Gwybodaeth
Dan
Reolaeth

Cyngor Gwynedd

TREFN WEITHREDU DIOGELWCH GWYBODAETH

3.0

Mai 2018

Gwasanaeth Rheoli Gwybodaeth

Trefn Weithredu Diogelwch Gwybodaeth

1. Cyflwyniad

Mae'r Cyngor yn ymdrin â miloedd o wahanol fathau o wybodaeth bob diwrnod. Amrywia hyn o ddogfennau cyhoeddus i wybodaeth hynod o sensitif a chyfrinachol. Fel pob ased busnes pwysig, mae'r wybodaeth hon yn werthfawr ac mae angen ei diogelu'n briodol.

O ran gwybodaeth bersonol a sensitif, mae'n hanfodol bod pawb yn ymwybodol o'r angen i gadw'r safonau uchaf o ddiogelwch gwybodaeth, er mwyn rhoi'r gorau i bobl Gwynedd trwy sicrhau ein bod yn cadw eu manylion personol yn ddiogel,a hefyd sicrhau bod y Cyngor yn cydymffurfio gyda'r ddeddfwriaeth berthnasol yn arbennig felly deddfwriaeth Diogelu Data.

2. Amcanion

Bwriad y drefn weithredu yw sicrhau bod pob defnyddiwr a rheolwr yn deall ei gyfrifoldeb i ddiogelu unrhyw wybodaeth gyfrinachol a phersonol sydd o dan ei ofal.

3. Sgôp

Mae'r drefn hon yn berthnasol i'r holl staff sydd wedi'u contractio yn uniongyrchol ac yn anuniongyrchol ac unrhyw un arall sy'n gweithio i'r Cyngor.

4. Diffiniad

Mae gwybodaeth bersonol yn golygu unrhyw wybodaeth sy'n cyfeirio at unigolyn.

Mae gwybodaeth sensitif yn cynnwys gwybodaeth am iechyd, troseddau, ethnigrwydd, crefydd, credoau gwleidyddol, gwybodaeth geneteg neu biometrig, aelodaeth undeb lafur, bywyd rhywiol neu rywioldeb.

Gall gwybodaeth gyfrinachol gynnwys gwybodaeth nad yw am bobl, e.e contractau/materion masnachol, camau cyfreithiol, neu drafodaethau am bolisiau.

5. Dogfennau papur sydd yn cynnwys gwybodaeth bersonol ac/neu gyfrinachol

Desg Glir

Os nad yw unigolyn wrth ei ddesg, ni ddylid gadael ffeiliau/papurau sy'n cynnwys gwybodaeth bersonol a chyfrinachol lle gall eraill eu gweld. Dylid cadw dogfennau mewn cwpwrdd cloëdig dros nos ac ni ddylid gadael y goriad yn y clo.

Ni ddylid gadael unrhyw wybodaeth bersonol na chyfrinachol ar ddesgiau, argraffyddion, llungopiwyr na pheiriannau ffacs ar ddiwedd y dydd.

Argraffu

Dylid cymryd gofal arbennig wrth argraffu gwybodaeth bersonol i lungopïwr neu argraffydd sy'n cael ei rannu gydag eraill er mwyn sicrhau nad yw papurau sy'n perthyn i rywun arall yn cael eu codi trwy gamgymeriad.

Dylid defnyddio'r cyfleuster 'secure print' bob amser er mwyn osgoi hyn ble mae ar gael.

Ffacsio
Dylid ond defnyddio peiriant ffacs os nad oes dewis arall ar gael i drosglwyddo'r wybodaeth.

- Rhaid rhoi 'Preifat a Chyfrinachol' ar y dudalen glawr bob amser a dylai gynnwys:
    - Enw'r person sydd i dderbyn y ffacs
    - Enw'r person sydd yn anfon y ffacs (enw'r tîm a'i leoliad), rhif ffôn a rhif ffacs
    - Eglurhad am beth i'w wneud os yw'r person anghywir yn derbyn y ffacs (e.e. cysylltu â chi ar unwaith, peidio â darllen y cynnwys na'i rannu â neb arall)

- Cyn anfon ffacs cyfrinachol, dylid ffonio'r person sydd i fod i'w dderbyn i adael iddo/ iddi wybod ffacs cyfrinachol ar ei ffordd

- Dylid gofyn i'r unigolyn pen arall ffonio i gadarnhau ei bod/ fod wedi'i dderbyn neu eu ffonio ar ôl anfon y ffacs

- Wrth ddefnyddio rhif ffacs sydd wedi'i raglennu, dylid sicrhau bod y dewis yr un iawn a dylid gwirio yn rheolaidd fod y rhifau sydd wedi'u rhaglennu'n parhau yn gywir.

