PRIFYSGOL
BANGOR
UNIVERSITY

POLISI DIOGELWCH GWYBODAETH

Dyddiad	Pwrpas Cyhoeddi/Disgrifiad o'r Newid	Cwblhau AEC
Mehefin 2011	Cyhoeddiad Cyntaf	
29ain Mawrth 2012	Ail gyhoeddiad	
15fed Ebrill 2013	Trydydd cyhoeddiad	
8fed Mehefin 2015	Pedwerydd Cyhoeddiad	28ain Gorffennaf, 2015
28ain Ionawr 2019	Pumed Cyhoeddiad	

Swyddog Polisi	Uwch Swyddog Cyfrifol	Cymeradwywyd gan	Dyddiad
Pennaeth Llywodraethu a Chydymffurfio	Ysgrifennydd y Brifysgol	Grŵp Tasg Cydymffurfio	28ain Ionawr, 2019

Polisi Diogelwch Gwybodaeth

1. Rhagarweiniad

1.1 Polisi Prifysgol Bangor yw y bydd

[a] Yr wybodaeth a reolir ganddi (ar ffurf papur ac yn electronig) yn cael ei diogelu'n briodol er mwyn:

(i) sicrhau y cydymffurfir â deddfwriaeth ac arweiniad perthnasol; a,
(ii) sicrhau bod y wybodaeth ar gael dim ond i'r rhai sydd ag angen dilys i fynd at y wybodaeth, a diogelu rhag mynediad heb awdurdod; a,
(iii) sicrhau bod cyfrinachedd yn cael ei gynnal, yn enwedig lle delir data trydydd parti neu ddata personol; a
(iv) sicrhau parhad busnes a gwarchod asedau;
(v) atal methiannau o ran cywirdeb, neu ymyriadau ag argaeledd yr wybodaeth honno.

[b] Hyfforddir staff am bolisïau ac arferion diogelwch gwybodaeth

[c] Mae cyngor arbenigol ar ddiogelwch gwybodaeth ar gael drwy'r brifysgol.

[d] Mae systemau, technoleg a chymwysiadau'r brifysgol a ddefnyddir i gadw neu brosesu data personol, sensitif neu gyfrinachol yn ddiogel, yn ddilys a chedwir copïau wrth gefn.

[e] Caiff unrhyw achosion o dorri rheolau diogelwch gwybodaeth, neu bu ond y dim iddynt gael eu torri, eu cofnodi i sicrhau bod camau priodol a mesurau ataliol yn cael eu gweithredu.

1.2 Mae'r Polisi Diogelwch Gwybodaeth hwn yn darparu cyfeiriad rheoli a chefnogaeth ar gyfer diogelwch gwybodaeth ar draws y Brifysgol. Bydd polisïau atodol penodol a chyfarwyddyd yn cael eu hystyried fel rhan o'r Polisi hwn. Drwy'r polisïau, y gweithdrefnau a'r strwythurau hyn, bydd y Brifysgol yn hwyluso llif gwybodaeth yn ddiogel a di-dor o fewn y Brifysgol ac ym mhob gohebiaeth allanol.

1.3 Cymeradwywyd y Polisi hwn gan y Grŵp Tasg Cydymffurfio a'i gadarnhau gan y Pwyllgor Gweithredu ac y mae'n rhan o bolisïau a gweithdrefnau Prifysgol Bangor. Y mae'n berthnasol i'r holl staff, myfyrwyr a thrydydd partïon eraill perthnasol a bydd yn cael ei gyfleu iddynt.

1.4 Bob tro y torrir y Polisi hwn, boed yn ddamweiniol neu'n fwriadol, yn wirioneddol neu a amheuir, byddant yn cael eu hadrodd a'u hymchwilio'n unol ag Adran 8 y Polisi hwn.

2. Diffiniad

2.1 I ddibenion y Polisi hwn diffinnir diogelwch gwybodaeth fel yr ymarfer o sicrhau nad yw gwybodaeth yn cael ei darllen, ei chlywed, ei diwygio, ei throsglwyddo, ei darlledu na'i defnyddio mewn unrhyw fodd arall ond gan bobl sydd â hawl ac angen i wneud hynny.

2.2 Mae gwybodaeth yn bodoli o fewn y Brifysgol ar sawl ffurf. Er enghraifft, gallai gwybodaeth fod:

- wedi'i hargraffu neu ei hysgrifennu ar bapur,
- wedi'i storio'n electronig,
- wedi'i throsglwyddo drwy'r post neu gan ddefnyddio dulliau electronig,
- wedi'i darlledu,
- ar lafar

3. Cyfrifoldeb dros Ddiogelwch Gwybodaeth

3.1 Bydd unrhyw achos o dorri'r polisi hwn neu unrhyw bolisi atodol neu gyfarwyddyd yn cael ei drin o ddifri gan y Brifysgol ac fe allai arwain at gamau disgyblu a/neu achos cyfreithiol.

