Polisi Trin Data Personol

Fersiwn 4.0

sirgar.llyw.cymru

Cyngor Sir Gâr
Carmarthenshire
County Council

Cynnwys

Rhan 1

1. Cyflwyniad

1.1 Mae Cyngor Sir Caerfyrddin (Y Cyngor) yn casglu ac yn defnyddio amrywiaeth eang o wybodaeth am unigolion er mwyn cyflawni ei swyddogaethau a darparu ei wasanaethau. Mae'r bobl hyn yn cynnwys ein cwsmeriaid, cleientiaid, gweithwyr a thrigolion y Sir a'u data personol nhw yw'r wybodaeth rydym ni'n ei chadw amdanynt Os methwn â gofalu'n ddigonol am y data personol sy'n cael ei drin gennym, a'i fod yn cael ei golli, ei ddwyn, ei ddatgelu mewn modd amhriodol, neu ei gamddefnyddio mewn modd arall, gallai effaith hynny ar yr unigolion dan sylw fod yn ddifrifol, gan amrywio o boen meddwl i niwed corfforol. Felly mae data personol yn ased gwerthfawr, ond byddwn hefyd yn atebol os byddwn yn trin y wybodaeth honno mewn modd anghywir.

1.2 Lluniwyd y polisi felly er mwyn sicrhau bod data personol yn cael ei drin yn ddiogel, ac yn enwedig ei storio a'i drosglwyddo, er mwyn cynorthwyo i gydymffurfio â rhwymedigaethau cyfreithiol y Cyngor. Mae'r Polisi hwn hefyd yn nodi gofynion y Cyngor ar gyfer sicrhau bod achosion o dorri rheolau data yn cael eu riportio ac yr ymatebir iddynt mewn modd amserol ac effeithlon.

1.3 Mae'r polisi hwn yn disodli'r Polisi a'r Weithdrefn ar gyfer Trin Gwybodaeth Bersonol a'r Polisi Rhoi gwybod am Achosion Torri Amodau ac Ymateb iddynt.

2. Mesur cydymffurfiaeth

2.1 Mae'n orfodol cydymffurfio â'r polisi hwn. Os bydd staff yn torri'r polisi hwn, yna gall arwain at gymryd camau disgyblu yn erbyn y gweithwyr sy'n gyfrifol am wneud hynny.

3. Noddwr

3.1 Eiddo'r Grŵp Llywodraethu Gwybodaeth Corfforaethol yw'r polisi hwn.

4. Gwarchodwr

4.1 Cyfrifoldeb y Swyddog Diogelu Data yw sicrhau bod y polisi hwn yn cael ei adolygu a'i ddiweddaru.

5. Datganiadau polisi

5.1 Mae Cyngor Sir Caerfyrddin wedi ymrwymo i brosesu data personol yn unol â gofynion y Ddeddfwriaeth Diogelu Data.

5.2 Mae'r Cyngor yn ystyried bod trin data personol mewn modd priodol yn hanfodol wrth ddarparu ein gwasanaethau a chynnal hyder y bobl rydym yn ymdrin â nhw.

5.3 Bydd pob gwybodaeth bersonol a gedwir gan y Cyngor nad yw'n agored i'r cyhoedd yn cael ei hystyried bob amser yn wybodaeth gwbl gyfrinachol.

5.4 Bydd y Cyngor yn defnyddio dulliau electronig diogel gymaint â phosibl i brosesu data personol, gan gynnwys ei greu, ei storio a'i drosglwyddo.

5.5 Cafodd y polisi hwn ei gymeradwyo gan Gabinet y Cyngor ac mae'n cael ei gefnogi'n llwyr ganddo.

6. 5. Diffiniad o ddata personol

6.1 Y diffiniad cyfreithiol o ddata personol yw unrhyw wybodaeth sy'n ymwneud â phersonau naturiol (hynny yw, unigolion yn hytrach na sefydliadau) y gellir eu hadnabod, neu y gellir eu hadnabod yn uniongyrchol o'r wybodaeth, neu y gellir eu hadnabod yn anuniongyrchol o'r wybodaeth, mewn cyfuniad â gwybodaeth arall. Defnyddir y termau 'data personol' a 'gwybodaeth bersonol' yn y polisi hwn a'r un yw eu hystyr.

6.2 Yn ymarferol, mae hyn yn debygol o gynnwys amrywiaeth eang iawn o ddata, gan gynnwys y canlynol, ond nid y canlynol yn unig:

- Enwau, cyfeiriadau a dyddiadau geni
- Cyfeirnodau, megis rhifau gweithwyr neu rifau yswiriant gwladol
- Gwybodaeth ariannol bersonol megis manylion banc
- Gwybodaeth ddisgrifiadol neu fywgraffyddol am unigolyn
- Ffotograffau neu ddelweddau eraill

6.3 Hefyd mae categorïau arbennig o ddata personol ac mae'n rhaid inni fod yn ofnadwy o ofalus wrth ymdrin â'r rhain. Y categorïau arbennig hyn yw data personol ynghylch:

- Hil neu gefndir ethnig
- Barn wleidyddol
- Cred Grefyddol neu Athronyddol
- Aelodaeth o undeb llafur
- Data genetig
- Data Biometrig
- Iechyd
- Bywyd rhywiol neu gyfeiriadedd rhywiol

6.4 Yn ogystal mae gofynion penodol ar gyfer data personol mewn perthynas â chollfarnau troseddol a throseddau.

7. Cefndir Cyfreithiol

7.1 Mae'r ddeddfwriaeth Diogelu Data (sy'n cynnwys Deddf Diogelu Data 2018 a Rheoliad Diogelu Data Cyffredinol y DU) yn nodi rheolau sy'n ymwneud â phrosesu data personol. Diffinnir prosesu fel casglu, cofnodi, storio a gwneud unrhyw ddefnydd o'r data personol, gan gynnwys ei ddatgelu a'i waredu.

