Polisi Diogelwch Gwybodaeth

Ombwdsmon Gwasanaethau Cyhoeddus Cymru
Polisi Diogelwch Gwybodaeth, Rhagfyr 2019

Cynnwys

1 Diben

1.1. Mae Ombwdsmon Gwasanaethau Cyhoeddus Cymru (yr Ombwdsmon) yn gorff cyhoeddus, ac mae prosesu gwybodaeth yn rhan sylfaenol o'i swyddogaeth. Mae'n bwysig bod gennym Bolisi Diogelwch Gwybodaeth clir a pherthnasol. Mae hyn yn hanfodol ar gyfer ein cydymffurfiaeth â deddfwriaeth diogelu data a deddfwriaethau eraill ac er mwyn parchu cyfrinachedd y wybodaeth a ymddiriedir i ni.

1.2. Diben y polisi hwn yw diogelu, i safon uchel gyson, pob ased gwybodaeth. Mae'r polisi yn cwmpasu mesurau diogelwch a gymhwysir drwy fesurau technegol a sefydliadol yn ogystal ag ymddygiad pobl sy'n rheoli'r wybodaeth yn unol â'n prosesau busnes.

1.3. Mae'r polisi hwn yn elfen allweddol o fframwaith rheoli diogelwch gwybodaeth cyffredinol yr Ombwdsmon, a dylid ei ystyried ochr yn ochr â dogfennaeth arall yr Ombwdsmon, gan gynnwys:

- Cynllun wrth Gefn Parhad Busnes
- Safonau Ymddygiad Staff
- Y Gofrestr Risgiau
- Polisi Rhyddid Gwybodaeth/Diogelu Data
- Datgelu cyfrinachol (Chwythu'r chwiban)

2 Nodau

2.1 Nodau Polisi Diogelwch Gwybodaeth yr Ombwdsmon yw diogelu:

- **Cyfrinachedd** – Cyfyngir ar fynediad at ddata i'r rhai ag awdurdod priodol.
- **Integredd** – Bydd y wybodaeth yn gyflawn a chywir. Bydd pob system, ased a rhwydwaith yn gweithredu'n gywir, yn unol â'r fanyleb.
- **Argaeledd** – Bydd y wybodaeth ar gael ac yn cael ei chyflenwi i'r person cywir, ar yr adeg y bydd ei hangen.

- **Cadernid** – bydd systemau yn parhau i weithredu mewn amodau gwael ac yn cael eu hadfer i gyflwr effeithiol.

3 Amcanion

3.1 Amcanion y polisi hwn yw sefydlu a chynnal diogelwch a chyfrinachedd gwybodaeth, systemau gwybodaeth, cymwysiadau a rhwydweithiau (asedau gwybodaeth) y mae'r Ombwdsmon yn berchen arnynt neu'n eu cynnal, drwy:

- Sicrhau bod pob aelod o staff yn ymwybodol o, ac yn cydymffurfio'n llwyr â'r ddeddfwriaeth fel y'i disgrifir yn y polisi hwn ac mewn polisïau eraill.
- Disgrifio egwyddorion diogelwch ac esbonio sut y byddant yn cael eu gweithredu yn y sefydliad.
- Cyflwyno dull cyson at ddiogelwch, gan sicrhau bod pob aelod o staff yn deall eu cyfrifoldebau eu hunain yn llwyr.
- Creu a chynnal lefel o ymwybyddiaeth o fewn y sefydliad o'r angen am ddiogelwch gwybodaeth fel rhan hollbwysig o'r busnes o ddydd i ddydd.
- Diogelu asedau gwybodaeth y mae'r sefydliad yn eu rheoli, gan gynnwys cydweithio gyda chyflenwyr i ddatblygu a chynnal systemau a phrosesau diogel.
- Creu hinsawdd sy'n annog pobl i adrodd achosion o dorri'r polisi hwn.

4 Cwmpas

4.1 Mae'r polisi hwn yn berthnasol i holl wybodaeth, systemau gwybodaeth, rhwydweithiau, cymwysiadau, lleoliadau a defnyddwyr gwasanaethau'r Ombwdsmon neu wasanaethau sy'n cael eu cyflenwi o dan gontract i'r Ombwdsmon.

4.2 Mae'r polisi'n berthnasol i bob aelod o staff yr Ombwdsmon (gan gynnwys staff parhaol, staff contract, staff dros dro) ac unigolion neu sefydliadau sy'n cael eu contractio'n uniongyrchol gan yr Ombwdsmon).

5 Diffiniadau

Yr Ombwdsmon	Ombwdsmon Gwasanaethau Cyhoeddus Cymru
COODOI	Y Prif Swyddog Gweithredol a'r Cyfarwyddwr Gwelliannau
ITM	Rheolwr Technoleg Gwybodaeth
CLADOI	Y Prif Gynghorydd Cyfreithiol a'r Cyfarwyddwr Ymchwiliadau (SIRO hefyd)
SIRO	Uwch Berchennog Risgiau Gwybodaeth
IGM	Rheolwr Llywodraethu Gwybodaeth
Personal data	a ddiffinnir yn Erthygl 4(1) Y Rheoliad Cyffredinol ar Ddiogelu Data (GDPR) fel a ganlyn: *'Data personol' yw unrhyw wybodaeth sy'n gysylltiedig â pherson naturiol sydd wedi'u hadnabod neu y gellir eu hadnabod ('pwnc y data'); mae person naturiol y gellir ei adnabod yn un y gellir ei adnabod, yn uniongyrchol neu'n anuniongyrchol, yn arbennig drwy gyfeirio at adnabyddwr megis enw, rhif adnabod, data ar leoliad, adnabyddwr ar-lein neu fod un neu fwy o ffactorau sy'n benodol i hunaniaeth gorfforol, ffisiolegol, genetig, meddyliol, economaidd, diwylliannol neu gymdeithasol y person naturiol hwnnw.*
Categorïau arbennig o ddata	A ddiffinnir yn Erthygl 9(1) GDPR
	• tarddiad hil neu ethnig;
	• safbwyntiau gwleidyddol;
	• credoau crefyddol neu athronyddol;
	• aelodaeth undeb llafur;
	• data genetig;
	• data biometreg at y diben penodol o adnabod person naturiol;
	• data sy'n ymwneud ag iechyd; a
	• data sy'n ymwneud â bywyd rhyw neu gyfeiriadedd rhywiol person naturiol.

Data am euogfarnau troseddol	Fel y'i diffinnir yn Erthygl 10, mae'n golygu data personol sy'n gysylltiedig ag euogfarnau troseddol a throseddau.
Gwybodaeth bersonol sensitif arall	Data personol a allai achosi gofid o gael ei ddatgelu heb ganiatâd pwnc y data (er enghraifft, gwybodaeth ariannol, gwybodaeth am sefyllfa deuluol unigolyn [ond nad yw'n cynrychioli data personol sensitif]. Mae'r categoreiddio hwn yn debygol o fod yn oddrychol a, phan fydd aelod o staff yn ansicr, dylent drin y wybodaeth gyda mwy o ofal.
Ffugenwau	Fel y'u diffinnir yn Erthygl 4(5) GDPR: *prosesu data personol mewn dull na ellir ei briodoli mwyach i bwnc data personol heb ddefnyddio gwybodaeth ychwanegol, ar yr amod y cedwir gwybodaeth ychwanegol o'r fath ar wahân a'i fod yn destun mesurau technegol a sefydliadol i sicrhau nad yw'r data personol yn cael ei briodoli i berson naturiol sydd wedi'i adnabod neu y gellir eu hadnabod*

6 Rolau a Chyfrifoldebau

6.1 Mae'r COODOI yn atebol i'r Ombwdsmon am lywodraethu gwybodaeth yn gyffredinol. Y CLADol yw Uwch Berchennog Risgiau Gwybodaeth (SIRO) y sefydliad, sy'n gyfrifol am fonitro rheolaeth risg gwybodaeth yn y sefydliad.

6.2 Yr IGM a'r ITM sy'n gyfrifol am reoli a gweithredu'r polisi a'r gweithdrefnau cysylltiedig sy'n atebol i'r CLADOI a'r COODOI.

