



CYNGOR BWRDEISTREF SIROL RHONDDA CYNON TAF

CANLLAWIAU YNGHYLCH – TROSGWLWYDDO GWYBODAETH BERSONOL

Fersiwn: 3

Gwybodaeth am y ddogfen	
Fersiwn:	3
Statws:	FERSIWN DERFYNOL
Dyddiad:	2 Rhagfyr 2025

Cynnwys

1.	Cyflwyniad	3
2.	Beth yw Gwybodaeth Bersonol a Chyfrinachol?	3
3.	Pam ei bod yn Bwysig Diogelu'r Wybodaeth yma?	4
4.	Risgiau Cyffredin wrth Drosglwyddo Gwybodaeth	4

Canllawiau: Trosglwyddo Gwybodaeth Bersonol

1.	Penderfynu ar y Modd Gorau o Drosglwyddo Gwybodaeth	5
2.	Trosglwyddo Gwybodaeth ar E-bost	6
3.	Trosglwyddo Gwybodaeth mewn Llythyr – Sy'n Cael ei Ddanfon Wyneb yn Wyneb neu ei Anfon Drwy'r Post	8
4.	Trosglwyddo Gwybodaeth dros y Ffôn	11
5.	Trosglwyddo Gwybodaeth drwy Borth Diogel neu Uwchlwytho ar y We	12
6.	Trosglwyddo Gwybodaeth drwy System Ffacs	13
7.	Rhoi Gwybod am Ddigwyddiad: Os Bydd Camgymeriadau'n Digwydd	13

1. Cyflwyniad

Yn ystod ein diwrnod gwaith, mae trosglwyddo gwybodaeth bersonol a chyfrinachol yn dasg gyffredin sy'n rhan o'n swyddi. Mae modd i'r canlynol fod yn rhan o hyn; rhannu gwybodaeth yn fewnol, er enghraifft drwy anfon manylion i gydweithiwr neu adran arall, neu'n allanol wrth gyfathrebu â dinasyddion, cwsmeriaid, cleientiaid, defnyddwyr gwasanaethau, neu sefydliadau partner.

Wrth drosglwyddo gwybodaeth bersonol neu gyfrinachol, dros e-bost, ffôn, drwy'r post neu unrhyw fodd arall, mae'n bosibl i gamgymeriadau ddigwydd. Mae camgymeriadau o ran cyfathrebu yn un o brif achosion torri amodau diogelu data a chyfrinachedd yn y DU. Yn y canllaw yma mae esboniad ynghylch y risgiau. Mae camau ymarferol yn cael eu cynnig yma hefyd i'ch helpu chi i leihau'r risgiau dan sylw. Bydd hyn oll yn eich helpu chi i rannu gwybodaeth yn ddiogel ac mewn modd priodol er mwyn diogelu unigolion a'r Cyngor.

Mae'r canllawiau yma'n berthnasol i bob cyflogai yn y Cyngor, felly hefyd staff asiantaethau, hyfforddeion, unigolion ar leoliadau gwaith, contractwyr, aelodau etholedig, ac unrhyw un sy'n gweithio ar ran y Cyngor (boed dros dro neu'n barhaol) sy'n ymdrin â gwybodaeth y Cyngor. Yn y canllawiau yma, mae'r canlynol yn cael eu cwmpasu: trosglwyddo gwybodaeth, boed hynny'n fewnol neu'n allanol, a phu'n a yw'r wybodaeth yn electronig, ar bapur neu mewn fformat arall.

2. Beth yw Gwybodaeth Bersonol a Chyfrinachol?

Rydyn ni'n defnyddio ystod eang o wybodaeth ynghylch ein dinasyddion a defnyddwyr gwasanaethau er mwyn cynnig gwasanaethau'r Cyngor. Mae'n debygol y bydd yn yr wybodaeth yma fanylion personol megis enwau, cyfeiriadau, gwybodaeth gyswllt, ac unrhyw ddata arall y mae modd adnabod rhywun yn eu sgil. Mae modd i wybodaeth bersonol gael ei chadw mewn sawl fformat, gan gynnwys ffeiliau papur, cofnodion electronig, ffotograffau a recordiadau awdio.

Mae unrhyw wybodaeth sydd heb ei bwriadu i'w rhannu'n gyhoeddus, hefyd yn wybodaeth gyfrinachol. Mae modd i'r canlynol fod ymhlith gwybodaeth o'r fath: gwybodaeth sy'n sensitif yn fasnachol felly, dogfennau mewnol y Cyngor, cofnodion ariannol, adroddiadau drafft, neu fanylion ynghylch gweithrediadau'r Cyngor, staff neu ddefnyddiwr gwasanaethau. Hyd yn oed os nad yw'n datgelu hunaniaeth unigolyn, mae gofyn ymdrin â gwybodaeth gyfrinachol yn ofalus yn sgil ei natur sensitif.