7.2 Mae'n ofynnol i ni ddilyn chwe egwyddor mewn perthynas â phrosesu data personol sef:

- Rhaid prosesu data personol mewn modd cyfreithlon, teg a thryloyw.
- Rhaid casglu data personol dim ond at ddibenion penodol, eglur a chyfreithlon, a rhaid i unrhyw ddefnydd arall fod yn unol â'r dibenion hyn
- Rhaid i ddata personol fod yn ddigonol, yn berthnasol ac yn gyfyngedig i'r hyn sy'n angenrheidiol i'r dibenion y caiff ei ddefnyddio
- Rhaid i'r wybodaeth bersonol a gedwir fod yn fanwl gywir a rhaid ei diweddaru, lle bo angen
- Rhaid peidio â chadw data personol yn hirach nag sy'n rhaid
- Rhaid prosesu data personol mewn modd diogel, gan gynnwys sicrhau nad yw data personol yn cael ei ddefnyddio heb awdurdod neu'n anghyfreithlon a gwneud yn siŵr nad yw'n cael ei golli, ei ddinistrio neu ei ddifrodi ar ddamwain, gan ddefnyddio camau technegol a sefydliadol priodol

7.3 Mae'r polisi hwn yn ymwneud yn bennaf â chadw at y chweched egwyddor, fel y nodir uchod.

7.3 Mae'r 'egwyddor atebolrwydd', a bennir yn Erthygl 5 (2) o Reoliad Diogelu Data Cyffredinol y DU hefyd yn ei gwneud yn ofynnol i'r Cyngor gymryd cyfrifoldeb am yr hyn a wnawn gyda data personol a sut rydym yn cydymffurfio â'r chwe egwyddor. Rhaid bod mesurau priodol ar waith i allu dangos cydymffurfiaeth. Felly mae'r polisi hwn yn rhan o gydymffurfiaeth y Cyngor â'r egwyddor hon.

7.4 Os methir â thrin data personol yn gywir gallai olygu y bydd canlyniadau difrifol i'r Cyngor, gan y gellir rhoi cosbau sylweddol am achosion difrifol o dorri rheolau data personol.

8. Cwmpas

8.1 Mae'r polisi yn berthnasol i'r holl ddata personol sy'n eiddo i'r Cyngor.

8.2 Mae'r polisi hwn a'r weithdrefn yn berthnasol i holl weithwyr y Cyngor, gan gynnwys:

- Gweithwyr dros dro a gweithwyr asiantaeth
- Gwirfoddolwyr
- Contractwyr sy'n gweithredu fel proseswyr data

8.3 Hefyd argymhellir bod egwyddorion y polisi hwn yn cael eu mabwysiadu a'u defnyddio gan yr holl Aelodau Etholedig ac ysgolion yr Awdurdod Addysg Lleol.

9. Perchenogion Asedau Gwybodaeth

9.1 Mae **Polisi Diogelwch Gwybodaeth** y Cyngor yn diffinio Perchnogion Asedau Gwybodaeth fel Penaethiaid Gwasanaeth.

10. Cyfrifoldebau

10.1 Mae gweithwyr yn gyfrifol am y canlynol:

- Diogelu'r data personol y maent yn ei brosesu drwy gadw'n llawn at y polisi hwn.

10.2 Mae Rheolwyr a Pherchnogion Asedau Gwybodaeth yn gyfrifol am y canlynol:

- Sicrhau bod eu gweithwyr yn gwybod am y polisi hwn ac yn deall ei ofynion
- Sicrhau bod gofynion y polisi yn cael eu gweithredu'n llawn o fewn eu hadeiniau/timoedd
- Sicrhau bod eu gweithwyr wedi derbyn hyfforddiant priodol ynghylch gofynion Diogelu Data
- Cymryd camau priodol pan fydd y polisi wedi cael ei dorri

Rhan 2

11. Defnyddio dyfeisiau cludadwy a chyfryngau symudadwy

11.1. Mae'r dyfeisiau cludadwy yn cynnwys y canlynol, ond nid y canlynol yn unig:

- Gliniaduron
- Llechi
- Ffonau clyfar

11.2. Mae'r cyfryngau symudadwy yn cynnwys y canlynol, ond nid y canlynol yn unig:

- Cof bach USB/Dyfeisiau storio
- Cardiau SD
- CD-R a DVD-R

11.3 Rhaid peidio â phrosesu data personol ar gyfryngau symudadwy nad ydynt yn eiddo i'r Cyngor.

11.4 Rhaid peidio â phrosesu data personol ar ddyfais bersonol oni bai bod y ddyfais wedi'i chofrestru yng nghynllun Dewch â'ch Dyfais Eich Hun y Cyngor. Os oes gan staff unrhyw amheuon, dylent gysylltu â'r Adran TG i gael cymorth pellach.

11.5. Rhaid defnyddio dyfeisiau cludadwy neu gyfryngau symudadwy i gasglu, storio, cludo neu drosglwyddo data personol dim ond os oes gwir angen gwneud hynny ac nad oes opsiwn arall ar gael.

11.6 Cyn defnyddio dyfeisiau cludadwy neu gyfryngau symudadwy i gasglu, storio, cludo neu drosglwyddo data personol, rhaid cael caniatâd gan y rheolwr perthnasol neu'r Perchennog Asedau Gwybodaeth.

