth – byddwn yn defnyddio'r marciau hyn i ddangos sensitifrwydd 'ased'.

7 Dylai dogfennau unigol a data yn ymwneud â'r ased gwybodaeth gael eu marcio'n ffisegol (yn electronig) pan gânt eu creu. Fodd bynnag, mewn rhai meysydd (er enghraifft mewn negeseuon e-bost neu ddogfennau papur), rhaid i'r sawl sy'n anfon neu'n derbyn y ddogfen sicrhau bod y marciau amddiffynnol yn cael eu rhoi. Yn ddiofyn, byddwn yn cadw'r dosbarthiad a nodwyd gan y ffynhonnell. Os na fydd y ffynhonnell yn rhoi dosbarthiad, neu os defnyddiwyd dosbarthiad anhysbys, rhaid i'r derbynnydd adolygu'r cynnwys a rhoi marc amddiffynnol ar y wybodaeth, fel y bo'n briodol.

8 Rhaid i'n gwybodaeth gael ei labelu â'r marc amddiffynnol priodol. Rhaid i'r marciau hyn fod mewn priflythrennau trwm a'u rhoi ym mhenynnau a/neu droedynnau'r ddogfen.

9 Disgwylir y bydd y mwyafrif o'n gwybodaeth yn annosbarthedig ac na fydd angen unrhyw farc amddiffynnol arni. Yr unig lefel o ddosbarthiad a ddefnyddir yn Estyn fydd **SWYDDOGOL.**

10 Os caiff gwybodaeth sydd wedi'i marcio'n **SWYDDOGOL** ei rhyddhau, mae'n debygol o:

- achosi trallod sylweddol i unigolion
- torri cyfrinachedd, a fydd yn lleihau ymddiriedaeth pobl ynom
- torri cyfyngiadau statudol yn ymwneud â datgelu gwybodaeth

11 Yn dibynnu ar ddifrifoldeb yr amgylchiadau, gallai:

- achosi colled ariannol, neu hwyluso elw neu fantais amhriodol i unigolion neu gwmnïau
- peryglu'r ymchwiliad neu hwyluso troseddu
- rhoi'r llywodraeth dan anfantais mewn trafodaethau masnachol neu bolisi â phobl eraill
- amharu ar ddatblygu neu weithredu polisïau'r llywodraeth yn effeithiol
- torri cyfyngiadau statudol yn ymwneud â datgelu gwybodaeth
- tanseilio rheolaeth briodol y sector cyhoeddus a'i weithrediadau

12 Dylai'r marc **SWYDDOGOL** gael ei ddilyn gan gyfarwyddiadau trin. Mae enghreifftiau'n cynnwys:

- '*Ar gyfer y sawl y cyfeirir ato'n unig'* – dim ond yr unigolyn yr anfonwyd y wybodaeth ato/ati'n wreiddiol a ddylai ei gweld

- '*At ddefnydd Adnoddau Dynol yn unig'* – ni ddylai'r wybodaeth gael ei rhannu y tu allan i'r tîm Adnoddau Dynol (gellir defnyddio cyfarwyddiadau tebyg ar gyfer grwpiau eraill e.e. UDRh)
- '*Ymgynghorwch â'r sawl a greodd y wybodaeth cyn ei rhannu ymhellach'* – gofynnwch i'r unigolyn a greodd y wybodaeth a chewch ei rhannu â rhywun arall rydych chi'n credu y mae angen iddo/iddi ei gweld
- '*Peidiwch â rhannu'n allanol'* – gallai hyn fod yn berthnasol i wybodaeth sydd i'w defnyddio'n fewnol yn unig neu ddogfen nad yw'n barod i'w chyhoeddi e.e. adroddiad arolygu drafft neu gyhoeddiad sydd dan embargo

13 Dylai PAGau gynnwys y cyfarwyddiadau trin ar gyfer gwybodaeth a dogfennau y mae angen marciau amddiffynnol arnynt sy'n cael eu cofnodi yn eu Cofrestrau Asedau Gwybodaeth. Dylid cynnwys marciau amddiffynnol a chyfarwyddiadau trin, fel y bo'n briodol, ar dempledi ffurflenni a dogfennau eraill, a chyfeirio atynt yn y cyfarwyddiadau desg perthnasol ar gyfer prosesu gwybodaeth. Bydd ond angen marcio ffurflen wag os yw'n cynnwys gwybodaeth sensitif. Gellir argraffu rhai ffurflenni gwag, sy'n cynnwys gwybodaeth sensitif ar ôl eu llenwi bob tro, â'r marciau arnynt yn barod. Bydd y Grŵp Rheoli Gwybodaeth yn adolygu'r cofrestrau hyn yn flynyddol er mwyn sicrhau eu bod yn briodol.