6.3 Bydd angen hysbysu'r ITM neu'r IGM ynglŷn ag unrhyw achosion o dorri'r polisi hwn cyn gynted â phosibl ar ôl i'r achos ddod yn hysbys.

6.4 Yr ITM a'r IGM sy'n gyfrifol am sicrhau bod pob person sydd â mynediad awdurdodedig at systemau TG yr Ombwdsmon yn ymwybodol o:

- Y polisïau diogelwch gwybodaeth sy'n berthnasol i'w meysydd gwaith
- Eu cyfrifoldebau personol dros ddiogelwch gwybodaeth
- Sut i gael cyngor ar faterion diogelwch gwybodaeth

6.5 Bydd pob aelod o staff yn cydymffurfio â'r gweithdrefnau diogelwch gwybodaeth, gan gynnwys cynnal cyfrinachedd data ac integredd data.

6.6 Bydd y Polisi Diogelwch Gwybodaeth yn cael ei gynnal, ei adolygu a'i ddiweddaru gan yr ITM a'r IGM.

6.7 Bydd pob aelod o staff yn gyfrifol yn unigol am ddiogelwch eu hamgylcheddau ffisegol lle bydd gwybodaeth yn cael ei phrosesu neu ei storio.

6.8 Bydd pob defnyddiwr system yn cydymffurfio â'r gofynion diogelwch sydd mewn grym ar hyn o bryd, ac am sicrhau hefyd bod cyfrinachedd, integredd ac argaeledd y wybodaeth a ddefnyddir ganddynt yn cael ei chynnal i'r safon uchaf.

6.9 Bydd contractau gyda chontractwyr allanol sy'n caniatáu mynediad at systemau gwybodaeth y sefydliad yn weithredol cyn y caniateir mynediad. Bydd y contractau hyn yn sicrhau y bydd staff neu isgontractwyr y sefydliad allanol yn cydymffurfio â phob polisi diogelwch priodol.

7 Deddfwriaeth

7.1 Mae'n ofynnol i'r Ombwdsmon ddilyn holl ddeddfwriaethau perthnasol y DU a'r Undeb Ewropeaidd. Bydd yr Ombwdsmon yn cydymffurfio â'r deddfwriaethau canlynol a deddfwriaethau eraill, fel y bo'n briodol:

- Deddf Ombwdsmon Gwasanaethau Cyhoeddus (Cymru) 2005
- Deddf Hawlfraint, Dyluniadau a Phatentau (1988)
- Deddf Camddefnyddio Cyfrifiaduron (1990)
- Deddf Iechyd a Diogelwch yn y Gwaith (1974)
- Deddf Hawliau Dynol (1998)
- Deddf Rhyddid Gwybodaeth (2000)
- Deddf Cydraddoldeb 2010
- Y Rheoliad Cyffredinol ar Ddiogelu Data
- Deddf Diogelu Data 2018

8 Rheoli gwybodaeth, ymwybyddiaeth a mynediad

8.1 **Categorïau o wybodaeth a ddelir gan yr Ombwdsmon**

Mae'r holl wybodaeth a ddelir gan yr Ombwdsmon wedi'i chynnwys un un o'r categorïau canlynol:

- Gwybodaeth gwaith achos ymchwiliadau
- Gwybodaeth gwaith achos ceisiadau am wybodaeth
- Gwybodaeth gwaith achos Cwynion Amdanom Ni
- Gwybodaeth y tîm rheoli
- Gwybodaeth y Panel Cynghori
- Gwybodaeth y Pwyllgor Archwilio a Sicrhau Ansawdd
- Gwybodaeth Adnoddau Dynol
- Gwybodaeth y gyflogres
- Gwybodaeth ariannol a chyfrifyddu
- Gwybodaeth cyflenwyr, adeiladau a chyfleusterau

8.2 **Rheoli diogelwch gwybodaeth**

Yr ITM a'r IGM fydd yn gyfrifol am weithredu, monitro, dogfennu a chyfathrebu gofynion diogelwch ar gyfer y sefydliad.

8.3 **Hyfforddiant ymwybyddiaeth am ddiogelwch gwybodaeth**

- Bydd hyfforddiant ymwybyddiaeth am ddiogelwch gwybodaeth yn cael ei gynnwys yn y broses sefydlu staff. Bydd yr hyfforddiant hwn yn cynnwys deall y polisi hwn yn llawn a sut mae'n berthnasol i weithgareddau'r aelod o staff o ddydd i ddydd.

- Mae strategaeth hyfforddiant llywodraethu gwybodaeth flynyddol yn nodi gofynion hyfforddiant a datblygu llywodraethu gwybodaeth y staff, gan gynnwys yr elfennau gorfodol. Mae'r strategaeth hefyd yn cynnwys cynllun cyfathrebu sy'n nodi negeseuon allweddol ar gyfer y flwyddyn i ddod. Mae hyfforddiant diweddaru gorfodol yn cael ei nodi a'i gynnwys yng nghynllun hyfforddiant blynyddol y sefydliad.

8.4 **Contractau cyflogaeth**

Bydd gofynion diogelwch staff yn cael eu trafod ar y cam recriwtio a bydd pob contract cyflogaeth yn cynnwys cymal cyfrinachedd, sy'n cyfyngu ar ddatgelu gwybodaeth gyfrinachol a gafwyd yn ystod eu cyflogaeth gyda'r Ombwdsmon.

8.5 **Rheolaethau mynediad**

Dim ond personél awdurdodedig sydd ag angen busnes y gellir ei gyfiawnhau a'i gymeradwyo fydd yn cael mynediad at ardaloedd cyfyngedig sy'n cynnwys systemau gwybodaeth neu ddata wedi'i storio. Mae pob drws i ardaloedd gwarchodedig wedi'u sicrhau gan glo ffisegol neu drwy'r system mynediad cerdyn adnabod sy'n cael ei rheoli gan y Gwasanaethau Corfforaethol.

- Y Dderbynfa: Mae'r ardal hon yn agored i'r cyhoedd yn ystod oriau swyddfa yn unig ac mae'n cynnwys un cyfrifiadur personol sydd wedi'i ddiogelu gan enw defnyddiwr a chyfrinair.
- Y Swyddfa Gyffredinol: Gall unrhyw aelod o staff roi awdurdod i gael mynediad at swyddfa cynllun agored yr Ombwdsmon, ond mae'n rhaid i'r aelod o staff perthnasol maent yn ymweld â hwy fod yn gwmni iddynt. Darperir mynediad diofyn i staff yr Ombwdsmon yn unig a hefyd dim ond i lanhawr y swyddfa berthnasol.

- Yr Ystafell Gyfathrebu TG: Y tîm TG sy'n rheoli awdurdodiad ar gyfer y mynediad hwn. Y statws mynediad diofyn yw 'dim mynediad' ac eithrio staff TG yr Ombwdsmon.
- Yr Ystafell archif: Y Gwasanaethau Corfforaethol sy'n rheoli awdurdodiad ar gyfer y mynediad hwn. Y statws mynediad diofyn yw 'dim mynediad' ac eithrio Swyddogion Gwasanaethau Corfforaethol/Cymorth Gwaith Achosion a Swyddogion Gwaith Achos CAT.

8.6 **Rheolaethau mynediad defnyddwyr**

Dylid cyfyngu mynediad at wybodaeth i ddefnyddwyr awdurdodedig ag angen busnes gwirioneddol ar gyfer cael mynediad at y wybodaeth. Y Gwasanaethau Corfforaethol sy'n rheoli hawliau mynediad ffisegol. Tîm TG yr Ombwdsmon sy'n rheoli hawliau mynediad TG.

9 Risgiau a Pharhad Busnes

9.1 **Nodi a thrin risgiau**

Mae egwyddor sylfaenol asesu a rheoli risgiau yn galw am nodi a meintioli risgiau diogelwch gwybodaeth yn nhermau eu gwerth canfyddedig o ased, difrifoldeb yr effaith a'r tebygolrwydd y bydd yn digwydd ar gyfer pob categori o wybodaeth.