11.7 Rhaid peidio byth â chadw data personol ar gyfryngau symudadwy oni bai ei fod wedi'i amgryptio.

11.8 Rhaid i ddyfeisiau cludadwy neu gyfryngau symudadwy sy'n cynnwys data personol gael eu storio a'u cludo'n ddiogel.

12. Storio a defnyddio data personol yn ddiogel

12.1 Dylid storio a defnyddio data personol ar bapur cyn lleied â phosibl yn unol â datganiad polisi'r Cyngor ar ddefnyddio cymaint â phosibl o ddulliau electronig diogel i storio a throsglwyddo data personol.

12.2 Rhaid i ddata personol gael ei storio bob amser mewn man priodol ar rwydwaith y Cyngor a byth ar ddisg caled y ddyfais. Mae hyn yn diogelu'r data os bydd seiberdroseddu, y cyfrifiadur yn methu neu'n cael ei ddwyn.

12.3 Rhaid peidio â gadael data personol heb neb yn gofalu amdano lle gall unigolion anawdurdodedig gael gafael ynddo, megis ar ddesgiau, siliau ffenestri, coridorau ac argraffwyr/llun-gopïwyr.

12.4 Rhaid peidio â phrosesu data personol ar offer cyfrifiadurol nad ydynt yn eiddo i'r Cyngor.

12.5 Ni ddylid byth â gadael data personol yn weladwy ar sgrin cyfrifiadur pan nad oes neb yno - rhaid i'r defnyddiwr gloi'r cyfrifiadur.

12.6 Wrth ddefnyddio rhaglenni megis Teams i rannu sgrin, rhaid i weithwyr sicrhau nad yw unrhyw ddata personol na fwriedir ei rannu yn weladwy.

12.7 Rhaid peidio byth â llwytho/storio data personol ar gwmwl sydd heb ei ddarparu gan y Cyngor. Mae hyn yn cynnwys y canlynol, ond nid y canlynol yn unig:

- Cyfrifon e-bost personol (megis Gmail, Hotmail)
- Microsoft OneDrive
- WhatsApp
- Dropbox

12.8 Rhaid peidio byth â llwytho data personol i fewnrwyd y Cyngor, cyfryngau cymdeithasol nac unrhyw wefan oni bai am y rhesymau canlynol:

- Gellir gosod y data personol yn gyfreithlon yn y parth cyhoeddus gyda'r bwriad o'i gyhoeddi, er enghraifft, ceisiadau cynllunio neu ddelweddau o bobl sydd wedi cydsynio i hyn
- Mae'r data personol wedi'i gymeradwyo gan uwch-reolwr neu Berchennog Asedau Gwybodaeth i'w gyhoeddi

13. Gweithio gyda data personol allan o'r swyddfa

13.1 Pan fyddwch yn gweithio gartref neu mewn man cyhoeddus, lle mae pobl anawdurdodedig yn bresennol fel teulu neu aelodau o'r cyhoedd, ni ddylid caniatáu iddynt o dan unrhyw amgylchiadau gael mynediad at ddata personol y Cyngor ar unrhyw ffurf. O dan y gofyniad hwn, dylid sicrhau:

- Nad yw data personol yn weladwy i bobl anawdurdodedig ar sgriniau gliniaduron
- Na ellir clywed gwybodaeth am ddata personol, er enghraifft wrth ei drafod ar Teams, unrhyw blatfform cyfathrebu digidol arall, neu dros y ffôn
- Nad yw data personol sydd wedi'i gynnwys mewn unrhyw ddogfennau papur yn hygyrch i bobl anawdurdodedig
- Nad yw dyfeisiau cludadwy'r Cyngor, a ddarperir at ddibenion gwaith yn unig, yn cael eu defnyddio gan bobl anawdurdodedig fel aelodau o'r teulu
- Pan fo gwir angen mynd â dyfeisiau cludadwy neu gyfryngau symudadwy o un lleoliad i'r llall, dylid eu cludo'n ddiogel a pheidio â'u gadael heb oruchwyliaeth

ac yn ddiamddiffyn megis o fewn cerbydau neu mewn ardaloedd y gall y cyhoedd eu gweld.

13.2 Rhaid peidio â mynd â data personol o'r man lle caiff ei storio ar safle'r Cyngor oni bai fod hynny'n gwbl angenrheidiol a dim ond gyda chaniatâd y rheolwr perthnasol neu'r Perchennog Asedau Gwybodaeth.

13.3 Rhaid i gofnodion papur sy'n cynnwys data personol gael eu cludo i gartref gweithiwr dim ond gyda chaniatâd y rheolwr, sydd hefyd yn gyfrifol am sicrhau:

- Bod ffordd o storio papurau fel drôr neu gabinet ar gael y gellir ei gloi yn ddiogel
- Cedwir cofnod o'r wybodaeth sy'n cael ei chymryd oddi ar y safle, pa bryd y cafodd ei chymryd, gan bwy a pha bryd y caiff ei dychwelyd

13.4 Pan fydd gweithwyr yn mynd â data personol ar bapur allan o safle'r Cyngor neu'n ei symud o un lleoliad i'r llall, rhaid iddynt byth ei adael heb oruchwyliaeth lle gallai pobl anawdurdodedig gael mynediad ato fel mewn cerbydau neu fannau cyhoeddus.

13.5 Rhaid cario cofnodion papur sy'n cynnwys data personol yn ddiogel o un lleoliad i'r llall ac ni ddylid fyth eu cludo fel tudalennau rhydd. Rhaid defnyddio cas addas, cwdyn post neu debyg, y gellir ei gau yn ddiogel bob amser. Ni ddylid byth cario papurau fel tudalennau rhydd.

13.6 Rhaid i weithwyr beidio ag argraffu, sganio na llungopïo dogfennau sy'n cynnwys data personol gan ddefnyddio dyfeisiau nad yw'r Cyngor yn berchen arnynt. Mae hyn yn cynnwys dyfeisiau personol yn y cartref a'r rhai sydd ar gael i'w defnyddio mewn safleoedd manwerthu.