3.2 Mae diogelwch gwybodaeth yn gyfrifoldeb personol, proffesiynol a chyfreithiol i'r holl staff (gan gynnwys contractwyr, staff dros gyfnod byr, staff gwirfoddol ac unrhyw un â chyfrif TG y Brifysgol) a myfyrwyr. Disgwylir i bob person sy'n ymdrin â gwybodaeth neu'n defnyddio systemau gwybodaeth y Brifysgol fod ag ymwybyddiaeth briodol o'r polisïau a'r gweithdrefnau a nodir yn y Polisi hwn a glynu wrthynt, yn ystod a, lle bo'n briodol ar ôl eu cyfnod yn y Brifysgol a gweithredu mewn ffordd gyfrifol a phroffesiynol.

3.3 Bydd Deoniaid Colegau, Penaethiaid Ysgol a Chyfarwyddwyr Gwasanaeth Proffesiynol yn gyfrifol am fonitro a chynnal ymwybyddiaeth o'r Polisi o fewn eu Coleg / Ysgol / Adran.

3.4 Gellid ategu'r polisi hwn gan ddehongliad manylach ar gyfer safleoedd, systemau a gwasanaethau penodol.

3.5 Rheolir gweithrediad y polisi drwy'r Pennaeth Llywodraethu a Chydymffurfio mewn ymgynghoriad â'r Uwch Swyddogion hynny sydd â chyfrifoldebau penodol dros ddiogelwch gwybodaeth yn y Brifysgol.

3.6 Gellir cael mwy o arweiniad ar ddiogelwch gwybodaeth yn Atodiad 1.

4. Defnyddio'r Polisi hwn

4.1 Bydd y Polisi hwn yn berthnasol i bob lleoliad lle y storir neu lle y gellir cael mynediad at systemau, data neu wybodaeth y Brifysgol, boed ar gyfer ymchwil, adnoddau dynol, derbyn myfyrwyr neu weithgareddau eraill. Bydd hyn yn ymestyn i ddefnydd yn y cartref a phob safle arall nad ydynt yn y Brifysgol lle bo'n briodol.

5. Cydymffurfio

Mae'n ofynnol i'r Brifysgol gynnal diogelwch yn unol â deddfwriaeth, gan gynnwys, ond heb fod yn gyfyngedig i'r canlynol:-

[a] Diogelu Data

Mae Prifysgol Bangor yn dal ac yn prosesu gwybodaeth bersonol am staff, myfyrwyr a thrydydd partïon i ddibenion academaidd, gweinyddol a masnachol. Nodir y cyfrifoldebau dan Ddeddf

Diogelu Data 2018, a'r Rheoliadau Diogelu Data Cyffredinol (GDPR) ym Mholisi Diogelu Data y Brifysgol.

[b] Deddf Gwrthderfysgaeth a Diogelwch

Mae gan y Brifysgol ddyletswydd statudol i atal pobl rhag cael eu tynnu i mewn i derfysgaeth (o dan y Ddeddf Gwrthderfysgaeth a Diogelwch 2015). Ni ddylai staff a myfyrwyr gyflawni unrhyw weithredoedd a allai ysgogi neu hyrwyddo eithafiaeth yn cynnwys, ond heb fod yn fod yn gyfyngedig i, gael mynediad i wefannau neu rannu deunydd a ellir ei gysylltu â sefydliadau eithafol neu derfysgol.

[c] Hawlfraint

Polisi'r Brifysgol yw cydymffurfio â phob rhwymedigaeth gyfreithiol a sicrhau nad oes unrhyw ddeunydd dan hawlfraint un ai'n cael ei gopïo heb ganiatâd y perchennog neu'n cael ei gopïo mewn ffordd sydd y tu allan i gylch gorchwyl cynlluniau thrwyddedu cyfunol y Brifysgol.

[d] Rheoli Cofnodion

Nodir canllawiau ar gadw, storio, trin a gwaredu cofnodion a gwybodaeth y Brifysgol ym Mholisi Rheoli Cofnodion y Brifysgol.

Nodir cyfnodau cadw data ar gyfer e-byst (a phob cofnod arall) yn Atodlen Gadw'r Brifysgol. Caiff cofnodion Office365 (gan gynnwys e-byst) eu dileu'n barhaol un mis ar ôl cael eu dileu o gyfrif defnyddiwr.

Mae cyfrifoldeb ar bob aelod o staff i sicrhau bod gwybodaeth bersonol a ddefnyddir yn ystod eu gwaith yn cael ei gwaredu'n ddiogel. Gellir dod o hyd i fwy o ganllawiau yng *Nghanllawiau Cadw a Gwaredu Gwybodaeth Bersonol* y Brifysgol.

[e] Adnoddau TG

[i] Darperir Adnoddau TG y Brifysgol ar yr amod y defnyddir hwy i ddibenion derbyniol awdurdodedig yn unig. Nodir datganiad o gyfrifoldebau defnyddwyr mewn perthynas ag adnoddau TG yn *Rheoliadau Defnyddio Gwybodaeth a Gwasanaetha*u y Brifysgol. Nodir cyfrifoldebau defnyddwyr yng nghyswllt gwaredu ac ail-ddefnyddio offer TG ym *Mholisi Ail-ddefnyddio a Gwaredu Cyfrifiaduron, offer TG arall a Chyfryngau Storio Data'r* Brifysgol.