- Os nad yw'r rhif wedi ei raglennu, dylid ei wirio ddwywaith er mwyn sicrhau bod y rhif cywir yn cael ei ddefnyddio

Postio
- Dylid sicrhau fod y cyfeiriad yn gywir – yn enwedig wrth bostio gwybodaeth y tu allan i'r Cyngor

- Dylid gwirio'r cyfeiriad ac os yn bosib rhoi enw'r person sydd i fod i dderbyn y wybodaeth – nid adran neu dîm yn unig.

- Ni ddylid rhoi gwybodaeth mewn amlen ar ben eu hun; dylid amgau naill ai lythyr eglurhad neu slip cyfarch gyda'r wybodaeth.

- Dylid ysgrifennu'r cyfeiriad dychwelyd/ eich cyfeiriad ar gefn yr amlen – bydd hyn yn caniatáu i amlen a anfonwyd yn anghywir gael ei dychwelyd heb iddi gael ei hagor.

- Rhaid selio'r amlen yn ddiogel ac ysgrifennu **Preifat a Chyfrinachol** arni.

- Yn ymarferol, dylid anfon unrhyw wybodaeth bersonol neu wybodaeth sensitif drwy ddanfoniad cofrestredig a chadw'r wybodaeth tracio.

- Os oes modd, dylid defnyddio label wedi ei deipio neu amlen hefo ffenestr (gan sicrhau mai dim ond y cyfeiriad gellir ei weld) – gall problemau godi os yw llawysgrifen yn cael ei chamddeall.

Cludo gwybodaeth bersonol a chyfrinachol allan o'r swyddfa

Os oes angen cludo ffeiliau papur neu unrhyw bapurau sy'n cynnwys gwybodaeth bersonol neu sensitif allan o'r swyddfa, yna rhaid sicrhau eu bod yn ddiogel bob amser.
Y peth gorau ydy ceisio osgoi cario ffeiliau/papurau os oes modd e.e gall gliniadur wedi ei amgryptio fod yn ddull mwy diogel.

Egwyddorion sylfaenol wrth gludo gwybodaeth bersonol a sensitif

- Dylid cadw cofnod o unrhyw bapurau sy'n mynd allan o'r swyddfa – dylai'r cofnod nodi lle mae'r ffeil wedi mynd, pryd, pam a phwy sy'n gyfrifol amdani

- Dim ond pan mae gwirioneddol raid y dylid mynd â gwybodaeth sensitif a phersonol o'r swyddfa, h.y. pan nad oes opsiwn arall, ac yna dylid dod â nhw nol cyn gynted â phosibl.

Camau ymarferol

- Y person sy'n cludo'r dogfennau papur sy'n gyfrifol am eu diogelwch – hyd yn oed os ydynt yn eu cludo ar ran rhywun arall.

- Dylid defnyddio bag priodol bob amser ar gyfer cludo ffeiliau neu ddogfennau h.y. bag y gellir ei gau ac sy'n dal dŵr - ni ddylid byth ddefnyddio bag siopa agored i gludo gwybodaeth bersonol neu ddogfennau cyfrinachol neu sensitif. Hyd yn oed os ydi'r dogfennau mewn ffeil gadarn, fe ddylai'r ffeil gael ei chludo mewn bag.

- I staff sy'n mynd â ffeiliau allan o'r swyddfa yn aml, dylid darparu cês neu fag y gellir ei gloi

- Lle bo nifer fawr o ffeiliau yn cael eu cymryd o'r swyddfa yn aml, dylid eu cludo mewn cês neu fag sydd ar olwynion

- Dylid sicrhau bod unrhyw ffeiliau neu ffolderi mewn cyflwr da a bod papurau unigol yn sownd y tu mewn iddynt – os yw papurau yn disgyn allan neu mae'r ffeil wedi ei difrodi, dylid rhoi'r papurau mewn ffeil newydd neu drwsio'r ffeil cyn ei chludo o'r swyddfa.