13.7 Wrth weithio gartref, er mwyn atal materion yn ymwneud â storio a gwaredu diogel, dylai staff, pan fo'n bosibl beidio â:

- Gwneud nodiadau mewn llawysgrifen sy'n cynnwys data personol
- Creu drafftiau ar bapur sy'n cynnwys data personol

13.8 Rhaid peidio â chadw data personol ar bapur yn y cartref am gyfnod hwy na'r hyn sy'n angenrheidiol a rhaid ei ddychwelyd i safle'r Cyngor cyn gynted ag y bo modd, gan gynnwys i'w waredu.

13.9 Rhaid peidio byth â chael gwared ar ddata personol ar bapur yn y cartref. Rhaid cael gwared ar hwn yn unol ag adran 19 o'r ddogfen hon a **Pholisi Rheoli Cofnodion** y Cyngor.

14. Cyfarfodydd dros y cyfrifiadur

14.1 Pan fydd angen trafod unrhyw ddata personol mewn cyfarfod, rhaid i gyfranogwyr sicrhau nad yw unrhyw berson nad yw wedi'i awdurdodi i gael mynediad i'r data personol yn ei glywed.

14.2 Wrth drefnu cyfarfod rhithwir ar Teams er enghraifft, rhaid i drefnydd y cyfarfod gymryd gofal i sicrhau bod y mynychwyr cywir yn cael eu dewis, er mwyn atal staff, nad ydynt wedi'u hawdurdodi i gael mynediad at unrhyw ddata personol sy'n cael ei drafod, rhag ymuno â'r cyfarfod.

14.3 Rhaid i gyfarfodydd lle trafodir data personol gael eu nodi fel rhai 'Preifat' er mwyn sicrhau na all unrhyw berson anawdurdodedig weld manylion y cyfarfod yn y calendr ac i atal pobl anawdurdodedig rhag ymuno.

15. Trosglwyddo data personol y tu allan i'r Cyngor

15.1 Mae hyn yn cynnwys anfon data personol at y canlynol:

- Awdurdodau lleol eraill
- Adrannau llywodraeth
- Asiantaethau allanol, cwmnïau a sefydliadau
- Unigolion - ein cwsmeriaid a'n cleientiaid

15.2 Rhaid peidio ag anfon data personol y tu allan i'r Cyngor oni bai fod hynny'n angenrheidiol a bod hynny'n unol â'r gyfraith.

15.3 Rhaid peidio â darparu data personol i unrhyw sefydliad allanol os gellid defnyddio gwybodaeth heb enwau, dan ffugenw neu wybodaeth ystadegol fel dewis arall.

15.4 Rhaid i unrhyw ddata personol a ddarperir fod yn berthnasol ac ni ddylai fod yn fwy na'r hyn sy'n gwbl angenrheidiol at bwrpas penodol a chyfreithlon.

16. Defnyddio dull electronig i drosglwyddo gwybodaeth

16.1 Y ffordd fwyaf diogel, cyflymaf a chost effeithiol o drosglwyddo data personol y tu allan i'r Cyngor yw trwy ddull electronig diogel. Rhaid ystyried hyn fel y dewis cyntaf bob amser a'i ddefnyddio lle bynnag y gellir. Pan fydd porth neu blatfform rhannu ffeiliau ar gael, rhaid defnyddio hwn yn hytrach nag anfon data personol trwy e-bost.

16.2 Mae'r Cyngor yn defnyddio Diogelwch Haen Cludo (TLS) i ddiogelu negeseuon e-bost a anfonir at sefydliadau'r sector cyhoeddus. Dyma ddull diogel felly o drosglwyddo data personol pan fo angen.

16.3 Cyhoeddir y canllawiau ar gyfer diogelu cyfeiriadau e-bost gan TLS gan y Cyngor ar ei Fewnrwyd, sy'n cael eu diweddaru pan fo angen ac y gellir eu cyrchu trwy'r dudalen Diogelwch TG.

16.4 Nid yw TLS yn diogelu cynnwys e-bost a anfonir at unrhyw dderbynwyr sector preifat, sy'n cynnwys ein cwsmeriaid a'n cleientiaid. Felly, ar gyfer yr holl dderbynwyr o'r fath, mae dulliau diogel yn cynnwys, ond heb fod yn gyfyngedig i:

- E-bost wedi'i amgryptio Office 365
- ShareFile y Cyngor

16.5 Pan fo'r cynnwys yn sensitif iawn, dylid ystyried defnyddio cyfrinair i ddiogelu dogfennau sydd ynghlwm wrth e-byst er mwyn gwneud yn siŵr nad oes neb yn gallu cyrchu'r data personol os caiff ei anfon at y derbynnydd anghywir a hefyd tra bydd derbynnydd bwriadedig yn ei gadw. Pan fyddwch yn diogelu dogfennau gyda chyfrinair, mae'n bwysig i:

- Ddarparu'r cyfrinair trwy e-bost ar wahân, neu trwy ddull gwahanol, fel galwad ffôn
- Gofyn am gadarnhad eich bod wedi derbyn yr e-bost cyntaf sy'n cynnwys y cyfrinair cyn anfon yr ail e-bost yn atodi dogfen
- Sicrhau mai dim ond y copi sy'n cael ei anfon sydd wedi'i ddiogelu gan gyfrinair ac nad yw mynediad i'r gwreiddiol a gedwir ar rwydwaith neu system y Cyngor wedi'i gyfyngu fel hyn

16.6 Wrth ddefnyddio e-bost, dylid osgoi anfon at grwpiau neu restri o gysylltiadau gan fod hynny'n golygu bod perygl y gellid datgelu data personol i dderbynwyr sydd heb yr awdurdod i gael mynediad i'r wybodaeth honno.