3. Pam ei bod hi'n Bwysig Diogelu'r Wybodaeth Yma?

Mae diogelu gwybodaeth bersonol a chyfrinachol yn hanfodol am sawl rheswm:

- **Cyfreithiol:** Mae rheidrwydd ar y Cyngor, yn gyfreithiol felly, (gan gynnwys Rheoleiddio Diogelu Data Cyffredinol a Deddf Diogelu Data 2018) i ddiogelu data personol a gofalu eu bod yn cael eu trin mewn modd diogel.
- **Moesegol:** Mae dinasyddion, defnyddwyr gwasanaethau a chydweithwyr yn ymddiried ynom ni i drin eu gwybodaeth â gofal a pharch.
- **Enw da:** Mae modd i dorri amodau data niweidio enw da'r Cyngor ac erydu hyder cyhoeddus yn ein gwasanaethau.
- **Ariannol:** Mae'n bosibl y byddai achosion difrifol o dorri amodau yn arwain at ddirwyon a chostau sylweddol y byddai gofyn i'r Cyngor eu talu.

4. Risgiau Cyffredin wrth Drosglwyddo Gwybodaeth

Mae risg ynghlwm â throsglwyddo gwybodaeth bob amser, boed hynny ar e-bost, drwy'r post, drwy borth diogel neu wyneb yn wyneb. Mae lefel a math y risg yn ddibynnol ar y dull rydych chi'n ei ddefnyddio, pa mor sensitif yw'r wybodaeth a pha mor ofalus rydych chi'n dilyn arfer da.

Mae rhai dulliau fel e-bost neu bost yn rhai cyflym a chyfleus, ond mae modd i gamgymeriadau gael eu gwneud yn rhwydd os nad yw'r manylion yn cael eu gwirio'n drylwyr. Mae eraill, fel pyrth diogel, wedi'u dylunio i leihau'r risgiau, ond mae gofyn eu defnyddio â gofal o hyd.

Ymhlith risgiau cyffredin mae:

- **Anfon gwybodaeth at y person anghywir** (er enghraifft, ar e-bost, drwy'r post, neu drwy drosglwyddo wyneb yn wyneb heb gadarnhau hunaniaeth y person)
- **Defnyddio dulliau anniogel i drosglwyddo data sensitif** (megis gwefannau sydd heb eu cymeradwyo, e-bost cyffredin ar gyfer dogfennau cyfrinachol, neu ffacs)
- **Rhannu rhagor o wybodaeth na sy'n angenrheidiol** (er enghraifft, gan gynnwys manylion personol sydd ddim yn angenrheidiol neu ffeiliau cyfan pan mae dim ond rhan ohonyn nhw sy'n angenrheidiol)
- **Peidio/methu â gwirio hunaniaeth y sawl mae'r data'n cael eu hanfon atyn nhw** (yn enwedig dros y ffôn neu wyneb yn wyneb)

Bydd bod yn effro i'r risgiau yma a dilyn y canllawiau sydd yn y ddogfen yma yn eich helpu chi ddewis y dull mwyaf diogel ac osgoi camgymeriadau cyffredin.

Canllawiau: Trosglwyddo Gwybodaeth Bersonol

1. Penderfynu ar y Modd Gorau o Drosglwyddo Gwybodaeth

Cyn i chi drosglwyddo gwybodaeth bersonol neu gyfrinachol, mae'n bwysig eich bod chi'n cymryd ennyd ac yn ystyried y modd gorau o wneud hynny. Mewn rhai achosion, bydd gofyn i chi wneud penderfyniad ar eich pen eich hun, wedi'i seilio ar y sefyllfa a sensitifrwydd yr wybodaeth. Mewn achosion eraill, efallai y bydd protocol neu weithdrefn benodol ar gyfer gwasanaeth y bydd yn angenrheidiol i chi ei ddilyn/dilyn ar gyfer trosglwyddo mathau arbennig o wybodaeth; gwiriwch bob amser a oes protocol perthnasol ar waith ar gyfer eich maes gwasanaeth chi.

Dylai'r dull rydych chi'n ei ddewis fod yn gydbwysedd rhwng yr angen am effeithlonrwydd a diogelwch. Dyma bethau allweddol i'w hystyried:

- **Pa mor sensitif yw'r wybodaeth?**

Wrth i lefel sensitifrwydd yr wybodaeth gynyddu (er enghraifft, manylion ynghylch iechyd, data ariannol, neu fusnes cyfrinachol y Cyngor), dylai lefel diogelwch y dull trosglwyddo data gynyddu hefyd.