Ar ôl eu nodi, bydd risgiau diogelwch gwybodaeth yn cael eu rheoli ar sail ffurfiol. Byddant yn cael eu cofnodi ar gofrestr risgiau'r Ombwdsmon a bydd cynlluniau gweithredu'n cael eu rhoi ar waith er mwyn rheoli'r risgiau hynny'n effeithiol. Bydd y gofrestr risg a'r holl gamau gweithredu cysylltiedig yn cael eu hadolygu gan y tîm rheoli ac yn cael eu hadrodd i'r Pwyllgor Archwilio a Sicrhau Risg (ARAC) yn rheolaidd. Bydd unrhyw drefniadau diogelwch gwybodaeth a roddir ar waith yn nodwedd a fydd yn cael ei hadolygu'n rheolaidd yn rhaglen rheoli risgiau'r Ombwdsmon. Bydd yr adolygiadau hyn yn helpu i nodi meysydd o arfer da parhaus a gwendidau posibl, yn ogystal â risgiau posibl a allai fod wedi codi ers cwblhau'r adolygiad diwethaf.

Dylai pob tîm gynnwys 'nodi risgiau' fel eitem sefydlog ar agenda eu

cyfarfodydd tîm.

9.2 **Digwyddiadau a gwendidau diogelwch gwybodaeth**

Mae angen hysbysu'r ITM neu'r IGM ynghylch pob digwyddiad diogelwch gwybodaeth ac unrhyw wendidau a amheuir. Bydd pob digwyddiad diogelwch gwybodaeth yn cael eu hymchwilio er mwyn sefydlu eu hachos a'u heffeithiau, gyda'r bwriad o osgoi digwyddiadau tebyg. Mae'r broses wedi'i chyflwyno yn y 'Polisi ar Weithdrefn Rheoli Digwyddiadau Diogelwch Gwybodaeth. <http://hub/LIST_Policy%20Control/Information%20Security%20Incident%20Mgt%20policy%20and%20procedure.docx>

9.3 **Parhad Busnes a chynlluniau Adfer ar ôl Trychineb**

Bydd y sefydliad yn sicrhau bod asesiadau effaith busnes, cynlluniau parhad busnes a chynlluniau adfer ar ôl trychineb yn cael eu cynhyrchu ar gyfer pob gwybodaeth, cymwysiadau, systemau a rhwydweithiau hanfodol.

Er mwyn cynorthwyo i adfer data os collir gwasanaethau, mae'n rhaid dilyn y camau gweithredu busnes fel arfer canlynol:

- Dylai'r aelod o staff cymorth perthnasol wneud copïau wrth gefn meddal (h.y. eu storio ar y gweinydd) yn dilyn unrhyw sesiwn cofnodi data/diwygio data ar unrhyw system sy'n bwysig i'r busnes sydd wedi'i gosod yn lleol e.e. systemau cyfrifyddu a'r gyflogres (Cyfrifon Sage a Chyflogres Sage).
- Cyflenwyr TG yr Ombwdsmon sy'n gyfrifol am sicrhau drychweddu gweinydd digonol, er mwyn gallu adfer data yn y tymor byr os bydd gweinydd/cymhwysiad yn methu.
- Y Tîm TG fydd yn gweinyddu'r copïau wrth gefn mewn cydweithrediad â darparwyr gwasanaeth TG yr Ombwdsmon.
- Copïau wrth gefn Dyddiol ac Wythnosol ar y Safle: Mae angen gwneud copïau wrth gefn llawn o'r gweinyddwyr yn ddyddiol ac yn wythnosol i'r gweinydd wrth gefn (sydd wedi'i leoli ar wahân i'r brif ystafell gweinyddwyr ar y llawr daear).
- Copïau wrth gefn oddi ar y safle: Bydd yr Ombwdsmon yn mynd â chopi o'r copïau wrth gefn wythnosol diweddaraf oddi ar y safle.

Mae yna dri chopi wrth gefn cludadwy y gellir eu cylchdroi'n wythnosol er mwyn sicrhau bod un copi wrth gefn bob amser oddi ar y safle ar unrhyw adeg, rhag ofn y bydd digwyddiad colli system trychinebus er enghraifft tân/lifogydd (bydd hyn yn cael ei ddisodli gan ateb copïau cwmwl cyn hir).

- Mae gwybodaeth bellach ar gael yng Nghynllun Parhad Busnes y sefydliad.

10 Polisi desg glir

10.1 Gofod desg a rhaniadau desg

- Ni ddylid gadael unrhyw wybodaeth bersonol (ac eithrio gwybodaeth bersonol y staff eu hunain) na gwybodaeth ffeil achosion ar ddesgiau heb oruchwyliaeth y tu allan i oriau swyddfa. Mae hyn yn cynnwys gwybodaeth mewn ffeiliau rhwymyn cylch, basgedi i mewn/allan, basgedi darnio 'Coch' a gwybodaeth wedi'i gosod ar raniadau desg.
- At ddibenion y polisi hwn, mae oriau swyddfa wedi'u diffinio fel dydd Llun i ddydd Gwener 9am i 5pm (ac eithrio gwyliau banc).
- Mae'n rhaid i unrhyw ddogfennau copi papur sy'n cynnwys gwybodaeth am waith achos neu unrhyw wybodaeth bersonol arall sydd i'w gwaredu gael eu dinistrio drwy ddefnyddio 'basged Goch', y mae'n rhaid ei gwagio'n ddyddiol i'r biniau gwastraff cyfrinachol mawr.
- Mae'n rhaid gwagio pob 'basged ddarnio goch' ym mhob tîm yn ddyddiol cyn i'r aelod o staff olaf yn y tîm hwnnw adael am y dydd. Rheolwyr llinell sy'n gyfrifol am sicrhau bod y broses hon yn cael ei dilyn.
- Mae gwybodaeth bersonol staff unigol (e.e. ffotograffau, eu manylion cyswllt personol eu hunain ac yn y blaen) wedi'u heithrio o'r uchod oherwydd dewis yr unigolyn yw gweledd eu data personol hwy eu hunain.

10.2 Cwpwrdd ffeilio ochr a phedestalau

Mae'n rhaid cloi pedestalau a chypyrddau ffeilio ochr desgiau (a thynnu'r allweddi a'u cadw'n ddiogel) y tu allan i oriau swyddfa os ydynt yn cynnwys ffeiliau achos/ gwybodaeth bersonol neu sensitif.

10.3 **Diogelwch mynediad**

Ni ddylid gadael eitemau sy'n galluogi mynediad at wybodaeth ddiogel (er enghraifft allweddi i ffeiliau byw/cypyrddau ffeilio ochr/cyfrineiriau ac yn y blaen) o fewn cyrraedd mewn ardaloedd hawdd eu hadnabod (e.e. ar raniadau desg, wedi'u gadael mewn pedestalau heb eu cloi ac yn y blaen) y tu allan i oriau swyddfa.

10.4 **Diogelwch ffeiliau 'archif' a ffeiliau 'byw'**

Cedwir y ffeiliau archif yn yr ystafell 'Archifau', a dylid sicrhau ei bod bob amser yn ddiogel. Bydd y Gwasanaethau Corfforaethol yn rheoli'r lefelau mynediad at y ffeiliau Archif drwy'r system cerdyn adnabod diogelwch. Bydd pob aelod o staff sy'n cael mynediad at y Ffeiliau Archif neu'r Ffeiliau Byw yn gyfrifol am sicrhau bod yr ardal yn ddiogel ar ôl ei defnyddio.

10.5 **Pob cabinet /ardal ffeilio arall**

Mae'n rhaid diogelu unrhyw ystafell/cabinet/drôr ac yn y blaen sy'n cynnwys gwybodaeth sensitif/bersonol neu waith achos, neu sy'n cynnwys asedau sy'n cael eu hystyried yn werthfawr y tu allan i oriau swyddfa.

Mae'n rhaid storio unrhyw gofnodion meddygol gwreiddiol yn ddiogel yn y sêff wrthdan y tu allan i oriau swyddfa arferol. Mae'n rhaid i staff sydd â dogfennaeth o'r fath yn eu meddiant sicrhau eu bod yn trafod y gofynion storio diogel gyda'r Gwasanaethau Cymorth Gwaith Achos neu'r Gwasanaethau Corfforaethol cyn 4pm.