16.7 Rhaid cymryd yr un gofal wrth ateb e-bost, oherwydd trwy ddewis ‘Ateb i bawb’ (reply to all) gallai hynny arwain at anfon gwybodaeth at dderbynwyr nas bwriedir ac sydd heb awdurdod i dderbyn y wybodaeth honno.

16.8 Wrth anfon e-bost at nifer o dderbynwyr, rhaid nodi unrhyw gyfeiriadau e-bost personol yn y maes *Blind Carbon Copy* neu ‘Bcc’ o fewn y neges yn hytrach nag yn ‘To’. Bydd hyn yn cuddio cyfeiriadau e-bost preifat unigolion ac yn eu hatal rhag cael eu gweld gan y derbynwyr eraill.

16.9 Wrth ddechrau teipio cyfeiriad e-bost, bydd y feddalwedd e-bost yn awgrymu amryw o gyfeiriadau tebyg a ddefnyddiwyd eisoes. Mae'n hanfodol bod y cyfeiriad cywir yn cael ei ddewis cyn anfon y neges. **Cyfrifoldeb yr anfonwr yw gwirio sawl gwaith fod y cyfeiriad cywir wedi'i nodi neu ei ddewis cyn anfon yr e-bost. Ni ellir gor-bwysleisio pa mor bwysig yw hyn - mae llawer o achosion o dorri rheolau data personol yn digwydd yn sgil anfon e-bost at y derbynnydd anghywir.**

16.10 Rhaid bod yn ofalus hefyd wrth anfon dilyniant o negeseuon e-bost. Efallai na fydd derbynwyr y neges ddiweddaraf wedi’u hawdurdodi i weld cynnwys e-byst cynharach ymhellach i lawr y dilyniant.

16.11 Rhaid cynnwys cyfarwyddiadau clir ynghylch y modd y dylai'r derbynnydd drin y wybodaeth, er enghraifft, os na ddylid anfon y wybodaeth ymlaen heb gysylltu â'r anfonwr yn gyntaf.

16.12 Pan nad oes dull electronig diogel ar gael ac nad yw'r wybodaeth yn ddata personol o gategori arbennig, neu fel arall yn debygol o achosi niwed neu ofid os caiff ei datgelu i drydydd parti, yna gellir ei hanfon drwy e-bost safonol. Enghraifft o hyn

fyddai ateb gohebiaeth unigolyn ynghylch mater sydd eisoes yn wybodaeth gyhoeddus. Er hynny, rhaid cymryd gofal i sicrhau bod y wybodaeth yn cael ei hanfon i'r cyfeiriad e-bost cywir.

16.13 Mae pob defnydd a wneir o'r e-bost yn cael ei reoli gan **Bolisi'r Cyngor ar gyfer defnyddio'r E-bost a'i Fonitro**.

17. Defnyddio dulliau eraill i drosglwyddo data personol

17.1 Mae dulliau eraill o drosglwyddo data personol yn cynnwys y canlynol, ond nid y canlynol yn unig:

- Y Post Brenhinol
- Negesydd
- Dosbarthu/casglu â llaw o safleoedd y Cyngor

17.2 Pan nad oes dull electronig diogel ar gael ac nad yw'r wybodaeth yn ddata personol o gategori arbennig, yna gellir ei hanfon drwy'r Post Brenhinol heb angen unrhyw asesiad pellach o risg. Enghraifft o hyn fyddai llythyr yn rhoi gwybod i berson ei fod wedi bod yn llwyddiannus yn ei gais am swydd. Hefyd mae angen inni fel mater o drefn anfon llythyrau sy'n cynnwys gwybodaeth bersonol at ein cwsmeriaid, er enghraifft, mewn perthynas â hawliadau am fudd-daliadau. Er hynny, rhaid cymryd gofal i sicrhau bod y wybodaeth yn cael ei hanfon i'r cyfeiriad cywir at dderbynnydd a enwir.

17.3 Os nad oes dull electronig diogel a bod y wybodaeth sydd i'w hanfon yn ddata personol o gategori arbennig, yna rhaid ystyried y canlynol bob amser wrth benderfynu pa ddull trosglwyddo sy'n briodol:

- Union natur y wybodaeth, pa mor sensitif, cyfrinachol neu werthfawr ydyw
- Pa ddifrod neu ofid a allai gael ei achosi i unigolion pe bai'r wybodaeth yn cael ei cholli neu ei chyrchu gan bobl anawdurdodedig
- Yr effaith y byddai unrhyw golled yn ei chael ar y Cyngor
- I ba raddau mae angen darparu'r wybodaeth ar fyrder, gan gymryd i ystyriaeth effaith peidio ag anfon y data, neu unrhyw oedi o ran anfon y data

17.4 Os bernir ei bod yn briodol anfon gwybodaeth bersonol o gategori arbennig drwy'r Post Brenhinol, rhaid dilyn y camau canlynol:

- Rhaid i'r amlen yr anfonir y wybodaeth ynddi fod â chyfeiriad wedi'i nodi'n glir arni at dderbynnydd a enwir
- Rhaid anfon y wybodaeth drwy ddull y gellir ei olrhain

17.5 Pan ddefnyddir negesydd i gludo unrhyw data personol, rhaid cymryd camau priodol i sicrhau bod y negesydd yn gweithredu o fewn safonau diogeledd priodol.

17.6 Os bernir nad yw'n briodol trosglwyddo data personol drwy'r Post Brenhinol neu negesydd ac os na ellir defnyddio dull electronig diogel, dylid darparu'r wybodaeth â

llaw i'r derbynnydd, neu dylid trefnu i'r data gael ei gasglu a chadw cofnod sy'n cynnwys:

- Disgrifiad byr o'r wybodaeth a ddarparwyd
- Y dyddiad y cafodd ei darparu
- Enw a manylion cyswllt y derbynnydd, ac os yw'n berthnasol, ei swydd

17.7 Pan fydd dogfennau'n cael eu rhyddhau i unigolion, dylai'r dogfennau hynny sy'n cynnwys data personol fod â dyfrnod sy'n nodi “Copi wedi'i ryddhau".