- Ni ddylid darllen ffeiliau personol ar gludiant cyhoeddus neu mewn unrhyw le arall lle gall eraill eu gweld.

- Ni ddylid byth gadael dogfennau mewn car neu gerbyd lle gall eraill eu gweld.

- Cyn gadael adeilad neu gar a chyn cychwyn ar siwrne ar ôl cyfarfod/apwyntiad, dylid gwneud yn siŵr fod eich bag gyda chi.

- Dylid rhoi unrhyw ddogfennau yng nghist y car wrth deithio ac ni ddylid gadael dogfennau nag offer yng nghist car dros nos. Os bydd angen mynd â gwaith papur adra, dylid mynd â'r ffeiliau i mewn i'r tŷ a'u cadw'n ddiogel.

Gwaredu gwastraff cyfrinachol

Dylai unrhyw waith sy'n cynnwys gwybodaeth bersonol neu wybodaeth gyfrinachol gael ei waredu'n briodol ac yn unol â'r Polisi Gwaredu Gwastraff Cyfrinachol.

6. Gwybodaeth ar gyfrifiadur ac mewn adeiladau

Cyfrineiriau

Dylai cyfrineiriau fod wedi'u diogelu bob amser.

Ni ddylid arddangos cyfrineiriau ar gyfer defnydd unigol neu eu gwneud i fod ar gael i eraill mewn unrhyw ddull arall.

Mae modd addasu hawliau ar gyfer y sawl fyddai angen mynediad at adnodd penodol. Dylid cyflwyno cais wedi ei gymeradwyo i'r Ddesg Gymorth TG mewn achos o'r fath.

Mae angen i gyfrineiriau fod yn gymleth. Mae angen hyd lleiaf o 12 nod yn cynnwys llythrennau mawr a bach, rhif a symbol arbennig.

Bydd angen newid unrhyw gyfrineiriau sydd wedi eu cyfaddawdu mor fuan â sy'n ymarferol bosib.

Ni ddylid ysgrifennu cyfrineiriau na gwybodaeth logio na'u rhannu ag unrhyw un arall.

Dyfeisiau

Rhaid cloi cyfrifiaduron (CTRL+ ALT + DEL) pan adewir desgiau heb neb yn eu goruchwylio.

Dylid gogwyddo sgriniau ac allweddfyrddau i ffwrdd oddi wrth ardaloedd ble mae'r cyhoedd â mynediad a dylid gogwyddo sgriniau i ffwrdd oddi wrth ffenestri.

Mynediad Trydydd Parti

Ni ddylid rhoi manylion am sut i gael mynediad at rwydwaith y Cyngor i bartneriaid na chyflenwyr trydydd parti heb ddilyn y llwybr awdurdodi priodol. Mae prosesau ar gyfer cyfrifon trydydd parti, fel cwmnïau cefnogi systemau, wedi ei fanylu yn y polisi mynediad trydydd parti. Rhaid i gyfrifon ar gyfer unigolion o sefydliadau partneriaeth sydd angen cysylltu â'r parth corfforaethol fod wedi eu cymeradwyo gan y Tîm Cefnogaeth Gorfforaethol.

Anfon e-byst personol a chyfrinachol

- Wrth anfon neges tu allan i'r Cyngor dylid ystyried a ddylid amgryptio neu roi cyfrinair ar yr e-bost. Gall y gwasanaeth TG gynorthwyo gyda hyn.
- Wrth deipio enw'r sawl sy'n mynd i dderbyn yr e-bost, gall Outlook awgrymu enwau a ddefnyddiwyd o'r blaen. Dylid sicrhau bod yr enw a'r cyfeiriad yn gywir cyn anfon yr e-bost.
- Wrth anfon e-bost at lawer o bobl, ystyriwch os y byddai yn briodol i ddefnyddio 'bcc' nid 'cc' er mwyn sicrhau nad yw cyfeiriadau personol unigolion yn cael eu rhyddhau i unigolion eraill.
- Dylid cymryd gofal wrth ddefnyddio cyfeiriad e-bost ar gyfer grŵp. Dylid gwirio pwy sydd yn y grŵp a sicrhau bod pawb sydd ynddo i fod i dderbyn y neges.
- Mae ystyriaeth priodol angen eu gymryd cyn argraffu negeseuon ebost sy'n cynnwys data cyfrinachol gan y byddai hynny yn cyflwyno fectorau risg newydd.