- **Pa mor gyflym y bydd yn cyrraedd?**

Weithiau mae cyflymdra yn bwysig, ond ddylai diogelwch fyth gael ei ddiystyru. Os yw dull diogel yn cymryd ychydig yn rhagor o amser, mae fel arfer werth aros.

- **Pwy rydych chi'n anfon yr wybodaeth atyn nhw?**

Ydyn nhw'n gydweithiwr, sefydliad partner, neu'n aelod o'r cyhoedd? Ydych chi'n sicr mai nhw yw'r person cywir a bod gyda nhw'r hawl i gael yr wybodaeth?

- **Faint o wybodaeth rydych chi'n ei rhannu?**

Mae lefel y risg yn cynyddu wrth i swmp y wybodaeth gynyddu, os y bydd rhywbeth yn mynd o'i le. Mae'n bosibl y bydd gofyn defnyddio mesurau diogelu pellach ar gyfer trosglwyddo trosglwyddiadau swmpus neu drosglwyddiadau ar raddfa.

- **Beth allai fynd o'i le?**

Ystyriwch y risgiau, yw hi'n bosibl y bydd yr wybodaeth yn mynd ar goll, cael ei hanfon at y person anghywir, neu fyddai hi'n bosibl i rywun arall gael mynediad ati, sydd ddim i fod i'w gweld? Mae camgymeriadau cyfathrebu, megis anfon gwybodaeth at y person anghywir neu ddefnyddio dull anniogel ymhlith yr achosion mwyaf cyffredin o dorri amodau data.

Dewiswch y dull mwyaf diogel sy'n ymarferol bosibl ar gyfer eich sefyllfa chi.

Os fyddwch chi'n ansicr ar unrhyw adeg, gwiriwch gyda'ch rheolwr llinell neu'r garfan Rheoli Gwybodaeth cyn anfon unrhyw beth.

2. Trosglwyddo Gwybodaeth ar E-bost

Mae e-bost yn cael ei ddefnyddio'n gyffredin ar gyfer rhannu gwybodaeth, ond mae hefyd yn un o'r ffynonellau mwyaf cyffredin o dorri amodau data. O gymryd ychydig rhagor o amser i wirio manylion cyn anfon mae modd atal camgymeriadau a diogelu unigolion a'r Cyngor fel ei gilydd.

1. Gwirio Cyfeiriadau E-bost y Derbynnnydd

- **Gwiriwch bob amser bod y manylion cyswllt ar gyfer defnyddwyr gwasanaethau, dinasyddion neu bartneriaid yn gyfredol ac yn gywir.** Peidiwch â dibynnu ar hen gofnodion neu e-byst blaenorol, mae modd i fanylion e-bost pobl newid yn aml.
- **Cymrwch ofal ychwanegol wrth deipio cyfeiriad e-bost o'r newydd.** Mae modd i hyd yn oed un llythyren neu ddigid coll arwain at eich neges yn cyrraedd y person anghywir.
- **Byddwch yn wyliadwrus wrth ddewis enw'r person mae'r e-bost yn cael ei anfon ato o'r rhestr cyfeiriadau global.** Mae gyda nifer o bobl enwau tebyg neu sydd yn union yr un fath â'i gilydd. Gwiriwch deitlau swyddi, adrannau neu fanylion eraill i ofalu eich bod wedi dewis y person cywir.
- **Ail-wiriwch gyfeiriad e-bost y derbynnnydd, yn enwedig os ydych chi'n defnyddio cwblhau awtomataidd.** Mae dewis y person cyswllt anghywir yn wall sy'n gallu digwydd yn rhwydd.

2. Atodiadau

- **Byddwch yn ofalus wrth ddewis pa ffeil i'w hatodi** Gofalwch eich bod yn dewis y ddogfen gywir ar gyfer y person cywir.
- **Adolygwch gynnwys y ddogfen yn ei chyfanrwydd cyn ei hanfon.** **Cadarnhewch mai dim ond yr wybodaeth angenrheidiol rydych chi'n ei rhannu.** Ar gyfer taenlenni, gwiriwch am resi, colofnau neu daflenni sydd wedi'u cuddio sydd â data sensitif neu amherthnasol ynddyn nhw / arnyn nhw, gan gael gwared arnyn nhw os nad ydyn nhw'n angenrheidiol.
- **Labelwch atodiadau yn glir ac mewn modd addas.** Osgowch enwau generig ar ffeiliau fel "dogfen1.pdf." Defnyddiwch enwau disgrifiadol i'w gwneud hi'n eglur beth yw'r ddogfen.
- **Unwaith y bydd wedi'i hatodi, agorwch y ffeil o'r drafft o'ch e-bost er mwyn ail-wirio ei bod yn gywir, ac mai hon yw'r fersiwn derfynol.** Mae hyn yn helpu o ran osgoi camgymeriadau, megis anfon y ffeil anghywir neu fersiwn sydd wedi dyddio.