18. Gwirio gwybodaeth cyn ei hanfon

18.1 Pan fydd data personol o gategori arbennig, neu data personol a fyddai fel arall yn debygol o achosi niwed neu ofid os yw'n cael ei datgelu i drydydd parti, yn cael ei hanfon y tu allan i'r Cyngor mewn unrhyw fformat, dylai'r anfonwr ystyried cael rhywun arall i wirio'r wybodaeth cyn ei hanfon.

18.2 Mae'r unigolyn sy'n anfon y wybodaeth yn gyfrifol am y canlynol:

- Sicrhau bod y cyfeiriad e-bost neu bost yr anfonir y wybodaeth iddo yn gywir
- Sicrhau pan ddarperir gwybodaeth ar ffurf copi caled, bod y derbynnydd a enwir sy'n mynd i dderbyn y wybodaeth yn cael ei nodi'n glir
- Sicrhau nad oes dim gwybodaeth mewn perthynas â thrydydd parti wedi cael ei chynnwys mewn camgymeriad, naill ai mewn llythyr/e-bost neu ddogfen atodedig

18.3 Os bernir ei bod yn angenrheidiol i unigolyn arall wirio'r wybodaeth, mae'r unigolyn arall yn gyfrifol am y canlynol:

- Gwirio bod y cyfeiriad e-bost neu bost yr anfonir y wybodaeth iddo yn gywir
- Pan ddarperir gwybodaeth ar ffurf copi caled, gwirio bod enw cywir y derbynnydd a enwir sy'n mynd i dderbyn y wybodaeth wedi cael ei nodi
- Gwirio nad oes dim gwybodaeth mewn perthynas â thrydydd parti wedi cael ei chynnwys mewn camgymeriad, naill ai mewn llythyr/e-bost neu ddogfen atodedig
- Cofnodi eu bod wedi gwirio'r e-bost, y llythyr neu/ac yr atodiadau

19. Trosglwyddo gwybodaeth bersonol yn ddiogel o fewn y Cyngor

19.1 Rhaid peidio â throsglwyddo data personol o fewn y Cyngor oni bai fod hynny'n gwbl angenrheidiol. Lle bo hynny'n bosibl ac yn briodol, dylid cael mynediad i ddata personol drwy rwydwaith y Cyngor

19.2 Rhaid peidio â symud data personol o un adran i un arall pan fyddai gwybodaeth heb enwau, dan ffugenw neu wybodaeth ystadegol yn ddigonol. Rhaid i unrhyw wybodaeth a drosglwyddir fod yn berthnasol ac ni ddylai fod yn fwy na'r hyn sy'n gwbl angenrheidiol at bwrpas penodol a chyfreithlon.

19.3 Mae'r angen gwirioneddol i drosglwyddo data personol ar bapur o fewn y Cyngor yn gyfyngedig, o gofio'r dewisiadau amgen mwy diogel, haws a chyflymach sydd ar gael. Fodd bynnag, pan fydd angen trosglwyddo dogfennau papur sy'n cynnwys data personol, rhaid eu darparu bob amser mewn amlen wedi'i selio wedi'i chyfeirio at dderbynnydd a enwir. Lle bo angen darparu gwaith papur sylweddol, er enghraifft un ffeil neu fwy, rhaid defnyddio amlen ddiogel, gadarn.

19.4 Os bernir ei bod yn amhriodol i unrhyw un arall heblaw'r derbynnydd a fwriedir weld y wybodaeth bersonol sydd yn y ddogfen, rhaid nodi'r geiriau 'Cyfrinachol - derbynnydd yn unig' ar yr amlen.

20. Cadw gwybodaeth bersonol

20.1 Pan nad oes angen cadw data personol ar ddyfeisiau cludadwy neu gyfryngau symudadwy bellach, dylid ei ddileu ar unwaith.

20.2 Os defnyddir dyfais gludadwy i gasglu data personol, ni ddylid cadw'r wybodaeth arni ond cyhyd ag sy'n gwbl angenrheidiol. Dylid cadw'r wybodaeth ar rwydwaith y Cyngor cyn gynted ag y bo modd a'i dileu oddi ar y ddyfais.

20.3 Ym mhob achos arall, os penderfynir nad oes angen cadw gwybodaeth bersonol bellach, rhaid cyfeirio at **Ganllawiau'r Cyngor ar gyfer Cadw Gwybodaeth** cyn dileu neu ddifetha cofnodion.

20.4 Rhaid cael gwared â chofnodion papur sy'n cynnwys gwybodaeth bersonol mewn modd diogel, drwy eu rhwygo'n fân neu drwy ddefnyddio'r gwasanaeth gwastraff cyfrinachol yn unol â **Pholisi Rheoli Cofnodion y Cyngor.**

20.5 Gwasanaethau TG y Cyngor yn unig sydd â'r hawl i waredu offer TG a hynny'n unol â **Pholisi Diogelwch Gwybodaeth** y Cyngor.

Rhan 3

21. Torri rheolau data personol

21.1 Byddai'r rhain yn cynnwys achosion lle mae data personol, ar ffurf electronig neu ar bapur, yn cael ei golli neu ei ddwyn. Byddai'r enghreifftiau eraill yn cynnwys e-bostio data personol at dderbynnydd nas bwriedir neu osod data personol ar wefan y Cyngor yn ddamweiniol.