11 Hawliau a rheolaeth dros fynediad at TG

11.1 **Defnyddio cyfrifiaduron personol**

- Mae'n rhaid diogelu mynediad at unrhyw gyfrifiadur personol gyda chyfrinair, ac ni ddylid ei rannu. Mae'n rhaid trefnu'r system fel y bydd yn gwrthod cyfrineiriau nad ydynt yn cyflawni'r safon ofynnol o ran cymhlethdod (mae'n rhaid iddo gynnwys nodau llythrennau bach a mawr, rhif, a nod rheoli e.e. $, ac mae'n rhaid iddo fod yn 9 nod neu fwy o hyd).

- Mae'n rhaid 'cloi' sgriniau cyfrifiaduron (neu ddyfais symudol gyfatebol) pan fydd aelod o staff yn gadael eu desg ac yn symud y tu hwnt i ystod weladwy'r sgrin. Gwneir hyn er mwyn diogelu gwybodaeth bersonol a allai fod mewn golwg, yn ogystal â diogelu yn erbyn mynediad diawdurdod i'r system TG.
- Ni ddylid gadael sgriniau cyfrifiaduron (neu ddyfais symudol gyfatebol) mewn golwg, sy'n galluogi i aelodau'r cyhoedd neu staff heb angen cyfiawn i weld y wybodaeth weld y data personol.
- Dylid troi cyfrifiaduron personol neu liniaduron nad ydynt yn cael eu defnyddio i ffwrdd neu dylid allgofnodi neu ddefnyddio dyfais arbedwr sgrin ddiogel.

11.2 **Rheoli mynediad cyfrifiadurol**

Bydd mynediad at y cyfleusterau cyfrifiadurol yn cael ei gyfyngu i ddefnyddwyr awdurdodedig sydd ag angen busnes i ddefnyddio'r cyfleusterau. Dim ond defnyddwyr sydd wedi'u hawdurdodi gan yr ITM (neu aelod dirprwyedig o'r tîm TG) y gellir eu hychwanegu i systemau TG yr Ombwdsmon.

11.3 **Rheoli mynediad cymwysiadau**

Dylid rheoli a chyfyngu mynediad at ddata, cyfleustodau system a llyfrgelloedd ffynonellau rhaglenni i'r defnyddwyr awdurdodedig hynny sydd ag angen busnes dilys e.e. gweinyddwyr systemau neu gronfeydd data. Bydd awdurdod i ddefnyddio cymhwysiad yn ddibynnol ar argaeledd trwydded gan y cyflenwr.

11.4 **Diogelu rhag meddalwedd maleisus**

Bydd y sefydliad yn cysylltu â chyflenwyr TG yr Ombwdsmon i gael cyngor ac argymhellion ar wrthfesurau a gweithdrefnau rheoli meddalwedd digonol er mwyn diogelu ei hun yn erbyn y bygythiad o feddalwedd maleisus. Disgwylir i bob aelod o staff gydweithredu'n llawn â'r polisi hwn. Ni all defnyddwyr osod unrhyw feddalwedd ar eiddo'r sefydliad heb ganiatâd gan yr ITM.

11.5 **Cof bach USB neu gyfryngau tebyg defnyddwyr**

Mae'n rhaid sicrhau cymeradwyaeth y gwasanaethau TG cyn y gellir defnyddio unrhyw ddyfeisiau cof cludadwy nad ydynt wedi'u darparu gan yr Ombwdsmon ar eu systemau, er enghraifft cof bach USB neu gyfrwng tebyg. Mae'n rhaid cynnal gwiriad rhag firysau hefyd ar gyfryngau o'r fath cyn eu defnyddio ar offer y sefydliad. Er nad yw hyn yn berthnasol i CD/DVD sy'n cael eu hanfon gan Gyrff Perthnasol oherwydd y risg is o gynnwys maleisus, er hynny, mae'n bwysig bod CD/DVD sy'n cael eu hanfon gan aelodau'r cyhoedd yn cael eu cyfeirio at y gwasanaethau TG er mwyn sicrhau nad oes unrhyw ffeiliau gweithredadwy wedi'u cynnwys ynddynt.

11.6 **Dyfeisiau symudol (e.e. gliniaduron/cyfrifiaduron llechi/ffonau clyfar)**

At ddibenion parhad busnes a chyfarfodydd yr Ombwdsmon, gall yr Ombwdsmon ddarparu ffôn clyfar a/neu gyfrifiadur llechen yr Ombwdsmon i staff awdurdodedig.

Mae polisi safonol yr Ombwdsmon ar ddefnyddio cyfrifiaduron personol yn berthnasol i'r defnydd o'r dyfeisiau hyn fel y nodwyd yn y polisi hwn ac unrhyw bolisïau perthnasol eraill yr Ombwdsmon e.e. polisi safonau ymddygiad staff.

Dylai staff sydd wedi'u hawdurdodi i ddefnyddio dyfeisiau symudol yr Ombwdsmon sicrhau bod trefniadau diogelwch digonol ar waith ar gyfer sicrhau diogelwch ffisegol y ddyfais symudol yn erbyn lladrad a / neu fynediad diawdurdod at unrhyw ddata sydd wedi'i gynnwys yn y ddyfais symudol.

- Peidiwch â defnyddio eich dyfais symudol yn gyhoeddus lle gellir gweld gwybodaeth am eich gwaith 'dros eich ysgwydd'.
- Defnyddiwch fesurau diogelu arbedwr sgrin a chyfrinair bob amser ar gyfer mynediad at ddyfeisiau symudol, a pheidiwch â rhannu'r cyfrinair hwn.
- Cadwch eich dyfais symudol mewn lleoliadau diogel bob amser, a byth heb oruchwyliaeth lle gellir ei gweld (hyd yn oed os yw'n ddiogel, e.e. ar sedd gefn eich car).

- Oni bai mae hwn yw'r opsiwn mwyaf diogel ar gael, peidiwch â gadael eich dyfais symudol yng nghist y car pan fydd y car heb oruchwyliaeth am gyfnodau estynedig, yn arbennig dros nos.
- Peidiwch â gadael i unrhyw un fewnforio dogfennau i'ch dyfais symudol gan ddefnyddio dyfeisiau cyfryngau diawdurdod. Dylid ond defnyddio dyfeisiau cyfryngau cludadwy sydd wedi'u hawdurdodi gan yr Ombwdsmon i drosglwyddo dogfennau.

Mae manylion pellach am y mesurau i'w cymryd ar gael yn yr adran 'Gweithio i ffwrdd o'r swyddfa'.

11.7 **Monitro mynediad a'r defnydd o systemau**

Bydd llwybr archwilio o fynediad at systemau a'r defnydd a wneir o ddata gan y staff yn cael ei gynnal a'i adolygu'n rheolaidd gan yr ITM.

11.8 **Achredu systemau gwybodaeth**

Bydd y sefydliad yn sicrhau bod asesiad risg yn cael ei gynnal ar unrhyw systemau, cymwysiadau a rhwydweithiau gwybodaeth newydd cyn eu gosod a'u defnyddio, at ddibenion diogelwch.

11.9 **Rheoli newidiadau system**

Bydd yr ITM yn adolygu ac yn cymeradwyo newidiadau i systemau, cymwysiadau neu rwydweithiau gwybodaeth.

11.10 **Hawliau eiddo deallusol**

Bydd y sefydliad yn sicrhau bod pob cynnyrch gwybodaeth yn cael eu trwyddedu a'u cymeradwyo'n briodol gan yr ITM. Ni fydd defnyddwyr yn gosod meddalwedd ar eiddo'r sefydliad heb ganiatâd gan yr ITM.

11.11 **Rheoli asedau'n ddiogel**

Bydd pob ased TG (caledwedd, meddalwedd, cymhwysiad neu ddata) yn derbyn ceidwad a enwir, a fydd yn gyfrifol am ddiogelwch gwybodaeth yr ased hwnnw pan fydd yn cael ei symud y tu allan i eiddo'r Ombwdsmon.

11.12 **Gweithdrefnau cyfrifiadurol a rhwydweithiau**

Bydd y broses o reoli cyfrifiaduron a rhwydweithiau yn cael eu rheoli drwy weithdrefnau safonol y Tîm TG, sydd wedi'u dogfennu ac sydd wedi'u hawdurdodi gan yr ITM.