- **Rhowch gyn lleied o wybodaeth bersonol a chyfrinachol â phosibl yng nghorff yr e-bost.** Defnyddiwch atodiad ar gyfer cynnwys sensitif pryd bynnag fo hynny'n bosibl.
- **Os ydych chi'n anfon gwybodaeth sensitif, ystyriwch ychwanegu haen ychwanegol o ddiogelwch drwy ddefnyddio cyfrinair diogelu ar yr atodiad, yn enwedig ar gyfer e-byst allanol.** Mae'n arfer da ar gyfer gwybodaeth sy'n arbennig o sensitif neu sydd o natur risg uchel. Anfonwch y cyfrinair ar wahân (er enghraifft, mewn e-bost dilynol neu dros y ffôn).

3. E-byst ar Raddfa Fawr, Diogelu Cyfeiriadau E-bost, a defnyddio BCC

- **Peidiwch fyth â defnyddio e-bost cyffredin i anfon negeseuon ar raddfa fawr i grwpiau mawr o ddefnyddwyr gwasanaethau, dinasyddion, neu gysylltiadau allanol.**
Er enghraifft, mae hyn yn cynnwys anfon cylchlythyrau, diweddariadau marchnata, neu ddatganiadau pwysig i bob cwsmer, dinesydd neu ddefnyddiwr gwasanaethau. Os oes arnoch chi angen cysylltu â mwy na 75 derbynnydd, peidiwch â defnyddio e-bost confensiynol. Mae anfon e-byst ar raddfa yn cynyddu'r risg o ran torri amodau data, megis datgelu cyfeiriadau e-byst derbynnyddion neu anfon gwybodaeth i'r person anghywir.
- **Os oes arnoch chi angen anfon e-byst ar raddfa, cysylltwch â'r Swyddog Gwelliannau Digidol yn gyntaf.** Bydd modd iddyn nhw roi cyngor ynghylch datrysiadau diogel ar gyfer anfon e-byst ar raddfa sy'n diogelu gwybodaeth bersonol ac yn cydymffurfio â pholisïau'r Cyngor.
- **Wrth anfon e-bost at sawl derbynnydd ar yr un pryd, na ddylen nhw weld cyfeiriadau e-bost ei gilydd (er enghraifft defnyddwyr gwasanaethau neu bersonau cyswllt allanol), defnyddiwch y maes BCC (blind carbon copy) bob tro.** Mae hyn yn fodd o helpu i ddiogelu preifatrwydd ac atal datgelu manylion cyswllt ar ddamwain.
- **Os ydych chi'n ansicr ynghylch defnyddio BCC neu os oes arnoch chi angen cyngor ynghylch cyfathrebu ar raddfa, gwiriwch gyda'ch rheolwr llinell.**

4. Ar Ôl Anfon

- **Ble bynnag bo'n bosibl, gofynnwch am dderbynneg danfon a darllen fel eich bod chi'n gwybod bod yr e-bost wedi cyrraedd a chael ei agor.**
- **Monitrowch am unrhyw bost sy'n cael ei anfon yn ôl neu nad oes modd ei ddanfon** a dilyn trywydd hynny i ofalu bod yr wybodaeth yn cyrraedd y derbynnydd.
- **Os byddwch chi'n sylweddoli eich bod wedi gwneud camgymeriad** (er enghraifft, wedi anfon gwybodaeth at y person anghywir neu wedi atodi'r ffeil anghywir), rhowch wybod ar unwaith a dilyn gweithdrefnau'r Cyngor. Mae modd i weithredu chwim helpu i reoli unrhyw niwed posibl.

3. Trosglwyddo Gwybodaeth mewn Llythyr – Wyneb yn Wyneb neu yn Y Post

Mae hi'n ofynnol anfon gwybodaeth mewn llythyr neu yn y post weithiau, ond mae risgiau unigryw ynghlwm â hynny, megis mynd ar goll, dwyn, neu gael ei anfon/ddanfon i'r cyfeiriad anghywir. Mae cymryd gofal ychwanegol ar bob cam yn fodd o helpu i gadw gwybodaeth yn ddiogel.