21.2 Mae'r Ddeddfwriaeth Diogelu Data yn gorfodi'r Cyngor i gofnodi pob achos o dorri rheolau sy'n ymwneud â Data Personol; i bob pwrpas, i gadw cofrestr fewnol o bob achos o'r fath.

21.3 Hefyd mae'n ofynnol i'r Cyngor riportio i Swyddfa'r Comisiynydd Gwybodaeth (ICO) achosion o dorri rheolau sy'n debygol o arwain at beryglu *"hawliau a rhyddid"* unigolion a rhoi gwybod, mewn achosion penodol, i'r unigolion yr effeithiwyd ar eu data personol.

21.4 Dyma ddiffiniad o achos o dorri rheolau data, fel y'i defnyddir yn y polisi hwn:

"achos o dramgwyddo diogelwch sy'n arwain at ddinistrio, colli, newid, datgelu neu roi mynediad i ddata personol heb ganiatâd, boed yn ddata personol a drosglwyddir, a gedwir neu a brosesir."

Mae'r rhan hon o'r polisi felly'n cwmpasu achosion o beryglu cyfrinachedd, cywirdeb ac argaeledd data personol, ym mha ffurf bynnag.

21.5 Dyma enghreifftiau o achosion o dorri rheolau data:

- Colli neu ladrata offer TGCh megis gliniaduron, llechi, ffonau clyfar neu gof bach USB sy'n cynnwys data personol
- Colli neu ladrata cofnodion papur megis ffeiliau, dogfennau unigol neu lyfrau nodiadau sy'n cynnwys data personol
- Colli neu ladrata gwybodaeth ariannol megis cyfrif banc neu fanylion cerdyn banc
- Datgelu gwybodaeth yn ddamweiniol megis drwy anfon neges e-bost neu lythyr sy'n cynnwys data personol at y bobl anghywir
- Dileu cofnodion yn ddamweiniol gan effeithio ar y gwaith o ddarparu gwasanaethau ac o bosibl ar lesiant unigolion
- Cael mynediad heb ganiatâd i systemau TG; ymosodiadau seiber a meddalwedd wystlo

22. Riportio achosion

22.1 Mae achosion yn fwy tebygol o ddod i'r amlwg o ganlyniad i'r canlynol:

- Cŵyn neu sylw gan aelod o'r cyhoedd neu gan rywun o sefydliad allanol

- Achos a riportir i'r ddesg gymorth TG
- Staff yn sylwi ar broblem wrth gyflawni eu dyletswyddau
- Prosesydd data yn rhoi gwybod i'r Cyngor am ddigwyddiad

22.2 Mae'n rhaid reportio pob achos o dorri rheolau yn unol â'r polisi hwn, beth bynnag fo natur y digwyddiad.

22.3 Er mwyn sicrhau y gellir cymryd camau i unioni achosion o dorri rheolau data, dylai gweithwyr riportio achos i'w rheolwr llinell ar unwaith. Mae'n rhaid riportio'r achos i'r Tîm Ymateb i Achos o Dorri Rheolau Data drwy gyfeiriad e-bost canolog:

databreaches@sirgar.gov.uk

22.4 Y tu allan i oriau swyddfa, mae'n rhaid riportio achosion trwy Llesiant Delta (0300 333 2222).

22.5 Caiff yr ymateb i achosion ei gydlynu gan y Tîm Ymateb i Achos o Dorri Rheolau, sy'n cynnwys:

- Rheolwr Cwynion a Llywodraethu Gwybodaeth (DPO)
- Swyddog Diogelwch Digidol
- Rheolwr – Systemau Gwybodaeth a Diogelwch

22.6 Gan ddibynnu ar natur yr achos o dorri rheolau data, bydd un neu ragor o'r swyddogion hyn yn arwain ar gydlynu'r ymateb.

23. Y Weithdrefn ar gyfer ymateb i achosion

23.1 Bydd yr ymateb i achos yn dilyn y camau canlynol:

- Rheoli ac adfer
- Asesu'r risg
- Rhoi gwybod am yr achos (lle bo angen)
- Gwerthuso ac ymateb

23.2 Ar ôl cael gwybod am achos o dorri rheolau, bydd y Tîm Ymateb i achos o Dorri Rheolau yn hysbysu'r rheolwr perthnasol a fydd wedyn yn dechrau dogfennu'r achos gan ddefnyddio'r **templed Adroddiad Achos** safonol.

23.3 Bydd manylion yr achos hefyd yn cael eu nodi ar gofrestr torri rheolau data personol a gadwir gan y DPO a bydd rhif digwyddiad unigryw yn cael ei greu.

23.3 Lle credir bod yr achos yn ymwneud â gwybodaeth ariannol megis manylion cyfrif banc, gwybodaeth am berchennog cerdyn talu neu system sy'n ymwneud â Diwydiant y Cardiau Talu (PCI), rhaid i'r Tîm Ymateb i Achos o Dorri Rheolau Data weithredu **Cynllun Ymateb i Achos - y PCI** (wedi'i atodi ar ffurf **Atodiad 1**) a hynny ar unwaith.