[ii] Mae'r ddogfen *Polisi ar Ddefnydd Personol o Wefannau Rhwydweithio Cymdeithasol a Thrydydd Partïon eraill* hefyd yn rhoi canllawiau i staff ar ddefnydd priodol o systemau.

[iii] Mae'n rhaid i bob dyfais symudol[1] a brynwyd gan y brifysgol neu ddyfeisiau personol a ddefnyddir gan aelodau staff y brifysgol i gael mynediad pell at ddata'r brifysgol gael eu hamgryptio, a rhaid i gliniaduron gael eu diogelu gan rif adnabod defnyddiwr a rhaid i

[1] Megis gliniaduron, ffonau clyfar, tabledi a recordyddion clywedol

ffonau clyfar a thabledi gael eu diogelu gan rif PIN[2]. Ni ddylid defnyddio dyfeisiau heb eu hamgryptio i gadw data'r brifysgol.

[iv] Mae modd i gamerâu fideo / recordyddion clywedol gadw data yn ogystal, ac mae angen i wybodaeth gael ei ddiogelu yn ffisegol a drwy ei amgryptio (lle mae hyn yn bosib). Ni ddylid gadael data fideo neu ddata clywedol personol ar ddyfais heb ei amgryptio. Gweler Atodiad 1 am fwy o wybodaeth.

[iv] Nid yw'n bosibl, o fewn Office365, i aelodau staff anfon eu cyfrif e-bost cyfan ymlaen oddi ar y safle i westeiwr e-bost trydydd parti. Os bydd aelodau staff yn dewis anfon ymlaen un neges e-bost dylid gwneud hyn gan roi ystyriaeth briodol i ofynion y polisi hwn a'r *Rheoliadau Defnydd Derbyniol*.

[f] Adroddiad Caldicott 1997

Mae Adroddiad Caldicott yn nodi argymhellion ar gyfer cynnal diogelwch manylion cleifion ac y mae o bwysigrwydd penodol i rai o Ysgolion y Brifysgol a dylent sicrhau eu bod yn llwyr ymwybodol o ofynion yr adroddiad.

[g] Systemau Busnes y Brifysgol

Diffinnir Perchennog Data ar gyfer pob system fusnes y Brifysgol (e.e. cofnodion myfyrwyr, adnoddau dynol a / neu systemau ariannol). Dylai'r Perchennog y Data sicrhau y cynhelir archwiliad blynyddol o holl ddefnyddwyr cofrestredig y system i sicrhau bod defnyddwyr yn parhau i fod â'r lefel briodol o fynediad.

Dylai Deoniaid Colegau / Penaethiaid Ysgol / Cyfarwyddwyr Gwasanaeth Proffesiynol sicrhau bod gan unrhyw gronfeydd data eraill o fewn eu cylch cyfrifoldeb berchennog data dynodedig, rheolaeth berthnasol ar fynediad a hefyd y cynhelir archwiliad blynyddol o holl ddefnyddwyr cofrestredig y gronfa ddata.

[h] Gwybodaeth heb fod yn gysylltiedig â'r Brifysgol

Mae unigolion yn bersonol gyfrifol am unrhyw wybodaeth a ddelir ganddynt nad yw'n ymwneud â'r gwaith, un ai ar fformat papur neu electronig, ar systemau ac yn adeiladau'r Brifysgol. Nid yw'r Brifysgol yn cymryd unrhyw gyfrifoldeb am yr wybodaeth hon.

6. Hyfforddiant Diogelwch Gwybodaeth ac Asesiadau Risg

6.1 Mae'r Brifysgol yn cydnabod yr angen i'r holl staff, myfyrwyr a defnyddwyr eraill gwybodaeth y Brifysgol gael hyfforddiant diogelwch gwybodaeth. Hwylusir yr hyfforddiant hwn gan y Swyddfa Llywodraethu a Chydymffurfio, a Gwasanaethau TG mewn ymgynghoriad â Gwasanaethau Canolog eraill perthnasol y Brifysgol.

[2] Mae'n bosib amgryptio gliniaduron sydd wedi eu cymeradwyo gan y Brifysgol (PC & MAC) a ffonau clyfar / dyfeisiadau tabled a gymeradwywyd

6.2 Bydd Deoniaid Colegau / Penaethiaid Ysgol / Cyfarwyddwyr Gwasanaethau Proffesiynol (drwy swyddog priodol) yn atebol am sicrhau y cynhelir asesiadau risg rheolaidd er mwyn deall pa wybodaeth a ddelir ganddynt a pha drefniadau diogelwch sy'n angenrheidiol er mwyn diogelu gwybodaeth o'r fath rhag unrhyw dorri ar fesurau diogelwch ac a roddir trefniadau o'r fath ar waith mewn gwirionedd.