1. Paratoi'r Wybodaeth

- **Gwiriwch fod y cyfeiriad yn gyfredol ac yn gywir.** Peidiwch â dibynnu ar hen gofnodion, cadarnhewch gyfeiriad y derbynnydd, yn enwedig ar gyfer defnyddwyr gwasanaethau, dinasyddion, neu bartneriaid allanol.
- **Ar gyfer dinasyddion neu ddefnyddwyr gwasanaethau:** Defnyddiwch eu henwau llawn (nid dim ond llythrennau cyntaf eu henwau) a chwblhau'r cyfeiriad gan gynnwys y cod post. Marciwch yr amlen yn glir at y derbynnydd mae'r post ar ei gyfer, yn enwedig wrth anfon gwybodaeth gyfrinachol neu sensitif.
- **Ar gyfer asiantaethau neu sefydliadau partner:** Cofiwch gynnwys enw llawn y cwmni neu'r sefydliad. Os yw'r llythyr at sylw person penodol, ychwanegwch ei enw llawn a theitl ei swydd. Ail-wiriwch lle dylech chi anfon y llythyr, gan ei bod yn bosibl y bydd y derbynnydd mae'r post ar ei gyfer, wedi'i leoli mewn lleoliad ar wahân i'r prif gyfeiriad postio. Marciwch yr amlen yn glir ar gyfer y derbynnydd mae'r post at ei gyfer er mwyn gofalu y bydd yn ei gyrraedd yn uniongyrchol neu y bydd yn dilyn y trywydd cywir i gyrraedd y person cywir.
- **Ail-wiriwch y cynnwys cyn anfon y llythyr.** Gofalwch eich bod dim ond yn anfon y dogfennau cywir, a dim ond yr hyn sy'n angenrheidiol.
- **Os ydych chi'n anfon gwybodaeth sensitif neu gyfrinachol, defnyddiwch amlen ddwbl.** Dodwch y dogfennau mewn amlen fewnol wedi'i nodi â "Preifat a Chyfrinachol," yna glynwch yr amlen honno â sêl a'i rhoi yn yr amlen allanol. Mae'r cam ychwanegol yma'n helpu i ddiogelu'r wybodaeth os bydd yr amlen allanol yn cael ei difrodi neu ei hagar wrth gael ei chludo, ac mae'n fodd o ofalu mae dim ond y sawl mae'r post ar ei gyfer fydd yn gweld y cynnwys sensitif.
- **Cofiwch gynnwys cyfeiriad dychwelyd ar yr amlen.** Mae hyn yn galluogi i'r post gael ei ddychwelyd yn ddiogel i'r Cyngor.

2. Anfon Gwybodaeth yn y Post

- **Dewiswch dull anfon diogel os yn angenrheidiol.** Ar gyfer gwybodaeth sy'n hynod sensitif neu'n risg-uchel, ystyriwch ddefnyddio gwasanaethau anfon ac olrhain

neu wasanaeth danfon mae modd ymddiried ynddo, fel bod modd i chi olrhain y post a chael cadarnhad ei fod wedi cyrraedd.

- **Gofalwch fod yr amlen yn ddigon cryf i gael ei chludo heb ei difrodi.** Defnyddiwch amlen sy'n ddigon cryf a diogel i ddiogelu'r cynnwys rhag difrod neu agor ar ddamwain yn ystod cludo, yn enwedig ar gyfer gwybodaeth sensitif neu gyfrinachol.
- **Cadwch mewn cof lle mae basgedi post allanol yn cael eu lleoli.** Ddylai basgedi post ddim cael eu gosod ar ddesgiau derbynfeydd mewn mannau cyhoeddus lle byddai modd i rywun symud y post neu ymyrryd ag e. Gofalwch bob amser bod post sydd i'w anfon yn cael ei gadw mewn ardal ddiogel hyd nes y bydd yn cael ei gasglu i'w anfon/ddanfon.
- **Cadwch gofnod o'r hyn gafodd ei anfon/ddanfon, at bwy a phryd.** Mae modd i hyn fod yn ddefnyddiol wrth olrhain, at ddibenion archwilio, neu mewn achosion o ddigwyddiad.
- **Gofynnwch am gadarnhad bod y post wedi cyrraedd lle bo hynny'n anghrheidiol** ar gyfer dogfennau sensitif a/neu wirio olrhain y post.
- **Monitrwch am bost sydd heb gyrraedd ei gyrchfan neu sydd wedi'i ddychwelyd.** Os bydd llythyr yn cael ei ddychwelyd neu eich bod yn effro i'r ffaith nad yw wedi cyrraedd ei gyrchfan, ewch ar drywydd hynny cyn gynted ag y bo modd a rhoi gwybod ynghylch unrhyw ddata y gallai fod ar gael neu unrhyw dorri amodau data posibl yn unol â gweithdrefnau'r Cyngor.