11.13 **Diogelwch offer**

Er mwyn lleihau'r risg o golli, neu ddifrod i bob ased, bydd yr offer yn cael eu diogelu'n ffisegol rhag bygythiadau a pheryglon amgylcheddol a rhoddir nodau diogelwch arnynt. Mae angen sicrhau bod pob cyfrifiadur personol, pan fyddant wedi'u lleoli yn yr amgylchedd swyddfa agored (h.y. heb eu storio mewn ystafell storio ddiogel â mynediad cyfyngedig), yn cael ei ddiogelu gan ddefnyddio clo a gwifren ddiogelwch.

11.14 **Cael gwared ar offer TG**

Mae'n rhaid i Dîm TG yr Ombwdsmon gadw rhestr o holl offer TG yr Ombwdsmon sydd wedi'u nodi i'w gwaredu, sydd â gwybodaeth bersonol wedi'i storio arnynt, ac mae angen nodi'r cwmni gwaredu a ddefnyddiwyd. Mae angen i gytundeb ysgrifenedig fod mewn grym gyda'r Ombwdsmon a'r cwmni gwaredu, sy'n nodi'r gofynion ar gyfer gwaredu, a dylai hyn gynnwys nodi'r cwmni gwaredu fel y 'prosesydd data' o dan reolaeth YR OMBWDSMON fel y 'rheolydd data'. Mae'n rhaid cynnwys gofyniad hefyd yn y cytundeb i'r cwmni gwaredu ddinistrio gwybodaeth bersonol mewn dull diogel a bod angen cynnwys tystysgrif dinistrio yn y cytundeb.

11.15 **E-bost**

Gall y staff ddefnyddio'r swyddogaeth 'autocomplete' ar Outlook, lle bydd Outlook yn awgrymu derbynwyr yn seiliedig ar lythrennau a ddewiswyd yn flaenorol. Fodd bynnag, mae angen i'r staff sicrhau eu bod yn adolygu'r rhestr o dderbynwyr yn rheolaidd, gyda hen gyfeiriadau'n cael eu dileu. Nodir cyfarwyddiadau isod:

<u>Dileu cyfeiriad o'r rhestr</u>

(i). Agorwch neges newydd a dechrau teipio'r cyfeiriad.

(ii). Defnyddiwch y bysellau saeth i fyny ac i lawr i ddewis y cyfeiriad i'w ddileu o'r cyfeiriadau a awgrymir. Pan fydd y cyfeiriad i'w ddileu wedi'i amlygu, pwyswch y fysell **Dileu.**

Troi 'auto-complete' i ffwrdd

(i). Dewiswch 'Tools', yna 'Options';

(ii). Dewiswch y tab 'Preferences', yna 'Email Options';

(iii). Dewiswch 'Advanced Email Options', yna clirio'r blwch gwirio ar gyfer 'Suggest names while completing To, Cc, and Bcc fields'

12 Gweithio i ffwrdd o'r swyddfa (gan gynnwys gweithio gartref): Diogelwch gwybodaeth ac offer TG

12.1 Mae'n rhaid cadw pob gwybodaeth ac offer yn ddiogel bob amser. Mae'n rhaid i staff fod yn fodlon bod rhagofalon digonol ar waith i gynnal cyfrinachedd deunydd yn unol â'r Ddeddf Diogelu Data a chanllawiau, polisïau a gweithdrefnau'r Ombwdsmon.

12.2 Pan fydd cyflogai yn mynd â deunydd (er enghraifft, ffeil achos ar bapur) oddi ar y safle, y cyflogai hwnnw fydd yn gyfrifol am y deunydd am y cyfnod llawn y bydd oddi ar y safle.

12.3 Pan fydd y cyflogai yn mynd â ffeil achos ar bapur oddi ar y safle, maent yn gyfrifol am ddiweddaru'r cofnod WorkPro i gadarnhau lleoliad newydd y ffeil – er enghraifft, 'Gweithio Gartref – Perchennog yr Achos'. Bydd angen diweddaru'r cofnod WorkPro cyn mynd â'r ffeil oddi ar y safle.

12.4 Bydd yr adroddiad 'Baich Gwaith y Swyddfa' yn darparu lleoliad pob ffeil copi papur. Bydd yr adroddiad 'Lleoliad ffeiliau achosion sydd wedi cau' (sy'n cael eu storio yn y ffolder Weinyddol) yn darparu lleoliad pob ffeil copi papur sydd wedi cau.

12.5 Y cyflogai sy'n gyfrifol am sicrhau bod ffeiliau achosion ar bapur, ac unrhyw offer TG (gan gynnwys cyfrifiaduron llechen neu ffonau symudol) yn ddiogel bob amser, gan gynnwys wrth deithio.

12.6 Wrth deithio, ni ddylai'r cyflogai adael unrhyw ddeunydd neu offer TG heb eu goruchwylio.

12.7 Pan fydd angen gadael deunydd neu offer TG heb oruchwyliaeth, dylid eu storio'n ddiogel ac allan o olwg. Er enghraifft, ni ddylid gadael ffeiliau ar sedd gefn cerbyd heb oruchwyliaeth a dylid eu symud i ardal ddiogel cist y car a chloi'r car.

12.8 Mae'n rhaid i gyflogeion gadw'r holl wybodaeth yn gyfrinachol a diogel. Dylid dilyn y Gweithdrefnau Polisi Rheoli Digwyddiadau Diogelwch Gwybodaeth os bydd unrhyw achos o golli neu risgiau posibl i wybodaeth. Er enghraifft, torri i mewn neu ymgais i dorri i mewn. Dylid hysbysu'r ITM neu'r IGM ynghylch digwyddiadau neu risgiau. Ni ddylai cyflogeion ddangos (na chaniatáu i rywun ddangos) unrhyw ddata i unrhyw aelodau o'u teulu neu ymwelwyr i'r aelwyd.

12.9 Wrth edrych ar wybodaeth gyfrinachol neu sensitif wrth deithio (e.e. ar drafnidiaeth gyhoeddus), dylai staff sicrhau na all teithwyr eraill ei gweld.

12.10 Nid yw'r Ombwdsmon yn gyfrifol am unrhyw gostau sy'n gysylltiedig ag offer TG y defnyddiwr ei hun h.y. prynu, gosod, cynnal a chadw, ffioedd rhyngrwyd/ffôn.

12.11 Nid yw'r Ombwdsmon yn gyfrifol am unrhyw gostau sy'n gysylltiedig ag atgyweirio os bydd unrhyw offer personol y mae'r cyflogai yn ei ddefnyddio yn cael ei golli neu ei ddifrodi.

12.12 Bydd cymorth TG ond ar gael gan y Tîm TG yn ystod oriau swyddfa "craidd" arferol a bydd ond yn berthnasol i osodiadau cyflunio ar gyfer cysylltu â gweinydd yr Ombwdsmon.

12.13 Y defnyddiwr sy'n gyfrifol am ddatrys unrhyw faterion TG nad ydynt yn ymwneud yn uniongyrchol â gosodiadau cyflunio ar gyfer cysylltu â gweinydd yr Ombwdsmon. Er enghraifft, nid yr Ombwdsmon sy'n gyfrifol am anallu i gysylltu â'r rhyngrwyd drwy ddarparwr rhyngrwyd y defnyddiwr.

Dylai staff weithio drwy'r porth mynediad diogel o bell a WorkPro ar gyfer unrhyw ddogfennau sy'n gysylltiedig â gwaith achos. Os ystyrir bod angen gweithio y tu allan i'r porth WorkPro dros dro, mae'n rhaid i ddefnyddwyr sicrhau bod unrhyw ddogfennau sy'n cael eu harbed ar eu cyfrifiadur personol/gliniadur personol hwy ac yn y blaen yn cael eu llwytho i WorkPro a'u dileu'n llwyr o'u dyfais eu hunain ar ddiwedd y sesiwn.

12.14 Dylid dychwelyd unrhyw ddeunyddiau sy'n cael eu cludo oddi ar y safle ar unwaith ar ôl i'r cyfnod o amser y cytunwyd arno i chi weithio o gartref ddod i ben. Pan fydd cyflogai yn gweithio gartref am gyfnod o amser estynedig, dylent ddychwelyd unrhyw ffeiliau nad ydynt mewn defnydd parhaus, cyn gynted â phosibl.