6.3 Rhaid i Ddeoniaid Colegau / Penaethiaid Ysgol / Cyfarwyddwyr Gwasanaeth Proffesiynol ddarparu adroddiad blynyddol i'r Grŵp Tasg Cydymffurfio ar gyfer cyfarfod cyntaf y flwyddyn academaidd yn cadarnhau y cydymffurfir â gofynion y Polisi hwn, yn eu maes cyfrifoldeb hwy.

6.4 Bydd y Grŵp Tasg Cydymffurfio yn gyfrifol am fonitro cydymffurfiad â pharagraffau 6.2 a 6.3 uchod, gan gynnwys ymgymryd ag archwiliadau rheolaidd a gwneud argymhellion fel y bo'n briodol.

7. Parhad Busnes

Mae'r Brifysgol yn rheoli ei chynlluniau parhad busnes drwy ofynion y Polisi Rheoli Argyfwng sy'n cynnwys gofyniad i Ddeoniaid Coleg / Penaethiaid Ysgol a Chyfarwyddwyr Gwasanaethau Proffesiynol i sefydlu cynllun parhad busnes. Gellir cael rhestr o gynlluniau corfforaethol wrth gefn y Brifysgol gan y Pennaeth Llywodraethu a Chydymffurfio, Swyddfa Llywodraethu a Chydymffurfio.

8. Rhoi gwybod am ddigwyddiadau a Chwynion

8.1 Dylid rhoi gwybod am bob achos o dorri'r Polisi Diogelwch Gwybodaeth hwn i'r Pennaeth Llywodraethu a Chydymffurfio yn y Swyddfa Llywodraethu a Chydymffurfio gan ddefnyddio'r ffurflen yn Atodiad 2 ac eithrio staff neu fyfyrwyr sy'n datgelu cyfrinair eu cyfrif TG yn anfwriadol. Yn yr achos hwnnw rhaid i'r unigolyn newid ei gyfrinair **a** hysbysu Desg Gymorth Gwasanaethau TG ar 01248 38811 **ar unwaith**, i sicrhau y gellir cymryd camau adferol i gyfyngu ar effaith eang datgeliad o'r fath.

8.2 Mae'n bwysig rhoi gwybod am unrhyw achos o dorri'r polisi cyn gynted â phosibl er mwyn lleihau'r niwed posibl i'r Brifysgol (gan gynnwys ei henw da), lleihau'r trallod i unigolion a lleihau'r risg o ddirwyon trwm a allai o bosibl fod yn sylweddol am dorri y Rheoliadau Diogelu Data Cyffredinol (GDPR) a'r Ddeddf Diogelu Data 2018.

8.3 Ni ddylai neb ar unrhyw gyfrif geisio celu tor-polisi o'r fath. Gall celu tor-polisi arwain at gamau disgyblu a gallai Swyddfa'r Comisiynydd Gwybodaeth hefyd gymryd camau yn erbyn unigolion.

8.4 Mae gan y Brifysgol hefyd *Bolisi Datgelu er Lles y Cyhoedd (Chwythu'r Chwiban)*. Mae hyn yn caniatáu i unigolion sydd â phryder ynghylch gweithredoedd person arall megis materion diogelwch neu gamddefnyddio gwybodaeth godi pryderon o'r fath mewn modd strwythuredig ac adeiladol.

ATODIAD 1

Canllawiau Diogelwch Gwybodaeth

1. Cadw Gwybodaeth Bersonol yn Ddiogel

Rhaid i bob data personol gael ei gadw mewn amgylchedd diogel gyda mynediad yn cael ei reoli - bydd y lefel o ddiogelwch a gymhwysir i'r wybodaeth yn dibynnu ar natur yr wybodaeth, a dylid gwneud hynny yn dilyn asesiad risg a ddylai sefydlu risg posibl mynediad heb awdurdod a / neu ladrata.

[a] Cofnodion papur

Byddai dulliau storio priodol ar gyfer cofnodion papur / llaw yn cynnwys:

- Cabinet metel dan glo, gyda'r allweddi wedi'u cyfyngu i staff awdurdodedig yn unig;
- Drôr wedi'i chloi mewn desg (neu fan storio arall) gyda'r allweddi wedi'u cyfyngu i staff awdurdodedig yn unig;
- Ystafell wedi'i chloi y gellir cael mynediad ati drwy gyfrwng allwedd neu glo gyda chod, gyda mynediad at yr allwedd / cod wedi'i gyfyngu i staff awdurdodedig yn unig;

[b] Cofnodion electronig a Systemau Cronfa Ddata

Byddai canllawiau ymarfer da ar gyfer cofnodion electronig yn cynnwys:

- **Peidiwch byth â datgelu eich cyfrinair/cyfrineiriau** - ni ofynnir i chi byth ddatgelu eich cyfrinair, a pheidiwch byth ag ateb e-bost sy'n gofyn i chi ddatgelu eich cyfrinair - os oes unrhyw amheuaeth, holwch y Gwasanaethau TG;
- Sicrhewch fod eich cyfrinair yn un cadarn - ddim yn air nac yn enw iawn, cyfuniad o lythrennau, rhif, llythrennau bach a mawr - newidiwch ef yn rheolaidd a chyfeiriwch at wefan TG am arweiniad.
- Logiwch i ffwrdd bob tro, neu gloi gweithfan cyn ei gadael;
- Pan fyddwch yn gwneud gwaith cyfrinachol sicrhewch nad oes modd i neb arall ddarllen y sgrin;
- Diogelwch offer rhag cael eu dwyn, mae hyn yn hanfodol bwysig ar gyfer offer cludadwy megis gliniaduron a ffonau symudol;
- Storiwch pob cofnod ar rwydwaith y Brifysgol (gyriant M neu U) - mae hyn yn sicrhau bod data'n cael ei gopïo gan y Gwasanaethau TG, ac mae'n lliniaru'r risg o golli / datgelu gwybodaeth drwy rannu cyfrifiadur neu ladrad cyfrifiadur. Lle nad yw hyn yn bosibl, sicrhewch fod pob data pwysig yn cael ei gopïo'n rheolaidd ac y cedwir y copïau mewn lleoliad diogel ar wahân. Cysylltwch â'r Gwasanaethau TG os oes angen cymorth arnoch.
- Sicrhewch fod lefel eich mynediad at systemau cronfa ddata sy'n cynnwys gwybodaeth bersonol (e.e. system myfyrwyr, system cyllid, system AD) yn berthnasol i rôl a chyfrifoldebau eich swydd. Os bydd eich swydd / cyfrifoldebau'n newid, rhowch wybod i berchnogion data pob system i sicrhau bod eich mynediad yn briodol.
- Mae angen bod yn hynod ofalus wrth anfon negeseuon e-byst ymlaen, yn arbennig rhai gydag atodiadau, fel nad yw'r wybodaeth yn cael ei hanfon ond i'r bobl sydd â gwir 'angen

gwybod'. Cyn anfon atodiadau ymlaen o gwbl, dylech wirio nad yw'r wybodaeth ar gael iddynt drwy ryw ffordd ddiogel arall.

[c] Defnyddio Adnoddau TG yn ddiogel i ffwrdd o'r Brifysgol

[i] Wrth ddefnyddio eich PC neu MAC ac yn gweithio i ffwrdd o'r Brifysgol, dylech fod yn ymwybodol y gellid storio gwybodaeth ar y ddyfais honno mewn dwy ffordd allweddol:

- eich bod yn penderfynu storio ffeil ar y ddyfais; neu**:**
- drwy broses megis darllen atodiad e-bost, caiff gwybodaeth ei gadael ar y ddyfais yn anfwriadol heb i chi wybod.

[ii] Y **dull diogel** o weithio i ffwrdd o'r Brifysgol gan roi sylw priodol i Ddiogelwch gwybodaeth (e.e. ar un o liniaduron y Brifysgol neu liniadur/cyfrifiaduron heb fod yn eiddo i'r Brifysgol) yw drwy ddefnyddio gwasanaeth Office365 a / neu *Desktop Anywhere* y Brifysgol. Mae'r dull hwn yn sicrhau bod pob gwybodaeth yn aros ar rwydwaith mewnol TG dan reolaeth y Brifysgol, ac na chaiff ei storio ar y ddyfais a ddefnyddiwyd. Wedi logio i mewn, defnyddiwch eicon dewislen "Bangor University Staff Desktop" er mwyn gweithio fel pe baech yn defnyddio cyfrifiadur yn y Brifysgol.

Gallwch hefyd fynd i'ch cyfrif e-bost Prifysgol Bangor yn ddiogel trwy ryngwyneb gwe Office 365 a chyfrif One Drive gan nad yw'r wybodaeth yn cael ei storio ar y ddyfais a ddefnyddir.

[iii] Ni ddylid defnyddio cofau bach USB o dan unrhyw amgylchiadau i ddal data Prifysgol (mae hyn yn cynnwys e-byst, dogfennau, data ymchwil ayyb.). Mae'n rhaid cael cytundeb ymlaen llaw i unrhyw eithriad i'r rheol hon gan y Pennaeth Llywodraethu a Chydymffurfio, fydd yn sicrhau nad oes unrhyw ddull diogelu arall ar gael, a bod asesiad risg addas wedi ei gwblhau.

[d] Cyfrifiadura Cwmwl

Mae defnyddio cyfrifiadura cwmwl yn cynyddu ac mae ei ddefnyddio o fudd i aelodau staff sy'n cydweithio neu'n gweithio oddi ar y safle.

Mae system calendr ac e-bost y Brifysgol eisoes ar y cwmwl (Microsoft Office365) ac yn cydymffurfio â deddfwriaeth diogelu data y Deyrnas Unedig. Efallai nad yw systemau calendr ac e-bost eraill yn cydymffurfio â'r ddeddfwriaeth a dylai aelodau staff sicrhau bod gofynion y Ddeddf Diogelu Data 2018 a'r Rheoliadau Diogelu Data Cyffredinol (GDPR) yn cael eu dilyn ar gyfer unrhyw ddata personol sy'n cael ei ddal mewn amgylchedd cyfrifiadura cwmwl.