14 Pan gaiff gwybodaeth ei diweddaru, rhaid i chi ailystyried lefel yr effaith a'r broses drin gysylltiedig. Gallai lefel yr effaith newid dros amser, er enghraifft pan gaiff dogfen ei chyhoeddi.

15 Pan gaiff gwybodaeth ei chronni mewn un lle (er enghraifft cronfa ddata, cabinet ffeilio neu ddyfais storio allanol wedi'i hamgryptio), rhaid ystyried lefel yr effaith ar gyfer y wybodaeth gyfunol. Rhaid ei marcio'n glir ar y clawr hefyd. Rhaid i'r marcio adlewyrchu'r lefel uchaf o sensitifrwydd mewn unrhyw eitem unigol o fewn y casgliad o ddata.

Mynd at wybodaeth sydd wedi'i marcio yn amddiffynnol

16 Rydym yn gweithredu polisi agored ar gyfer rhannu gwybodaeth annosbarthedig. Fodd bynnag, efallai y bydd angen cyfyngu'n fewnol ar fynediad at wybodaeth sydd â marc amddiffynnol.

17 Mae PAGau yn gyfrifol am oruchwylio'r mynediad a roddir at wybodaeth; dylid rhoi mynediad ar sail yr hyn y mae angen ei wybod yn unig, yn enwedig pan fydd y data'n sensitif.

18 Rhaid i PAGau a rheolwyr roi arweiniad ar drin data i unrhyw un sy'n gallu mynd at ddata sensitif sydd wedi'i storio ar ein systemau. Fel arfer, bydd yr arweiniad hwn yn cael ei roi drwy gyfarwyddiadau desg ar gyfer y broses fusnes benodol. Mae unigolion yn gyfrifol am ddilyn y cyfarwyddiadau hyn.

19 Dylai PAGau adolygu hawliau mynediad at systemau a gwybodaeth sydd wedi'u diogelu yn rheolaidd, er mwyn gwneud yn siŵr fod hawliau mynediad aelodau staff sy'n newid rolau neu'n gadael y sefydliad yn cael eu newid neu eu dileu.

20 Pan fydd prosesau busnes newydd yn cael eu sefydlu a fydd yn mynnu defnyddio marciau amddiffynnol, rhaid i'r PAG gynnal asesiad risg cyn rhoi'r broses ar waith. Mae hyn yn cynnwys gosod hawliau mynediad.

21 Mewn rhai amgylchiadau, efallai y bydd yn rhaid datgelu gwybodaeth sydd wedi'i marcio'n amddiffynnol i'r cyhoedd dan ofynion Rhyddid Gwybodaeth.

Diogelu gwybodaeth sensitif

22 Rhaid i staff sicrhau nad yw gwybodaeth sydd wedi'i marcio'n amddiffynnol yn cael ei datgelu i unrhyw un arall, oni bai bod gan yr unigolyn hwnnw'r awdurdod i'w chael.

23 Wrth ddarllen ac adolygu gwybodaeth, dylech fod yn ymwybodol o'r risg o golli data. Peidiwch â gadael dogfennau sydd wedi'u marcio'n **SWYDDOGOL** ar eu pen eu hunain, er enghraifft ar ddesgiau neu beiriannau argraffu yn y swyddfa neu gartref. Dilynwch ein polisi desg glir drwy roi dogfennau sydd wedi'u marcio'n amddiffynnol i'w cadw dan glo pan fyddwch yn gadael eich desg e.e. pan fyddwch yn mynd am ginio neu'n gorffen gwaith ar ddiwedd y dydd.

24 Peidiwch â thrafod unrhyw wybodaeth sensitif mewn lle cyhoeddus lle gall rhywun eich clywed. Hyd yn oed mewn sefyllfaoedd gwaith, ystyriwch pwy allai glywed eich sgyrsiau, eich galwadau ffôn neu gynadleddau fideo, a symudwch i ystafell breifat yn ôl yr angen.

25 Mae Cadeirydd cyfarfodydd yn gyfrifol am sicrhau bod gan y rhai sy'n bresennol hawl i weld y wybodaeth sy'n cael ei thrafod. Os ydych yn mynychu cyfarfod ac nad ydych yn siŵr beth y gallwch ei ddweud (neu ei glywed), yna gofynnwch i'r Cadeirydd gadarnhau.