Mae Polisi Defnydd Ebost gyda manylion pellach.

Mynediad i'r Rhyngrwyd

- Mae mynediad i'r Wê yn cael ei ganiatau i alluogi cydweithwyr i gael mynediad at wybodaeth ac adnoddau fel rhan o'i dyletswyddau.
- Pan arlein, dylai cydweithwyr gymryd camau cyfrifol i warchod eu hunain ac isadeiledd y Cyngor o ddeunydd niweidiol ynghyd â cholli data neu niwed arall o ganlyniad eu

gweithgareddau. Mae hyn yn cynnwys, ond nid yn gyfyngiedig i, peidio ymweld â safleoedd maleisus neu anllad, peidio gosod unrhyw negeseuon maleisus neu anllad ar y Wê a pheidio lawrlwytho eitemau o feddalwedd o'r Rhyngrwyd.

- Ni ddylid defnyddio adnodd trydydd parti anawdurdodol ar gyfer storio data yr Awdurdod os nad yw'r data i fod yn y parth cyhoeddus.
- Mae rheolaethau hidlo traffic gwê a gwrth feddalwedd maleisus mewn lle a ni ddylid cymryd unrhyw gamau i drechu neu osgoi rhain. Mae hidlo'r Wê yn cynnwys archwiliadau HTTPS fel bod modd adolygu traffic wedi ei amgryptio, am resymau cyfrinachedd defnyddwyr nid yw hynny yn cynnwys eitemau fel bancio a cyfathrebu arlein.
- Mae defnydd personol o'r Wê yn cael ei ganiatau ond dylid cyfyngu hynny i gyfnodau egwyl wedi eu cytuno yn swyddogol a ni ddylai amharu ar ddyletswyddau unrhyw unigolion.
- Mae log o ddefnydd Gwê yn cael ei gynnal a gellir ei ddefnyddio mewn achosion disgyblaeth.
- Mae polisi defnydd Rhyngrwyd gyda manylion pellach.

Mynediad i adeiladau

Dylai dulliau o reoli mynediad i adeiladau/ystafelloedd gyd-fynd â'r math o wybodaeth ac offer a gedwir yno. Mae hyn yn golygu:

- dim ond swyddogion sydd ag awdurdod i fynd i'r llefydd hynny ddylai fod yn berchen ar gyfarpar/drwydded adnabod a mynediad (e.e. bathodynnau, allweddi, codau mynediad ac ati). Ni ddylid eu rhoi/benthyg i unrhyw un arall.
- Dylai ymwelwyr arwyddo i mewn ac allan, gan nodi amser cyrraedd ac gadael, a dylent wisgo bathodyn adnabod.

Gwagio adeiladau

- Wrth gau adeilad, adleoli neu symud swyddfa, mae'n hanfodol bod unrhyw wybodaeth gyfrinachol a sensitif sydd ar bapur yn cael ei symud a naill ai'n cael ei gwaredu'n briodol neu ei symud i leoliad newydd. **Os mai chi ydi perchennog y wybodaeth dan sylw yna eich cyfrifoldeb chi ydi cymryd gofal o'r wybodaeth honno trwy gydol y broses symud.**
- Dylid cysylltu â'r Gwasanaeth Rheoli Gwybodaeth am gyngor
- Ni ddylid gadael unrhyw ddogfennau o'r math uchod yn yr eiddo.
- Yn yr un modd dylid sicrhau bod unrhyw gyfarpar cyfrifiadurol sydd ar safle yn cael ei gludo oddi yno.

7. Rhannu Gwybodaeth ar lafar

Dylid defnyddio gwybodaeth a gafwyd yn y gwaith i bwrpas gwaith yn unig. Ni ddylid trafod manylion personol gydag aelodau staff nad oes wnelo hwy ddim byd a'r mater dan sylw. Ni ddylid trafod materion cyfrinachol mewn mannau cyhoeddus y tu allan i'r gwaith na gyda pherthnasau a ffrindiau.