[e] Dyfeisiau Symudol

Bydd unrhyw ffôn clyfar/tabled y brifysgol neu bersonol sydd wedi'u ffurfweddu i ddefnyddio Office365 y brifysgol wedi'i alluogi â rhif PIN yn awtomatig, wedi'i alluogi ag amgryptiad, a glanhau o bell fel y gellir dileu data'r brifysgol o'r ddyfais os caiff ei cholli etc.

Mae gan aelodau staff unigol gyfrifoldeb am reoli a diogelu eu dyfeisiau symudol (er enghraifft iPhone/ffôn clyfar) a'r data maent yn eu cynnwys.

Y mae camau syml y dylech eu cymryd i ddiogelu eich dyfais symudol a'r data sydd arni.

- Dylech sicrhau bod eich dyfais wedi'i amgryptio (yn cynnwys unrhyw gardiau cof a all fod yn y ddyfais). Gofynnwch am gyngor y Gwasanaethau TG os oes angen.
- Sefydlu cyfrinair diogel neu rif PIN ar eich dyfais symudol. Pan na ddefnyddir y ddyfais am gyfnod o amser, bydd yn cloi a bydd angen y cod diogelwch i'w defnyddio eto, sy'n ychwanegu gwarchodaeth pe digwydd i'r ddyfais gael ei cholli neu ei dwyn.
- Gwneud copïau wrth gefn o unrhyw ddata sydd ar eich dyfeisiau, megis dogfennau, delweddau ayb. Os byddwch yn cysoni eich e-bost, calendr a'ch cysylltiadau â'ch cyfrif Prifysgol, nid oes angen i chi wneud copïau wrth gefn o'r data hwn gan y caiff ei storio'n ganolog yn y Brifysgol a dim ond golwg ar y data hwn a geir ar eich dyfais. Fodd bynnag, os oes gennych ddogfennau, delweddau neu ddata ychwanegol ar wahân i'ch cyfrif Prifysgol, dylech gopïo'r ffeiliau hyn yn rheolaidd i'ch PC, yn ddelfrydol, ffolder ar eich gyriant One Drive, i sicrhau bod gennych gopïau wrth gefn pe digwydd i'ch dyfais fethu neu fynd ar goll.

[f] Dyfeisiau recordio sain a recordio.

Defnyddir dyfeisiau sain a fideo yn rheolaidd gan aelodau o staff a / neu fyfyrwyr i recordio cyfweliadau ayyb. Dylech fod yn ymwybodol fod recordiau o'r fath, wrth gynnwys gwybodaeth bersonol ganfyddadwy, yn wybodaeth bersonol o dan ofynion y Ddeddf Diogelu Data 2018 a'r Rheoliadau Diogelu Data Cyffredinol (GDPR) ac felly fod rhaid eu diogelu'n briodol.

- Dylid ystyried dulliau electronig gwahanol i gamera neu recordydd clywedol penodedig. Mae gan bob dyfais tabled a ffonau clyfar gamerâu a'r gallu i recordio sain. Mae ansawdd y recordio ar y dyfeisiau hyn yn dda iawn erbyn hyn gyda'r rhan fwyaf o'r dyfeisiau newydd yn fideo HD. Mae dyfeisiau modern Android ac Apple wedi'u hampryptio hefyd a gallant gynnig ffordd syml i ateb gofynion. Rhaid cofio bod tabledi a ffonau sydd wedi'u hamgryptio yn hawdd i'w colli neu gael eu dwyn felly dylid gwneud copi wrth gefn o unrhyw ddata ar leoliad diogel cyn gynted ag y bo modd a'i ddileu o'r ffôn neu dabled i'w ddiogelu rhag cael ei golli.

- Byddwch yn ymwybodol fod dyfeisiadau cludadwy fideo a clywedol, a ddefnyddir ar gyfer recordiadau o'r fath yn dargedau dymunol i ladron. Pan nad ydynt yn cael eu defnyddio mae'n rhaid eu cadw dan glo mewn lleoliadau diogel allan o'r golwg. Ni ddylid byth eu gadael yn y golwg mewn cerbydau nac mewn mannau cyhoeddus heb neb yn cadw golwg arnynt.

- Mae'r Brifysgol yn argymell fod pob dyfais recordio clywedol a fideo, sy'n cael eu defnyddio i storio gwybodaeth bersonol / categori arbennig yn cael eu hamgryptio. Mae modd archebu recordyddion clywedol sy'n defnyddio storfa gof lle mae modd ei amgryptio. Cysylltwch â Desg Gymorth TG am gyngor ynglŷn â'r dyfeisiadau diweddar.

- Dylech fod yn ymwybodol fod nifer o ddyfeisiadau clywedol cyffredin, a phob camera fideo symudol yn defnyddio dyfais cof cyflwr solet (megis cerdyn micro SD), nad oes modd ei amgryptio. Gwnewch yn siŵr fod y dyfeisiadau yma, pe baent yn cael eu defnyddio gennych chi, neu gan fyfyrwyr o dan eich cyfarwyddyd / arweiniad, yn cael eu hamddiffyn rhag cael eu dwyn, a rhag datgelu gwybodaeth bersonol, categori arbennig a / neu gyfrinachol, heb awdurdod neu yn ddamweiniol.