26 Dylech bob amser roi'r clo ar eich cyfrifiadur pan fyddwch yn symud oddi wrtho drwy bwyso CTRL+ALT+DEL wedyn 'Enter'. Diffoddwch eich cyfrifiadur yn gyfan gwbl pan fyddwch wedi gorffen gwaith am y diwrnod neu os na fyddwch wrtho am gyfnod hir.

27 Gall storio gwybodaeth ar gyfryngau symudol beri mwy o risg o'i cholli neu ei rhannu'n amhriodol – dilynwch y Polisi ar Ddefnyddio TGCh wrth ddefnyddio cyfryngau symudol.

28 Peidiwch fyth â chadw data ar yriant caled cyfrifiaduron bwrdd gwaith. Yn wahanol i liniaduron, nid yw ein cyfrifiaduron bwrdd gwaith wedi'u hamgryptio, felly nid ydynt yn cynnig y lefel briodol o ddiogelu data os bydd y ddyfais yn cael ei dwyn neu os bydd rhywun heblaw'r defnyddiwr yn mynd ati. Defnyddiwch eich Gyriant Y neu'ch *One Drive* i gadw unrhyw ddata'n lleol.

29 Dylech gymryd pob cam rhesymol i ddiogelu eich gliniadur, yn unol â'n Polisi ar Ddefnyddio TGCh, p'un a ydych chi'n teithio neu yn eich cartref. Cofiwch fod amgryptio gliniadur dim ond yn gweithio pan fydd y cyfrifiadur wedi'i ddiffodd yn llawn.

30 Gallwch leihau'r risg o bobl anawdurdodedig yn darllen data drwy:

- leihau faint o wybodaeth bapur rydych chi'n ei chadw gyda chi neu'n ei storio gartref

- argraffu dogfennau dim ond pan fydd wir angen i chi wneud hynny
- storio dogfennau sydd wedi'u marcio'n amddiffynnol yn ddiogel (e.e. mewn cabinet ffeilio) pan nad ydynt yn cael eu defnyddio

31 Dylech ddileu negeseuon e-bost a ffeiliau ar unwaith pan na fydd eu hangen mwyach.

32 Rhaid i chi waredu gwybodaeth mewn ffordd sy'n golygu y bydd yn annhebygol adfer neu adalw'r cynnwys. Y Swyddog Diogeledd TG sy'n gyfrifol am oruchwylio'r gwaith o gael gwared ar yr holl offer TG yn ddiogel.

33 Yn y swyddfa, dylech ddefnyddio'r biniau papur priodol i waredu gwybodaeth sensitif. Gartref, storiwch unrhyw ddogfennau sensitif yn ddiogel a'u gwaredu yn y brif swyddfa, os yw'n bosibl, neu defnyddiwch beiriant rhwygo.

Trydydd partïon

34 Dylai staff sy'n gyfrifol am ymgysylltu â thrydydd partïon sicrhau bod cyflenwyr yn cydymffurfio â'r polisi hwn. Mae'r holl delerau ac amodau ffurfiol i gyflenwyr yn cynnwys protocolau ar gyfer diogelu data y mae'n rhaid eu dilyn.

Adran 3: Adrodd am achosion diogeledd gwybodaeth ac achosion trwch blewyd

35 Mae achos diogeledd gwybodaeth yn digwydd pan fydd gwybodaeth sensitif yn cael ei cholli, ei dwyn, neu ei rhyddhau i bartïon anawdurdodedig neu ei gweld ganddynt, er enghraifft:

- colli gliniadur neu gyfryngau symudol
- ceisio cael mynediad anawdurdodedig at ddata sensitif yn un o'n systemau, neu lwyddo i wneud hynny
- datgelu gwybodaeth am staff neu'r rhai rydym yn eu harolygu heb fod gennych yr awdurdod i wneud hynny
- anfon neges e-bost neu lythyr i un cyfeiriad anghywir neu fwy
- adrodd am beidio â derbyn negeseuon e-bost a llythyrau drwy'r post

36 Mae pob aelod staff yn gyfrifol am roi gwybod am achos diogeledd cyn gynted ag y byddant yn gwybod am unrhyw achos posibl o golli data. Mae'n hanfodol ymateb yn gyflym i gynyddu'r gobaith o adfer y data a lleihau effaith ei golli. Gallai fod canlyniadau difrifol yn sgil peidio â rhoi gwybod am achos neu oedi diangen wrth wneud hynny. Dan y Rheoliadau Cyffredinol ar Ddiogelu Data, rhaid rhoi gwybod i Swyddfa'r Comisiynydd Gwybodaeth am achosion penodol o dorri data personol cyn pen 72 awr.