12.15 Ni ddylai'r cyflogai ddinistrio na chael gwared ar unrhyw ddeunydd drwy wastraff domestig yr aelwyd. Dylid dychwelyd unrhyw ddeunydd i'r swyddfa a'i ddinistrio gan ddefnyddio biniau gwastraff cyfrinachol yr Ombwdsmon.

13 Trin gohebiaeth yn ddiogel

Gohebiaeth: Post/negesydd/e-bost allan

13.1 Mae'r adran hon yn nodi sut i drosglwyddo gwybodaeth ar ôl asesu bod y wybodaeth wedi'i hawdurdodi i'w throsglwyddo yn unol â deddfwriaethau perthnasol e.e. y Ddeddf Diogelu Data, Deddf Ombwdsmon Gwasanaethau Cyhoeddus Cymru ac yn y blaen. Cyfeiriwch at yr ITM os byddwch yn ansicr.

13.2 Mae'r adran hon o'r polisi yn cyfeirio at aelodau o staff canlynol yr Ombwdsmon;

- y CEISYDD: Yr aelod o staff hwn sy'n gwneud cais i wybodaeth gael ei hanfon.
- yr ANFONWR: Yr aelod o staff hwn sy'n gweithredu cais gan y CEISYDD. Gallai'r person hwn fod yr un unigolyn â'r ceisydd.

13.3 Mae'n rhaid i'r ceisydd ddilyn y canllawiau a nodir yn Atodiad A y polisi hwn a chyfarwyddo'r anfonwr yn unol â hynny.

13.4 Mae'n rhaid i'r holl wybodaeth a gynhwysir mewn gohebiaeth a anfonir allan, naill ai drwy'r post arferol, negesydd neu e-bost gael ei gwirio'n drylwyr gan y ceisydd, o ran y canlynol:

- manylion cywir y derbynnydd
- cynnwys cywir (gan gynnwys pob dogfen atodedig)
- Yn achos negeseuon e-bost ei bod yn briodol i unrhyw edefyn hanesyddol a'i gynnwys llawn gael ei gyfleu i'r derbynwyr bwriadedig (gan gynnwys derbynwyr CC a BCC). NODYN PWYSIG: Mae'n bolisi'r Ombwdsmon bod y ceisydd yn dileu pob neges e-bost fewnol sydd wedi'u cynnwys yn yr edefyn hanesyddol cyn anfon unrhyw neges e-bost y tu allan i'r Ombwdsmon. Mae hyn yn berthnasol i holl aelodau staff yr Ombwdsmon a phob neges e-bost yr Ombwdsmon ac nid dim ond negeseuon e-bost sy'n ymwneud ag achosion ymchwilio.
- A yw unrhyw ran o'r cynnwys yn cynnwys unrhyw wybodaeth bersonol sensitif?

13.5 Pan fydd achos yn newydd i weithiwr achos, a bod y gweithiwr achos yn anfon e-bost neu lythyr at berson sy'n gysylltiedig â chwyn am y tro cyntaf, mae'n rhaid i'r aelod o staff hwnnw gadarnhau bod yr e-bost neu'r llythyr wedi'i gyfeirio'n gywir yn erbyn ffynhonnell wreiddiol a ddarparwyd gan yr achwynwr neu'r person priodol. Er enghraifft:

- mae'n rhaid croesgyfeirio cyfeiriad post/e-bost achwynwr yn erbyn y ffurflen neu lythyr cwyno gwreiddiol;
- mae'n rhaid croesgyfeirio cyfeiriad post/e-bost aelod cyhuddedig yn erbyn gwybodaeth a dderbyniwyd gan y cyngor neu'r clerc perthnasol;
- mae'n rhaid croesgyfeirio cyfeiriad post/e-bost tyst yn erbyn gwybodaeth a dderbyniwyd gan y tyst ei hun neu'r person sydd wedi darparu eu manylion cyswllt.

13.6 Mae'r anfonwr yn gyfrifol am sicrhau:

- y rhoddir y llythyr olaf i'r gweithiwr achos (a fydd yn rhestru'r holl amgaeadau ar ddiwedd y llythyr ar ôl y llofnod) ynghyd â'r holl ddogfennau amgaeedig er mwyn i'r gweithiwr achos allu croesgyfeirio'r dogfennau hyn wrth lofnodi'r llythyr.
- na fydd unrhyw ddogfennau/gwybodaeth ychwanegol yn cael eu hanfon yn ychwanegol at y rhai y gofynnwyd amdanynt.
- y derbynnydd yw'r un y gofynnwyd amdano, mae'r cyfeiriad yn cyfateb â'r cofnod achos ar WorkPro ar gyfer y derbynnydd bwriadedig (ar y sail y bydd y gweithiwr achos eisoes wedi cadarnhau'r cyfeiriad post neu e-bost yn erbyn ffynhonnell wreiddiol a ddarparwyd gan yr achwynnwr neu'r person priodol).
- Os oes pryder ynghylch y cynnwys a sut y gofynnwyd iddo gael ei anfon, dylid ei gyfeirio'n ôl at y ceisydd e.e. mae'r anfonwr yn nodi bod y ceisydd wedi gofyn i ddogfen gael ei hanfon mewn ffordd sy'n groes i ganllawiau Atodiad A.

13.7 Dylai staff ddefnyddio proses e-bost ddiogel Egress i anfon gwybodaeth bersonol gyfrinachol neu sensitif yn ddiogel. Cyfeiriwch at broses Egress am ragor o wybodaeth.

13.8 Gall staff anfon data gyda ffugenw heb yr angen i amgryptio.

13.9 Dylai staff ddefnyddio Egress ar gyfer pob gohebiaeth gyda Chynghorwyr Proffesiynol Annibynnol. Cyfeiriwch at broses IPA am ragor o wybodaeth.

Gohebiaeth: I mewn drwy'r post/negesydd

13.10 Diogelwch wrth agor post – dylai pob aelod o staff sy'n gyfrifol am agor post fod yn ymwybodol o'r weithdrefn ar gyfer pecynnau amheus a dilyn y weithdrefn honno.

13.11 Dylai staff fod yn ymwybodol y gallai unrhyw ohebiaeth ysgrifenedig (ac eithrio'r rhai a nodir yn adran 13.6 i 13.20) a dderbynnir yn adeilad yr Ombwdsmon gael ei hagor, waeth beth yw'r marciau ar yr amlen.

Mae gohebiaeth sydd wedi'i chyfeirio at unigolyn a enwir yn eu capasiti fel aelod o'r Ombwdsmon yn berchen i'r Ombwdsmon, sydd â chyfrifoldeb dirprwyedig dros ei phrosesu i'r rheolwyr adrannol.

13.12 Os bydd aelod o staff yn gofyn i ohebiaeth bersonol gael ei hanfon i rywle ar wahân i'w cyfeiriad cartref, dylent wneud y trefniadau priodol gyda Swyddfa'r Post i ddechrau. Mewn amgylchiadau eithriadol, gall staff drefnu neu ganiatáu i ohebiaeth bersonol neu barseli gael eu hanfon i swyddfa'r Ombwdsmon, fodd bynnag, mae'n rhaid i'r staff fod yn ymwybodol y gallai gael ei hagor ac na fydd yr Ombwdsmon yn derbyn unrhyw gyfrifoldeb dros unrhyw ddifrod neu golli unrhyw gynnwys ar unrhyw gam.

13.13 Bydd achlysuron pan fydd angen anfon gohebiaeth bersonol o fewn y sefydliad ac ni fyddai'n briodol i unrhyw un, ar wahân i'r derbynnydd, agor yr ohebiaeth honno. Gallai hyn gynnwys gwybodaeth am gyflog, pensiynau, cwynion, achwyniadau ac ystod o faterion Adnoddau Dynol. Dylid ysgrifennu 'Cyfyngedig – Derbynnydd yn Unig / Restricted – Addressee Only' ar amlen gohebiaeth fewnol o natur bersonol sy'n cael ei hanfon rhwng unigolion o fewn y swyddfa.

13.14 Mae gan bob aelod o staff sy'n agor gohebiaeth gyfrifoldeb i gynnal cyfrinachedd.

13.15 Mae Erthygl 8 Deddf Hawliau Dynol 1998 - Yr hawl i barch am fywyd teuluol a phreifat - yn rhoi hawl i barch am fywyd teuluol a phreifat, cartref a gohebiaeth i bawb. Fodd bynnag, nid yw hyn yn hawl absoliwt ac mae'n rhaid i'r Ombwdsmon gydbwyso unrhyw ymyrraeth â'r hawl yn erbyn y nodau cyfreithlon sy'n cael eu dilyn.