- Os nad oes gennych fynediad at ddyfais wedi'i hamgryptio ar gyfer eich recordiadau yna dylech ystyried a oes angen cofnodi'r wybodaeth. A oes dull arall, efallai gyda llai o risg, i gadw neu ddiogelu'r wybodaeth?

- Os ydych yn gorfod defnyddio dyfais heb ei hamgryptio, ar ôl cysidro pob opsiwn, yna bydd raid i chi gymryd camau ar unwaith i amgryptio'r data a ddelir. Ar ôl cwblhau'r sesiwn recordio dylid trosglwyddo'r cynnwys o'r cerdyn cof a ddefnyddiwyd i ddyfais wedi ei hamgryptio (gliniadur fel rheol). Yna dylid dileu'r ffeiliau o'r cerdyn cof. Yn yr un modd â chofion bach USB, pan gaiff ffeil ei ddileu yn y ffordd arferol nid yw wedi ei ddileu'n llwyr hyd nes y caiff ei wrthwneud ac ni fydd defnyddiwr y ddyfais byth yn gwybod pryd fydd hynny'n digwydd. Felly rhaid dileu data gyda chyfleustod dileu diogel am ddim fel Disk (http://www.diskwipe.org/). Mae'n rhaid i chi sicrhau bod eich data wedi ei drosglwyddo'n llwyddiannus i'r ddyfais ddiogel cyn gwneud hyn gan ei fod yn weithred parhaol!

2. Mynediad at Ddata Personol

a) Dylai Deoniaid Colegau / Penaethiaid Ysgolion a Chyfarwyddwyr Gwasanaethau Proffesiynol sicrhau eu bod yn ymwybodol o'r aelodau o staff o fewn eu cylch cyfrifoldebau sydd, oherwydd natur eu swydd, wedi'i nodi fel rhai sydd angen mynediad cyfreithiol at ddata personol wrth gyflawni eu swydd.

b) Rhaid hefyd ddiffinio'r dibenion dynodedig y darperir mynediad at ddata personol ar eu cyfer. Ar gyfer rhai Colegau, Ysgolion a Gwasanaethau bydd hyn yn eglur oherwydd natur eu swyddogaeth e.e. Adnoddau Dynol. Fod bynnag, mewn achosion eraill bydd angen amlinellu'r rhain yn benodol.

c) Fel y nodwyd ym Mholisi Diogelu Data'r Brifysgol, rhaid i aelodau staff sicrhau:

- Y cedwir yn ddiogel yr holl wybodaeth bersonol a ymddiriedwyd iddynt wrth gyflawni eu swydd;
- Na ddatgelir unrhyw wybodaeth bersonol un ai ar lafar neu'n ysgrifenedig, yn ddamweiniol neu fel arall i unrhyw drydydd parti heb awdurdod.
- Ni ddylai staff fynd at wybodaeth bersonol am unrhyw reswm ac eithrio busnes dilys y brifysgol.
- Bydd unrhyw drosedd yn erbyn y Ddeddf Diogelu Data 2018 yn cael ei drin yn ddifrifol gan y Brifysgol a gallai gael ei ystyried dan gamau disgyblu.

d) Lle bo ffeil yn cynnwys data personol yn cael ei thynnu o'r system ffeilio diogel am reswm cyfreithlon gan aelod o staff awdurdodedig, dylai trefn lem o lofnodi wrth ei thynnu allan ac wrth ei dychwelyd fod mewn grym.

e) Dylai staff sicrhau nad yw data personol yn cael ei lungopïo ond lle bo hynny'n wirioneddol angenrheidiol a dylent sicrhau bod y copi a'r ddogfen wreiddiol yn destun yr un protocolau o ran diogelwch.

f) Oni bai fod hynny'n wirioneddol hanfodol ac wedi'i awdurdodi gan Ddeon Coleg / Pennaeth Ysgol neu Gyfarwyddwr Gwasanaeth, ni ddylai staff fynd â data personol allan o'r Brifysgol - un ai ar ffurf papur neu'n electronig. Pan fo'n hanfodol gwneud hyn rhaid cymryd camau diogelwch priodol i warchod yn erbyn lladrad neu fynediad heb awdurdod at y data hynny (gweler Adran 1 uchod).

g) Pan fo angen mynediad diogel at wybodaeth electronig a chronfeydd data oddi ar y safle, dylid defnyddio gwasanaeth One Drive neu *Desktop Anywhere* y Brifysgol. Mae hyn yn sicrhau nad yw gwybodaeth yn cael ei throsglwyddo'n gorfforol allan o'r Brifysgol ac y cyfnewidir gwybodaeth dros gyswllt wedi'i amgryptio. I ddefnyddio'r gwasanaeth mae angen enw defnyddiwr a chyfrinair Bangor.

h) Dylid ffurfweddu mynediad at e-bost oddi ar y safle yn unol â chyngor ITS i sicrhau trosglwyddiad diogel.