3. Danfon yr Wybodaeth Wyneb yn Wyneb

- **Ewch i'r lleoliad ar unwaith lle bynnag fo hynny'n bosibl a diogelu'r ddogfen sy'n cael ei chludo.**
- **Lle bynnag bo'n bosibl, rhwch y llythyr yn uniongyrchol yn llaw'r derbynnydd y mae'r llythyr ar ei gyfer.** Dyma'r modd mwyaf diogel o ofalu bod yr wybodaeth yn cyrraedd y person cywir.
- **Os oes arnoch chi angen postio'r llythyr drwy'r blwch llythyrau a bod dim ateb, postiwch y llythyr dim ond os ydych chi'n hyderus mai hwn yw'r cyfeiriad cywir.** Ail-wiriwch fanylion y cyfeiriad cyn postio, yn enwedig ar gyfer gwybodaeth sensitif neu gyfrinachol, er mwyn osgoi datgelu ar ddamwain.

Anfon Post ar Raddfa

Pan fydd arnoch chi angen anfon gwybodaeth at nifer fawr o unigolion (er enghraifft, pob defnyddiwr gwasanaethau, dinesydd, neu gwsmer), rydyn ni'n argymhell yn gryf eich bod yn

defnyddio gwasanaethau Argraffu/Post y Cyngor. Mae'r dull yma nid yn unig yn fwy diogel, ond mae'n gymorth hefyd o ran effeithlonrwydd ac arbedion o ran costau.

Wrth ddefnyddio'r gwasanaeth Argraffu/Postio, gofalwch eich bod yn nodi'n union sut y dylai'r dogfennau gael eu trin a'u diogelu, yn enwedig os oes ynddyn nhw wybodaeth gyfrinachol. I gael gwybodaeth neu i drefnu postio ar raddfa, cysylltwch â'r Uned Cymorth Busnes.

4. Trosglwyddo Gwybodaeth dros y Ffôn

Mae rhannu gwybodaeth bersonol dros y ffôn yn fodd cyflym a chyfleus, ond mae risgiau ynghlwm ag e hefyd, yn enwedig os nad oes modd i chi fod yn sicr eich bod yn siarad â'r person cywir. Cymrwch gamau pob amser i gadarnhau hunaniaeth a diogelu gwybodaeth.

1. Gwneud Galwad (Pan mae Chi sy'n Ffonio'r Person)

- **Cadarnhewch eich bod yn siarad â'r person cywir cyn rhannu unrhyw wybodaeth bersonol neu gyfrinachol.**

Mae hyn yn bwysig oherwydd mae'n bosibl y bydd rhywun arall yn ateb y ffôn (er enghraifft, aelod o'r teulu, cydweithiwr, neu swyddog y dderbynfa), neu mae'n bosibl y byddwch chi wedi deialu'n anghywir a chyrraedd y rhif anghywir.

- Gofynnwch i'r person gadarnhau manylion allweddol (megis eu henw llawn, cyfeiriad, neu gyfeirnod).
- Os byddwch chi'n cyrraedd rhywun arall, peidiwch â datgelu gwybodaeth; yn syml, gadewch eich enw, adran, a chais i'r derbynnydd mae'r wybodaeth ar ei chyfer eich ffonio chi nôl.

Peidiwch â gadael gwybodaeth bersonol na chyfrinachol mewn negeseuon voicemail. Gadewch eich enw, adran a chais i'r person perthnasol eich ffonio nôl, yn unig. Mae hyn yn bwysig yn enwedig ar gyfer llinellau daear, lle mae modd i eraill ar yr aelwyd, neu yn y gweithle gael mynediad at negeseuon.

- **Gofalwch na all neb glywed eich sgwrs.** Osgowch drafod gwybodaeth sensitif mewn swyddfeydd agored neu fannau cyhoeddus.

2. Derbynn Galwadau (Pan Fyddwch Chi'n Ateb yr Alwad)

- **Gwiriwch hunaniaeth y sawl sy'n galw bob amser, cyn rhannu unrhyw wybodaeth bersonol neu gyfrinachol.**
 - Ar gyfer defnyddwyr gwasanaethau, dinasyddion, neu gleientiaid, gofynnwch am y manylion y dylen nhw fod yn eu gwybod (megis enw llawn, cyfeiriad, dyddiad geni, neu gyfeirnod).
 - Ar gyfer sefydliadau neu asiantaethau partner, gofynnwch am enw llawn y person, teitl ei swydd, ac enw'r sefydliad. Os nad ydych chi'n eu hadnabod, cymrwch eu prif rif ffôn switsfwrdd a'u ffonio nhw nôl i gadarnhau eu hunaniaeth.
- **Os oes rhywun yn galw ar ran person arall, gwiriwch fod gyda chi'r hawl ac awdurdod priodol i drafod y mater neu i rannu gwybodaeth gyda nhw.** Peidiwch â chymryd yn ganiataol bod gyda chi'r hawl i wneud hynny, cadarnhewch cyn bwrw ymlaen.