37 Rhaid i staff roi gwybod i'r Swyddog Diogeledd TG (SDTG) a'u rheolwr llinell am unrhyw achos cyn gynted ag y bo modd.

38 Gallai peidio â rhoi gwybod am achos hysbys, neu wrthod gwneud hynny, arwain at gamau disgyblu. Gallai peidio â rhoi gwybod am achos hysbys, neu wrthod gwneud

hynny gan unrhyw un nad yw'n aelod o staff sy'n ymgymryd â gwaith i Estyn, arwain at derfynu contract neu gytundeb yr unigolyn hwnnw.

39 Gellir diffinio **achos trwch blewyn** fel unrhyw sefyllfa sy'n rhoi gwybodaeth mewn perygl, neu a all roi gwybodaeth mewn perygl o fynediad anawdurdodedig neu gael ei cholli. Gallai hyn gynnwys achlysuron lle mae ein harfer neu weithredoedd yn gwyro oddi wrth ein polisïau neu weithdrefnau diogeledd.

40 Mae gan unigolion gyfrifoldeb i roi gwybod i'r SDTG a'u rheolwr llinell am achosion diogeledd **posibl** hefyd, neu drwy'r ddefnyddio'r Polisi a gweithdrefnau chwythu'r chwiban os ydynt am fod yn ddienw.

41 Mae'r SDTG, ynghyd â'n Swyddog Diogelu Data, yn gyfrifol am reoli achosion. Byddant yn cynnwys unigolion eraill, fel PAG, yn y broses hon fel y bo'n briodol. Bydd y SDTG yn cofnodi manylion am yr achos mewn cofnod a bydd yn helpu i ddrafftio cynllun gweithredu i reoli'r achos, hysbysu'r rhai yr effeithiwyd arnynt ac atal achos tebyg rhag digwydd yn y dyfodol.

42 Mae'r SDTG hefyd yn gyfrifol am gynnal cofnodion a hysbysu sefydliadau perthnasol y Llywodraeth am unrhyw achosion sy'n cael eu hystyried yn 'Hysbysadwy' gan asiantaethau perthnasol, neu sy'n ofynnol gan ddeddfwriaeth. Bydd y SDTG yn rhoi gwybod i'r Grŵp Rheoli Gwybodaeth am unrhyw achosion er mwyn helpu i reoli risg yn y dyfodol a nodi unrhyw ofynion o ran rhagor o hyfforddiant neu ddogfennaeth i staff.

Adran 4: Rheoli prosiectau a sicrhau gwybodaeth

43 Mae'r adran hon yn rhoi arweiniad i reolwyr prosiectau neu raglenni. Mae prosiectau, er enghraifft adroddiadau thematig, yn gallu cynnwys newidiadau i'r ffordd rydym yn casglu neu'n defnyddio gwybodaeth, a dylid cynnwys sicrhau gwybodaeth yn y prosiect o'r cychwyn cyntaf.

Asesiad o'r effaith ar ddiogelu data

44 Ar ddechrau prosiect, dylai rheolwr y prosiect benderfynu a oes angen Asesiad o'r Effaith ar Ddiogelu Data.

45 Math o dechneg rheoli risg yw Asesiadau o'r Effaith ar Ddiogelu Data, a dylid eu dechrau'n gynnar ym mhroses rheoli'r prosiect i nodi risgiau a sicrhau bod y prosiect wedi'i gynllunio'n briodol. Mae rhagor o arweiniad a thempledi ar gael gan Swyddfa'r Comisiynydd Gwybodaeth (ICO) a'r Grŵp Rheoli Gwybodaeth.

46 Pan fydd prosiect neu raglen yn cynnwys elfen gaffael, dylai contractau gynnwys cymalau i sicrhau bod contractwyr yn deall safonau'r Llywodraeth ar gyfer mynediad diogel at wybodaeth, a rheoli gwybodaeth, a'u bod yn cadw atynt. Cysylltwch â'r Swyddog Cydymffurfio Caffael am fwy o gyngor.

47 Mae'r bwrdd prosiect ar gyfer pob prosiect yn gyfrifol am sicrhau cydymffurfiad â'r dull o sicrhau gwybodaeth sydd wedi'i amlinellu yn yr adran hon. Dylai'r bwrdd

prosiect wneud yn siŵr fod unrhyw ddata neu wybodaeth sy'n cael eu trosglwyddo y tu allan i'n sefydliad yn cael eu hawdurdodi gan y PAG.