3. Trosglwyddo Data Personol / Data Personol Sensitif

a) Cyn trosglwyddo na datgelu data personol y tu allan i'r Brifysgol, rhaid i staff ymgyfarwyddo â gofynion Polisi Diogelu Data'r Brifysgol. Dylid cymryd gofal penodol wrth anfon unrhyw atodiadau drwy e-bost.

b) Rhaid i staff sicrhau bod y rhagofalon diogelwch priodol yn eu lle (megis amgryptio) i leihau'r risg o golli'r data a / neu ddatgelu'r data'n ddamweiniol.

c) Rhaid i bob cyfathrebiad drwy'r post sy'n cynnwys data personol gael ei farcio *cwbl breifat a chyfrinachol* a rhaid ei gyfeirio at unigolyn a enwir.

d) Ni ddylid defnyddio dyfais gorfforol megis ffyn cof USB, CDs neu DVDs yn cynnwys data personol i anfon gwybodaeth, heb gael caniatâd gan y Pennaeth Llywodraethu a Chydymffurfio.

e) Ar gyfer post mewnol ac allanol yn cynnwys data personol rhaid ystyried y dull mwyaf priodol a diogel o anfon yr wybodaeth. Ar gyfer post allanol dylid bob amser ystyried defnyddio gwasanaeth 'Signed For' y Post Brenhinol neu gludwyr sy'n cynnig gwasanaeth tracio a llofnodi. Dylid gofyn am gyngor pellach o Ystafell Bost y Brifysgol.

f) Ni ddylid e-bostio data personol sensitif yn allanol dan unrhyw amgylchiadau oni fo wedi'i amgryptio (cysylltwch â'r Gwasanaethau TG am arweiniad pellach ar argaeledd amgryptio e-bost).

g) Rhaid anfon data personol ar bapur gan ddefnyddio gwasanaeth 'Signed For' neu wasanaeth Cludwr sy'n cynnig gwasanaeth tracio a llofnodi.

h) Lle bynnag y bo'n bosibl dylai cysylltiadau rhwydwaith diwifr ddefnyddio gwasanaethau a ddiogelwyd. Yn y Brifysgol y gwasanaeth diogel a ffafrir yw *eduroam* (a fydd hefyd yn gweithio mewn llawer o Brifysgolion eraill yn y DU a thramor). Mae gwefan y Gwasanaethau TG yn cynnwys gwybodaeth ar gysylltu â'r gwasanaeth. Mae cymorth hefyd ar gael drwy'r Ganolfan Cefnogi TG (X8111).

Gartref, dylai eich cysylltiad band eang diwifr fod wedi'i osod ar ddull cysylltu diogel a enwir WPA2. Gall eich darparwr gwasanaeth rhyngrwyd (DGRh) roi cymorth.

Mewn mannau cyhoeddus eraill, efallai na fydd gwasanaeth diogel ar gael. Yn yr achos hwn dylech fod yn ymwybodol y gallai unrhyw ddata a anfonir neu a dderbynnir drwy dudalennau gwe arferol, gael ei ryng-gipio. Ni ddylid anfon data sensitif ar rwydwaith heb ei ddiogelu ond gan ddefnyddio

tudalennau gwe a ddiogelwyd (mae cyfeiriad y rhain yn dechrau https:// - y llythyren ‘s’ yn nodi diogel).

i) Bydd llawer o ffurflenni gwe yn gofyn a ydych yn dymuno arbed cyfrinair a ddarparwyd gennych. Ym mhob achos defnyddiwch yr opsiwn - “byth ar gyfer y wefan hon”. Bydd hyn yn cynorthwyo i atal unrhyw fynediad heb awdurdod at unrhyw dudalennau gwe a ddiogelwyd.

j) Dylech osgoi defnyddio'r un cyfrinair at ddefnydd busnes a phreifat, a newid eich cyfrinair yn rheolaidd.

4. Rhagor o Wybodaeth

Gellir cael rhagor o wybodaeth neu arweiniad ar unrhyw agwedd ar y Canllawiau hyn o’r Swyddfa Llywodraethu a Chydymffurfio, neu gan y Gwasanaethau TG.

ATODIAD 2

FFURFLEN COFNODI DIGWYDDIAD DIOGELWCH GWYBODAETH

Eich Manylion

1. ENW …….
2. ADRAN …….
3. E-BOST …….
4. RHIF FFÔN …….

Manylion y Digwyddiad

1. Dyddiad y digwyddiad ……
2. Dyddiad yr adroddwyd ar y digwyddiad……
3. Darparwch grynodeb byr o'r tor-diogelwch neu golled data. (nodwch y math o wybodaeth, megis data masnachol neu bersonol, cofnodion meddygol, manylion ariannol, myfyrwyr neu staff):-

   ……
   ……
   ……
   ……
   ……
   ……

4. Rhowch wybod am unrhyw gamau dilynol neu gamau eraill a gymerwyd (os o gwbl).
   ……
   ……
   ……

5. Unrhyw wybodaeth arall y teimlwch sy'n berthnasol

……
……
……

Dychweler drwy e-bost at: Lynette Hunter, Swyddfa Llywodraethu a Chydymffurfio: info-compliance@bangor.ac.uk