Gohebiaeth na ddylai unrhyw berson ei agor ac eithrio'r derbynnydd a enwir

13.16 Gohebiaeth fewnol sydd wedi'i marcio â 'Cyfyngedig – Derbynnydd yn Unig'.

13.17 Gohebiaeth sydd wedi'i marcio gyda 'preifat' a/neu 'cyfrinachol' ac sydd wedi'i chyfeirio drwy enw i'r Ombwdsmon e.e. 'Preifat a Chyfrinachol, Nick Bennett' (h.y. nid "yr Ombwdsmon").

13.18 Dylid cyfeirio pob gohebiaeth sydd wedi'i chyfeirio at y 'Gwasanaethau Corfforaethol' heb ei hagor at y Gwasanaethau Corfforaethol oherwydd gallai gynnwys gwybodaeth Adnoddau Dynol bersonol am staff yr Ombwdsmon.

13.19 Dim ond y cynrychiolydd undeb perthnasol ddylai agor unrhyw ohebiaeth sydd wedi'i marcio 'ar gyfer swyddog yr undeb yn unig'.

13.20 Unrhyw ohebiaeth arall lle mae'n amlwg nad yw'n ymwneud â gwaith (e.e. gohebiaeth gan gymdeithasau staff/undebau, gohebiaeth gan ddarparwyr pensiwn sydd wedi'i marcio gyda "personol"). Yn yr achosion hyn, dylid anfon yr ohebiaeth ymlaen yn uniongyrchol at y cyfeiriwr (neu Gynorthwyydd Personol yr Ombwdsmon ar gyfer yr ail bwynt uchod).

Gohebiaeth y gellir ei hagor

13.21 Gellir agor unrhyw ohebiaeth arall, gan gynnwys gohebiaeth wedi'i marcio 'preifat a chyfrinachol' ac sydd wedi'i chyfeirio at ymchwilydd/swyddog achos, oherwydd byddai'r rhan fwyaf o achwynwyr yn cyfeirio gohebiaeth o'r fath at swyddogion achos yn breifat fel mater o drefn.

13.22 Ar ôl agor post, a chanfod ei fod o natur bersonol, dylid ei lofnodi a nodi'r rheswm dros ei agor a'i anfon at y cyfeiriwr, gan nodi 'Cyfyngedig – Derbynnydd yn Unig' ar yr amlen ac mewn amlen newydd wedi'i selio pan fydd hynny'n briodol.

13.23 Bydd angen agor cofnodion meddygol a ddaw i mewn yn ofalus heb ddifrodi'r amlen wreiddiol oherwydd efallai y bydd angen ei

chadw (e.e. ffolderi Pelydr X) ar gyfer anfon y dogfennau ymlaen/dychwelyd y dogfennau.

13.24 Dylid agor pob darn drwy agor y post ar letraws (ac eithrio amlenni Pelydr X y dylid eu cadw ar gyfer dychwelyd y delweddau Pelydr X) er mwyn sicrhau na fydd unrhyw gynnwys yn cael ei fethu neu'n cael ei adael yn yr amlen. Mae hyn yn cynnwys amlenni 'bagiau Jiffy'. Mae angen gosod pob amlen sydd wedi'i hagor yn y gwastraff cyfrinachol ar ôl sicrhau am yr ail waith bod holl gynnwys yr amlen wedi'i thynnu. Ni ddylid defnyddio amlenni neu 'fagiau Jiffy' eilwaith mewn unrhyw amgylchiadau.

13.25 Y Gwasanaethau Corfforaethol a Chymorth Gwaith Achos sy'n gyfrifol am gynnal y broses fewnol ar gyfer delio â phost sy'n dod i mewn, a dylai hyn gynnwys cyfryngau Corporate Services and Casework Support are responsible for maintaining the internal process for handling incoming post, which should also cover cludadwy sy'n dod i mewn.

Dilysu galwr sy'n dod i mewn

13.26 Dylai staff ddilysu hunaniaeth galwyr sy'n dymuno cael cyfrineiriau. Dylai staff ofyn am ddwy eitem o wybodaeth y mae'r achwynnwr (neu gynrychiolydd) yn debygol o'u gwybod – er enghraifft, enw, cyfeiriad, cod post, y corff y gwnaed cwyn amdanynt, neu unrhyw eitem o wybodaeth arall y mae'r staff yn ystyried y bydd yr achwynnwr (neu'r cynrychiolydd) yn debygol o'i gwybod. Ni ddylai staff ddatgelu cyfrineiriau oni fyddant yn fodlon bod prawf dilysu wedi'i basio.

Trosglwyddiadau ffacsimili a 'Hafan Ddiogel'

13.27 Mae'r Ombwdsmon yn gweithredu system ffacsimili electronig yn awr sy'n cael ei disgrifio fel gwasanaeth 'Hafan Ddiogel' i ddogfennau sy'n dod i mewn oherwydd dim ond drwy ddull diogelu gyda chyfrinair diogel y gellir cael mynediad ato.

13.28 Dylid ond anfon dogfennau allan sy'n cynnwys gwybodaeth bersonol drwy'r system hon yn dilyn cydsyniad penodol y derbynnydd, ar yr amod bod y wybodaeth bersonol ond yn ymwneud â hwy ac nid unrhyw drydydd parti. Mae'n rhaid i'r anfonwr gysylltu â'r derbynnydd bwriadedig cyn eu hanfon, i wneud yn siŵr bod y derbynnydd yn gallu eu derbyn ar unwaith. Dylai'r anfonwr gysylltu â'r derbynnydd hefyd ar ôl eu hanfon i gadarnhau eu bod wedi'u derbyn yn ddiogel. Mae'n rhaid hysbysu Rheolwr y Gwasanaethau Corfforaethol neu'r Tîm TG ynghylch unrhyw achosion pan fydd amheuaeth a fu'r trosglwyddiad yn llwyddiannus, er mwyn gallu cynnal archwiliad TG o lle'r anfonwyd y ddogfen iddo.

14 Adrodd ac Archwilio

14.1 Sicrwydd

Er bod diogelwch gwybodaeth yn ystyriaeth ddyddiol i'r ITM a'r IGM ac y bydd yr ITM neu'r IGM yn hysbysu'r Tîm Rheoli ynghylch unrhyw faterion sy'n cael effaith ddifrifol ar statws diogelwch y sefydliad, cyflwynir adroddiad blynyddol hefyd i'r tîm rheoli ac yna i'r Pwyllgor Archwilio a Sicrhau Ansawdd, a fydd yn cynnwys y canlynol:

- Mynediad TG: profion hacio allanol
- Mynediad TG: cydymffurfiaeth fewnol â'r polisi hwn
- Monitro ymwelwyr
- Profi cydymffurfiaeth wrth drosglwyddo gwybodaeth
- Unrhyw ddigwyddiadau colli data a chamau gweithredu dilynol ers yr adroddiad diwethaf.

14.2 Rheoli Digwyddiadau Diogelwch Gwybodaeth

Os bydd achos o ddigwyddiad a adroddwyd neu sy'n hysbys, sy'n ymwneud â cholli, neu ddatgelu data cyfrinachol mewn camgymeriad (naill ai ffeiliau electronig neu ffisegol) a ddelir gan yr Ombwdsmon, mae angen dilyn y weithdrefn ganlynol:

- Fel y nodir yn y Weithdrefn Rheoli Digwyddiad Diogelwch Gwybodaeth, mae'n rhaid hysbysu'r IGM neu'r ITM ynghylch y digwyddiad cyn gynted ag y daw i law. [Mae'r Gweithdrefnau ISIM yn cael eu diwygio yn awr]. Dylid cwblhau ffurflen digwyddiadau.

- Dylai'r IGM neu'r ITM adolygu'r ffurflen wedi'i chwblhau. Yna dylid cyfeirio'r digwyddiad at y COODOI a'r SIRO.