Adran 5: Cyfathrebu mewnol ac allanol

48 Rhaid i chi fod yn ofalus wrth gyfnewid gwybodaeth â sefydliadau eraill, yn enwedig gwybodaeth sensitif. Mae hyn yn cynnwys cyfnewid gwybodaeth a sefydliadau'r llywodraeth a sefydliadau yn y sector preifat. Dim ond gyda phartneriaid cydnabyddedig fel rhan gytûn o brosesau busnes y dylech gyfnewid gwybodaeth.

49 Rhaid i'r PAG gofnodi ac asesu risg yr holl brosesau busnes a all gynnwys cyfnewid gwybodaeth sensitif yn rheolaidd neu'n achlysurol. Mae hyn i wneud yn siŵr fod pawb dan sylw yn deall y gofynion diogeledd a bod y trosglwyddo'n cael ei reoli mewn modd archwiliadwy. Dylai rhannu data personol yn rheolaidd â sefydliad allanol gael ei gofnodi ar y Gofrestr Asedau Gwybodaeth.

50 Pan fyddwch yn trosglwyddo gwybodaeth neu ddogfennau, dylech ddileu unrhyw feysydd data nad oes eu hangen i gyflawni'r swyddogaeth fusnes. Gallai hyn gynnwys dileu colofnau rydym yn eu defnyddio'n fewnol ond nad oes eu hangen ar y parti arall i gyflawni ei waith.

51 Rhaid i negeseuon e-bost gael eu marcio'n unol â sensitifrwydd y wybodaeth maent yn ei chynnwys, gan gynnwys unrhyw atodiadau. Os yw'r wybodaeth wedi'i marcio'n amddiffynnol, rhaid labelu'r neges e-bost â'r marc amddiffynnol priodol a'r cyfarwyddyd trin **ar ddechrau'r** llinell pwnc. Dylid gwirio manylion adnabod derbynyddion ar-lein, fel cyfeiriadau e-bost, yn ofalus cyn anfon negeseuon bob tro.

52 Rhaid rhoi diogelwch ychwanegol i ddata personol a allai fod yn destun adroddiad i Swyddfa'r Comisiynydd Gwybodaeth, fel achosi o dorri data personol pe byddai'n cael ei golli neu ei rannu'n amhriodol (sy'n cael ei ddiffinio'n fras fel achos diogeledd sydd wedi effeithio ar gyfrinachedd, uniondeb neu argaeledd data personol) e.e. ei amgryptio neu ei ddiogelu â chyfrinair, cyn y gellir ei anfon drwy'r e-bost at rywun y tu allan i'r sefydliad. Cysylltwch â'r SDTG a'r Grŵp Rheoli Gwybodaeth am gyngor ar sut i wneud hynny.

53 Os byddwch yn nodi gofyniad newydd ar gyfer cyfnewid data electronig â thrydydd parti, dylech drafod hyn â'r Grŵp Rheoli Gwybodaeth i nodi'r dull trosglwyddo mwyaf priodol.

54 Peidiwch ag anfon dogfennau sydd wedi'u marcio'n amddiffynnol i gyfrif e-bost personol (e.e. Hotmail, Google neu Yahoo). Mae rhagor o reolau ac arweiniad ar ddefnyddio'r e-bost wedi'u cynnwys yn y Polisi ar Ddefnyddio TGCh.

55 Os byddwch yn anfon data at unrhyw sefydliad arall neu'n derbyn data ganddo, rhaid i chi gytuno ar y lefel sensitifrwydd a'r gweithdrefnau trin priodol gyda ffynhonnell y data. Pan fydd data'n cael ei rannu'n rheolaidd, dylid cytuno ar y trefniadau trin yn fwy ffurfiol, er enghraifft fel rhan o Gytundeb Mynediad Data, Memorandwm Cyd-ddealltwriaeth neu Gytundeb Lefel Gwasanaeth.

56 Mae gan Swyddfa'r Cabinet reolau llym ynghylch anfon gwybodaeth sensitif dramor. Cysylltwch â'r SDTG i gael cyngor os oes gennych unrhyw wybodaeth sensitif y mae angen ei hanfon dramor.

57 Os ydych yn ansicr ynghylch unrhyw beth yn y polisi hwn, cysylltwch ag aelod o'r Grŵp Rheoli Gwybodaeth am gyngor.