- **Peidiwch fyth a rhannu gwybodaeth os ydych chi'n ansicr ynghylch hunaniaeth y sawl sy'n galw.** Esboniwch yn gwrtais bod arnoch chi angen gwirio eu manylion cyn bwrw ymlaen.

5. Trosglwyddo Gwybodaeth drwy Byrth Diogel neu'r Uwchlwytho Dros y We

Mae'r Cyngor yn defnyddio systemau ar-lein diogel o'r enw "pyrth diogel" neu "uwchlwythiadau gwe" yn fwyfwy aml, ar gyfer rhannu gwybodaeth bersonol neu gyfrinachol. Gwefannau neu lwyfannau arbennig yw'r rhain sydd wedi'u dylunio i gadw gwybodaeth yn ddiogel pan mae hi'n cael ei rhannu rhwng aelodau o staff y Cyngor a sefydliadau partner. Er enghraifft, efallai y byddwch chi'n defnyddio porth diogel i anfon dogfennau at gorff cyhoeddus arall, uwchlwytho ffeiliau ar gyfer darparwr gwasanaeth dan gontract, neu ar gyfer rhannu gwybodaeth gydag asiantaeth bartner.

Wrth rannu gwybodaeth gyda dinasyddion neu ddefnyddwyr gwasanaethau, mae rhai gwasanaethau yn y Cyngor yn defnyddio Egress, system ddiogel ar gyfer e-byst a throsglwyddo ffeiliau, ar gyfer rhannu gwybodaeth sensitif a chyfrinachol yn rheolaidd. Mae mynediad at Egress yn cael ei roi pan fo angen busnes am hynny. Os yw'n angenrheidiol ar gyfer eich gwasanaeth, dylai'ch Rheolwr Llinell gysylltu â'r Ddesg Wasanaeth TGCh i gael gwybod rhagor.

Er bod y systemau yma'n fwy diogel nag e-bost neu'r post, mae'n bwysig o hyd, ein bod yn dilyn arfer da i ofalu bod gwybodaeth yn mynd drwy'r bobl iawn yn unig, ac yn cael ei diogelu o hyd.

Arfer Da ar gyfer Pyrth Diogel ac Uwchlwytho dros y We

- **Defnyddiwch byrth diogel neu systemau sydd wedi dilysu gan y Cyngor, yn unig.** Peidiwch fyth ag uwchlwytho gwybodaeth bersonol na chyfrinachol ar wefannau neu lwyfannau sydd heb eu dilysu. O bryd i'w gilydd, mae'n bosibl y byddwch chi'n cael dolen gan sefydliad neu asiantaeth partner sy'n gofyn i chi uwchlwytho gwybodaeth ac sydd â dolen we ynddi. **Peidiwch fyth ac uwchlwytho gwybodaeth oni bai eich bod chi'n gwbl sicr bod y mecanwaith uwchlwytho wedi'i ddilysu gan y Cyngor a bod y cais yn un dilys.** Os oes gyda chi unrhyw amheuaeth o gwbl ynghylch dilysrwydd/cyfreithlondeb y cais neu ddiogelwch y porth, gwiriwch gyda'ch Rheolwr Llinell, y garfan Rheoli Gwybodaeth, neu'r Adran TGCh cyn bwrw ymlaen.
- **Gwiriwch fod y wefan neu'r porth yn ddiogel.** Edrychwch am "https://" yn y cyfeiriad ac unrhyw frandio sy'n perthyn i'r Cyngor neu'r sefydliad partner.
- **Gwiriwch fynediad y derbynnydd.** Gofalwch mai unigolion sydd wedi'u cymeradwyo, yn unig, sydd â mynediad at yr wybodaeth rydych chi'n ei huwchlwytho neu ei rhannu.

- **Dilynwch unrhyw ganllawiau penodol ar gyfer uwchlwytho neu rannu ffeiliau.** Wrth ddefnyddio rhai systemau, mae gofyn i chi osod hawliau neu roi gwybod i'r derbynnydd ar wahân.
- **Ail-wiriwch yr wybodaeth cyn uwchlwytho.** Gofalwch eich bod chi'n rhannu'r ffeiliau cywir a dim ond yr wybodaeth sy'n angenrheidiol.
- **Cadwch gofnod o'r hyn sy'n cael ei uwchlwytho, at bwy, a phryd.** Mae modd i hyn helpu o ran dibenion olrhain ac archwilio.