Wrth rannu gwybodaeth dros y ffôn, dylid sicrhau bod gan yr unigolyn y pen arall yr hawl i dderbyn y wybodaeth.

8. Meddalwedd a Chadw Gwybodaeth mewn mannau eraill

Rhaid i phob eitem o feddalwedd ar ddyfeisiau corfforaethol fod yn cael ei gefnogi ac yn ddarostyngedig i gyweiriadau a diweddariadau. Rhaid i unrhyw eitem sydd ddim yn cydweddau â safonau diogelwch y Cyngor fod yn cael ei ddiweddaru, adnewyddu neu ei ddileu.

Dylid cyflwyno unrhyw geisiadau neu ymholiadau am eitemau newydd o feddalwedd i'r Gwasanaeth TG am adolygiad ac arweiniad.

Dylai pob eitem o feddalwedd gael ei osod a'i ffurfweddu gan y Gwasanaeth TG.

Mae'r Cyngor yn darparu amgylchedd sydd yn diogelu ffeiliau busnes a data sensitif ac ni ddylid cyfaddawdu hynny drwy ddefnyddio adnoddau trydydd parti na ellir rhoi sicrwydd amdanynt e.e. Dropbox.

Dylai holl ddata busnes gael ei storio o fewn y storfa wedi ei gymeradwyo gan y Cyngor.

Nid ydi cadw ffeiliau wedi eu gwarchod gyda cyfrinair yn cael ei annog gan fod cyfrineiriau yn cael eu colli yn aml ac mae prosesau o hysbysu eraill o gyfrineiriau yn gallu tanseilio'r mesurau diogelu. Dylid defnyddio hawliau rhesymegol system i weithredu gwarchodaeth data mewn ffeiliau.

9. Cyfryngau Symudadwy a Gliniaduron

Bydd cyfryngau symudadwy yn cynnwys ond nid yn gyfyngedig i'r hyn a ganlyn:

- CDs
- DVDs
- Disgiau Gweledol
- Disgiau Caled Allanol
- Cofbinnau USB
- Darllenwyr Cardiau Cyfryngau
- Microsglodion Planedig
- Chwaraewyr MP3
- Camerâu Digidol
- Tapiau Wrth Gefn
- Tapiau Sain

Dylid prynu'r uchod trwy'r gwasanaeth TG a dim ond os yw rheswm dilys yn cael ei gyflwyno y caniateir defnyddio'r dyfeisiadau hyn gan fod risg o firws. Ar gyfer USB, dylid cysylltu â'r Ddesg Gymorth am ffurflen a'i hanfon at USB@gwynedd.llyw.cymru

Rhaid cymryd gofal arbennig i ddiogelu'r ddyfais ei hun a'r wybodaeth sy'n cael ei storio arni. Dylid dangos fod pob gofal rhesymol wedi ei gymryd i osgoi difrod neu golled.

Os ydi gwybodaeth wedi ei storio mewn un lle, sef ar y ddyfais yn unig, mae mwy o risg i'r wybodaeth gael ei cholli, gan nad oes copïau wrth gefn. Dylid felly bob amser sicrhau bod y wybodaeth wedi ei storio yn rhywle arall hefyd e.e. ar y rhwydwaith.

Pan ddaw'r dyfeisiadau i ddiwedd eu hoes, dylid eu gwaredu'n ddiogel rhag i'r wybodaeth arnynt fynd i'r dwylo anghywir. (Gweler atodiad B y polisi gwaredu gwastraff cyfrinachol uchod)

Dim ond dyfeisiau sydd yn berchen y gorfforaeth neu wedi ei gymeradwyo dylid ei gysylltu â cyfrifiaduron corfforaethol.

10. Gweithio o Bell a Gweithio o Gartref

Dylai staff sy'n gweithio o bell sicrhau bod dyfeisiadau cyfrifiadurol cludadwy sydd dan berchnogaeth y Cyngor yn cael eu cysylltu â'r rhwydwaith corfforaethol o leiaf unwaith y mis fel bod meddalwedd gwrth firws a'r polisïau grŵp yn gallu cael eu diweddaru.

Bydd dyfeisiadau cyfrifiadurol cludadwy yn cynnwys, ond nid yn gyfyngedig, i'r hyn a ganlyn:

- Gliniaduron
- Llechen
- Ffonau symudol

Mae canllawiau gweithio o bell yn cynnwys manylion pellach.