Dylai'r IGM (neu'r ITM os bydd y digwyddiad yn ymwneud â diogelwch TG) adrodd y digwyddiad a'r camau gweithredu dilynol i'r Tîm Rheoli fel rhan o'r adroddiad misol. Pan fo'n briodol, dylid hysbysu'r Pwyllgor Archwilio a Sicrhau Risg ynghylch y digwyddiad hefyd.

Mae'n rhaid hysbysu'r rheolwr llinell ynghylch y digwyddiad er mwyn ystyried unrhyw gamau angenrheidiol (anffurfiol neu ffurfiol), gan ystyried (pan fydd angen) unrhyw bolisïau priodol, gan gynnwys y Polisi Rheoli Perfformiad a'r Polisi Disgyblu. Fodd bynnag, ni ddylid rhestru unrhyw gamau angenrheidiol ar y ffurflen, y gellir ei datgelu i Swyddfa'r Comisiynydd Gwybodaeth mewn achos o hysbysiad o'r achos o dor diogelwch.

15 Atodiad A: Gohebiaeth drwy e-bost a'r post

<table>
<tr><td colspan="8">Dechrau</td></tr>
<tr><td rowspan="2">A yw'n gofnod gwreiddiol neu'n dystysgrif wreiddiol</td><td rowspan="2">Ydy</td><td rowspan="2">Pelydr X?</td><td>Ydy</td><td>A</td><td colspan="2"></td></tr>
<tr><td>Na</td><td>B</td><td colspan="2"></td></tr>
<tr><td>Na</td><td colspan="6"></td></tr>
<tr><td rowspan="3">A yw'r cynnwys yn cynnwys data categorïau arbennig, data euogfarnau troseddol neu wybodaeth sensitif arall (e.e. ariannol) sy'n debygol o achosi niwed neu ofid pe byddai'n cael ei datgelu'n anfwriadol?</td><td rowspan="3">Ydy</td><td rowspan="3">Copi papur neu e-bost?</td><td rowspan="2">Copi Papur</td><td rowspan="2">A yw'n gallu ffitio i mewn i amlen A4?</td><td>Ydy</td><td>C</td></tr>
<tr><td>Na</td><td>D</td></tr>
<tr><td>E-bost</td><td>E</td><td colspan="2"></td></tr>
<tr><td>Na</td><td colspan="6">↑</td></tr>
<tr><td>Eitemau lluosog o ddata personol (e.e. enwau, cyfeiriadau ac yn y blaen)?</td><td>Ie</td><td colspan="5"></td></tr>
<tr><td>Na</td><td colspan="6"></td></tr>
<tr><td rowspan="2">Copi papur neu e-bost?</td><td rowspan="2">Copi papur</td><td rowspan="2">A yw'n gallu ffitio i mewn i amlen A4?</td><td>Ydy</td><td>F</td><td colspan="2"></td></tr>
<tr><td>Na</td><td>D</td><td colspan="2"></td></tr>
<tr><td>E-bost</td><td>G</td><td colspan="4"></td></tr>
</table>

A	Negesydd wedi'i olrhain. Os yn bosibl, dylid anfon delweddau Pelydr X yn y pecyn gwreiddiol lle cawsant eu derbyn a'i roi mewn amlen arall neu mewn bocs wedi'i farcio 'Preifat a Chyfrinachol'.
B	Negesydd wedi'i olrhain.
C	Post arferol ond wedi'i farcio 'Preifat a Chyfrinachol'
D	Negesydd wedi'i olrhain
E	Egress (mewn achosion eithriadol, gellir diogelu'r ddogfen gyda chyfrinair gan ddefnyddio meddalwedd pdf)
F	Post arferol
G	E-bost arferol

Mae'r uchod yn ofynion sylfaenol. Gall staff ddewis anfon y wybodaeth unrhyw adeg gan ddefnyddio lefel uwch o ddiogelwch.

Ar gyfer C ac F: Gall staff ofyn am ddosbarthiad wedi'i recordio y post brenhinol os oes angen prawf dosbarthu e.e. terfynau amser.

Ar gyfer E: Os bydd amheuaeth, dylai staff ddefnyddio negesydd neu amgryptio.

16 Atodiad B: Arfer da negeseuon e-bost

1. **Pennawd pwnc**
   Dylai'r pennawd pwnc gynnwys rhif cyfeirnod bob amser, ond dim gwybodaeth bersonol. Dangosir enghreifftiau o benawdau pwnc safonol yr Ombwdsmon ar gyfer negeseuon e-bost isod:

   - Rhif Adnabod Achos - 201999999 - Cydnabyddiaeth
   - Rhif Adnabod Achos - 201999999 – Ymateb i'ch ymholiad
   - Rhif Adnabod Achos - 201999999 - Penderfyniad drafft
   - Rhif Adnabod Achos - 201999999 – Ymateb i sylwadau penderfyniad drafft
   - Rhif Adnabod Achos - 201999999 – Ymateb Adolygiad

2. **Anfon drwy Egress neu Outlook**
   Mae hyn yn dibynnu a yw'r wybodaeth yn y neges e-bost yn cynnwys gwybodaeth bersonol (heb gynnwys enw'r derbynnydd a'u cyfeiriad e-bost). Dylai'r tabl ar ddechrau Atodiad A eich helpu i benderfynu i ddefnyddio Egress neu Outlook i anfon eich neges.

   Gallwch anfon negeseuon e-bost o fewn WorkPro. Mantais gwneud hynny yw:

   - Bydd gan bwnc yr e-bost 'Rif Adnabod Achos - 201499999' eisoes
   - Nid oes angen ystyried edefyn hanesyddol neges e-bost
   - Nid oes angen rheoli negeseuon e-bost â llaw yn eich Mewnflwch

3. **Cadwyni e-bost**
   Oni bai yr ystyrir bod hynny'n hanfodol ar gyfer y derbynnydd, mae'n well osgoi cadwyni e-bost hir. Gallwch ddechrau e-bost newydd ond dylid cyfeirio at yr ohebiaeth yr ydych yn ymateb iddi, e.e. "Diolch am eich e-bost dyddiedig XXXX..."

4. **Rheoli negeseuon e-bost**
   Mae angen arbed negeseuon e-bost yn y cofnod perthnasol lle bynnag y bo'n bosibl. Mae hyn yn sicrhau bod y cofnodion hynny yn gywir ac yn gyfredol gyda'r ohebiaeth ddiweddaraf. Nid yw negeseuon e-bost sy'n cael eu cadw mewn mewnflwch unigol neu dîm yn hygyrch i eraill yn yr Ombwdsmon, sydd â rheswm dilys dros gael mynediad at y cofnod.

   Mae'n rhaid llwytho pob neges e-bost sy'n ymwneud ag achos i WorkPro. Yna gellir dileu'r e-bost o Fewnflwch y defnyddiwr.

Cyfeiriwch at y Polisi Rheoli Cofnodion a'r amserlenni cadw cofnodion ategol ar gyfer y cyfnod cadw perthnasol ar gyfer y gwahanol fathau o gofnodion [sy'n destun adolygiad yn awr].

5. Llofnodion e-bost

Dylai pob aelod o staff ddefnyddio llofnod safonol yr Ombwdsmon ar gyfer negeseuon e-bost i dderbynwyr allanol:

Enw Staff
Teitl Swydd yn Gymraeg / Teitl Swydd yn Saesneg
Ffôn / Tel: 01656 64XXXX

Mae pob neges e-bost a anfonir allan yn cynnwys y datganiad canlynol yn awtomatig:

--
Public Services Ombudsman for Wales/Ombwdsmon Gwasanaethau Cyhoeddus Cymru
1 Ffordd yr Hen Gae
Pencoed
Bridgend/Pen-y-Bont ar Ogwr
CF35 5LJ

www.ombudsman-wales.org.uk

This email is subject to the conditions on Confidentiality, Content and Viruses set out on the Ombudsman's website.
Mae'r e-bost hwn yn rhwym wrth yr amodau Cyfrinachedd, Cynnwys a Firysau a nodir ar wefan yr Ombwdsmon.

All calls are recorded for training and reference purposes / Bydd pob galwad yn cael ei recordio ar gyfer dibenion hyfforddi a chyfeirio

Please consider the environment - do you really need to print this email?
Ystyriwch yr amgylchedd - a oes wir angen i chi argraffu'r neges e-bost hon?