Os ydych chi'n ansicr ynghylch diogelwch porth neu os oes gyda chi bryderon, cysylltwch â'r garfan Rheoli Gwybodaeth neu TGCh i gael cyngor cyn bwrw ymlaen.

6. Trosglwyddo gwybodaeth ar Ffacs

Dyw ffacs ddim yn cael ei ganiatáu bellach ar gyfer trosglwyddo gwybodaeth bersonol neu gyfrinachol yn y Cyngor. Y rheswm am hyn yw bod risgiau sylweddol o ran diogelwch gwybodaeth wrth ddefnyddio peiriannu ffacs. Mae modd i negeseuon ffacs gael eu deialu'n anghywir, a chanlyniad hynny yw bod dogfennau sensitif yn cael eu hanfon at y derbynnydd anghywir. Yn ogystal â hynny, mae peiriannau ffacs yn aml yn cael eu rhannu, neu maen nhw wedi'u lleoli mewn ardaloedd cyhoeddus neu gymunedol, a chanlyniad hynny yw ei bod yn bosibl i unigolion sydd heb awdurdod gael mynediad at y dogfennau, neu mae'n bosibl y bydd dogfennau'n cael eu gadael heb eu goruchwyllo. Does dim modd dibynadwy o gadarnhau pwy mae gwybodaeth sydd wedi'i throsglwyddo ar ffacs yn ei chyrraedd, na phwy sy'n ei chasglu, a dyw ffacs ddim yn darparu diogelwch digonol na llwybrau archwilio ar gyfer data sensitif.

Os bydd unrhyw un yn gofyn i chi anfon gwybodaeth bersonol neu gyfrinachol ar ffacs, peidiwch â gwneud hynny. Yn hytrach, defnyddiwch un o'r dulliau diogel sydd wedi'u hawdurdodi ac sydd wedi'u nodi yn y canllawiau yma, neu cysylltwch â'r garfan Rheoli Gwybodaeth i gael cyngor.

7. Rhoi Gwybod am Ddigwyddiadau: Os Bydd Camgymeriadau'n Digwydd

Er ymdrechion gorau pawb, mae modd i gamgymeriadau ddigwydd wrth drosglwyddo gwybodaeth bersonol neu gyfrinachol. Os ydych chi o'r farn bod gwybodaeth wedi mynd ar goll, wedi cael ei hanfon at y person anghywir, neu fod rhywun wedi cael mynediad ati sydd ddim i fod i wneud hynny, neu os oes gyda chi bryderon ynghylch torri amodau data, posibl, mae'n bwysig gweithredu ar unwaith. O roi gwybod yn gyflym mae modd i'r Cyngor archwilio, rhoi cymorth i'r sawl sydd wedi'u heffeithio a chymryd camau gweithredu i atal materion pellach rhag codi. Mae hefyd yn ein helpu i fodloni ein rhwymedigaethau cyfreithiol yn unol â deddfwriaeth diogelu data.

Beth sydd eisiau i chi ei wneud:

- **Rhaid i gyflogaeion, staff asiantaeth, hyfforddeion, unigolion ar leoliadau gwaith, ac unrhyw un sy'n gweithio i'r Cyngor neu ar ei ran (boed dros dro neu'n barhaol) roi gwybod ar unwaith am unrhyw achos neu ddigwyddiad diogelwch gwybodaeth posibl, amheus, neu wirioneddol, i'r canlynol:**
 - Eu Rheolwr Llinell, a
 - Desg Gwasanaeth TGCh
- **Rhaid i Aelodau Etholedig** roi gwybod am unrhyw achosion neu ddigwyddiadau diogelwch gwybodaeth posibl ar unwaith i Swyddog Monitro'r Cyngor, a fydd yn rhoi gwybod i'r Ddesg Gwasanaeth TGCh ar eu rhan.

Os fyddwch chi'n ansicr ar unrhyw adeg a yw rhywbeth yn ddigwyddiad, mae'n well rhoi gwybod amdano a gofyn am gyngor.

Rheoli'r Fersiwn

Rhif y Fersiwn	Yn ddilys o	Yn ddilys hyd at	Newidiadau wedi'u gwneud
1.0	30.06.2016	06.10.2016	Wedi'i ailfformatio yn ganllaw gweithdrefn.
2.0	07.10.2016	01.12.2025	Wedi'i ddiwygio i'r canllawiau.
3.0	02.12.2025		Yr adolygiad llawn wedi'i ddiweddarau gydag arfer gweithio ac arfer da cyfredol.