11. Digwyddiadau Diogelwch Gwybodaeth

Os bydd unrhyw wybodaeth bersonol / gyfrinachol yn cael ei cholli / lladrata neu ei datgelu mewn camgymeriad, rhaid adrodd am hyn wrth eich rheolwr llinell neu'r Rheolwr Gwybodaeth ar unwaith.

Rhaid adrodd i'r Comisiynydd Gwybodaeth am achosion o golled data sydd yn risg uchel i unigolion o fewn 72 awr o'r adeg y byddwch chi yn ymwybodol o'r golled.

Gall diffyg cydymffurfio difrifol, gan gynnwys datgelu anawdurdodedig / colli neu ladrata gwybodaeth bersonol, arwain at y Cyngor yn cael dirwy o hyd at €20 miliwn gan Swyddfa'r Comisiynydd Gwybodaeth.

12. Cyfrifoldebau am Ddiogelwch Gwybodaeth

Mae pob aelod o staff yn gyfrifol am ddiogelwch gwybodaeth. Gallai methiant i sicrhau trefniadau addas ar gyfer gwarchod gwybodaeth bersonol neu sensitif gael ei ystyried fel camymddwyn difrifol, ac felly'n destun proses ddisgyblu yn unol â pholisi a threfn disgyblu'r Cyngor.

Os ystyrir bod trosedd wedi'i chyflawni, efallai y cymerir camau pellach i gynorthwyo gydag erlyn y troseddwr/ troseddwyr.

Y Grŵp Rheoli a Diogelwch Gwybodaeth sy'n gyfrifol am oruchwylio'r drefn weithredu diogelwch gwybodaeth a sicrhau y glynir ato gan bob adran drwy'r Penaethiaid Gwasanaeth unigol.

Mae'n ofynnol i Benaethiaid Gwasanaeth weithredu'r drefn hon o ran papur a gwybodaeth electronig y gwasanaethau a byddant yn gyfrifol am sicrhau bod staff a phobl sydd eraill ag awdurdod i ddefnyddio'r systemau hynny, yn ymwybodol o'r drefn ac yn cydymffurfio ag ef yn ogystal â pholisïau eraill cysylltiedig, h.y.

- Polisi Rheoli Gwybodaeth
- Polisi Diogelu Data
- Polisi Gwaredu Gwastraff Cyfrinachol

Yr Uwch-Berchennog Risg Gwybodaeth (SIRO), Pennaeth Cefnogaeth Gorfforaethol, sydd â chyfrifoldeb yn y pen draw ac sydd â'r atebolrwydd am ddiogelwch asedau gwybodaeth y Cyngor.

13. Cyfrifoldebau Rheolwyr

Yn ychwanegol at yr uchod, mae rheolwyr â'r cyfrifoldebau a ganlyn:

- Sicrhau bod pob aelod o staff yn derbyn hyfforddiant priodol am ddiogelwch gwybodaeth a'i ddiweddaru'n rheolaidd fel sy'n briodol i'w swyddi.

- Adolygu hawliau mynediad defnyddwyr yn gyson er mwyn sicrhau bod yr hawliau cywir yn parhau i gael eu dyrannu

- Gwneud y trefniadau priodol i warchod gwybodaeth pan fo aelod o staff yn gadael neu yn newid swydd.

14. Cyfrifoldebau Cyfreithiol

Mae'r ddeddfwriaeth statudol ganlynol yn berthnasol i drefniadau diogelu gwybodaeth y Cyngor. Nid yw'r rhestr yn gyflawn.

Deddfwriaeth	**Meysydd perthnasol**
Deddf Cyfathrebu Electronig 2000	Cryptograffeg, llofnodion electronig
Rheoliad Cyffredinol Diogelu Data 2016 a Deddf Diogelu Data 2018	Diogelu a defnyddio gwybodaeth bersonol
Deddf Hawlfraint, Dyluniadau a Phatentau 1988	Lladrad meddalwedd, lawr lwythiadau cerddoriaeth, lladrata data'r Cyngor
Deddf Camddefnyddio Cyfrifiaduron 1990	Hacio a mynediad anawdurdodedig

15. Adolygu

Dylid adolygu'r drefn yma ymhen 2 flynedd.
.