23.4 Bydd y rheolwr yn gyfrifol am gychwyn ymchwiliad ar unwaith i achos(ion) yr achos o dorri rheolau ac am nodi a gweithredu'r camau rheoli ac adfer angenrheidiol. Rhaid i'r rhain gael eu cofnodi'n glir yn yr Adroddiad Achos. Dyma rai enghreifftiau o gamau o'r fath:

- Ceisio dod o hyd i gofnodion papur a fu ar goll, a'u dwyn yn eu hôl
- Dod o hyd i eitem o gyfarpar TGCh a fu ar goll
- Sicrhau bod neges e-bost a anfonwyd i'r cyfeiriad anghywir wedi cael ei dileu
- Rhoi gwybod i'r heddlu os oes lladrad wedi bod
- Newid y côd mynediad i ddrysau

23.5 Bydd y rheolwr yn cynnal asesiad o'r risg(iau) yn sgil yr achos ac yn cofnodi'r rhain yn yr Adroddiad Achos. Rhaid i'r asesiad ystyried y canlynol:

- Y math o ddata sydd dan sylw – ei natur, ei faint a pha mor sensitif ydyw
- A allai gwrthrych y data gael ei niweidio gan yr achos, er enghraifft, risg corfforol, dwyn hunaniaeth, twyll neu beri niwed i enw da
- Pwy yw'r unigolion, er enghraifft, plant neu bobl fregus eraill megis cleientiaid gofal cymdeithasol
- Nifer y gwrthrychau data yr effeithiwyd arnynt

23.6 Dylid ymgynghori â'r DPO ynghylch asesu risg a gellir defnyddio offeryn a chanllawiau **hunanasesu'r** ICO i gynorthwyo gyda hyn.

23.7 Unwaith y bydd y camau hyn wedi cael eu cwblhau a'u cofnodi, dychwelir yr Adroddiad Achos i'r Tîm Ymateb i Achos o Dorri Rheolau Data a'i atgyfeirio at yr Uwch-berchennog Risg Gwybodaeth (SIRO) neu yn ei absenoldeb, y Dirprwy Uwch-berchennog Risg Gwybodaeth a Pennaeth y Gwasanaeth fel IAO

23.8 Wedyn bydd y SIRO neu'r Dirprwy SIRO yn penderfynu a oes angen rhoi gwybod i Swyddfa'r Comisiynydd Gwybodaeth am yr achos, gan ystyried y sefyllfa fel y'i cofnodwyd. A bwrw bod angen rhoi gwybod, bydd y Tîm Ymateb i Achos o Dorri Rheolau Data yn rhoi'r holl wybodaeth sy'n ofynnol o dan y ddeddfwriaeth Diogelu Data i Swyddfa'r Comisiynydd Gwybodaeth.

23.9 Ar sail yr asesiad risg, bydd Pennaeth y Gwasanaeth, gan ymgynghori â'r Rheolwr a'r Tîm Ymateb i Achos o Dorri Rheolau Data, yn penderfynu a oes angen rhoi gwybod i wrthrych(au) y data yr effeithiwyd arno/arnynt gan yr achos. Lle ystyrir bod hynny'n angenrheidiol, rhaid darparu'r wybodaeth sydd i'w chyfleu i'r gwrthrych yn llawn, yn unol â'r ddeddfwriaeth Diogelu Data.

23.10 Rhaid cwblhau'r camau a nodir rhwng 20.1 a 20.8 uchod o fewn pum diwrnod gwaith.

23.11 Yn olaf, bydd y Tîm Ymateb i Achos o Dorri Rheolau Data, gan ymgynghori â'r Rheolwr, yn nodi ac yn cofnodi unrhyw argymhellion neu gamau pellach. Er enghraifft, os achoswyd yr achos gan broblemau systemig a pharhaus, efallai y bydd angen cymryd camau fel y rhai canlynol:

- Newid gweithdrefnau a systemau
- Adolygu polisïau
- Hyfforddiant/ymwybyddiaeth i'r staff

23.12 Rhaid darparu copi o'r Adroddiad am achos o Dorri Rheolau wedi'i gwblhau i'r Cyfarwyddwr perthnasol bob amser.

23.13 Bydd y gofrestr o dorri rheolau data personol ar gael i aelodau'r Grŵp Llywodraethu Gwybodaeth Gorfforaethol a fydd hefyd yn ystyried torri rheolau data personol fel eitem sefydlog ar yr agenda.

24. Polisïau neu weithdrefnau eraill

24.1 Lle bydd achos o dorri data personol yn gofyn am uwchgyfeirio achos ymhellach oherwydd amgylchiadau'r achos, bydd y SIRO yn penderfynu a ddylid bwrw ymlaen ag ymchwiliad ffurfiol o dan **Bolisi Ymchwiliadau**'r Cyngor.

24.2 Lle bydd achos o dorri rheolau data yn rhoi bod i gŵyn, darperir ymateb i'r achwynydd yn unol â **Pholisi Cwynion y Cyngor**.

24.3 Lle ystyrir bod achos a riportir hefyd yn mynd yn groes i unrhyw un o bolisïau eraill y Cyngor, bydd gofynion y polisi perthnasol yn cael eu dilyn, a allai gynnwys cymryd camau disgyblu.

Rhan 4

25. 6. Datganiad cydraddoldebau

25.1 Rhaid i bob gweithiwr fabwysiadu agwedd gadarnhaol, agored a theg a gofalu y cedwir at **Bolisi Cydraddoldeb ac Amrywiaeth** yr Awdurdod ac y caiff ei weithredu'n gyson heb ystyried hil, lliw, cenedligrwydd, gwreiddiau ethnig neu genedlaethol, anabledd, crefydd a chred neu ddiffyg cred, oed, rhyw, ailbennu rhywedd, hunaniaeth rhywedd a mynegiant rhywedd, cyfeiriadedd rhywiol, beichiogrwydd neu famolaeth, statws priodasol neu bartneriaeth sifil.

25.2 Yn ogystal, mae Safonau'r Gymraeg yn gofyn i ni 'sicrhau nad yw'r iaith yn cael ei thrin yn llai ffafriol na'r Saesneg' a dylid defnyddio'r egwyddor hon wrth gymhwyso'r polisi hwn.

Os oes angen y ddogfen hon arnoch mewn fformat arall, e-bostiwch **diogeludata@sirgar.gov.uk**

Cymeradwywyd y polisi gan y Bwrdd Gweithredol ar: 13/09/2021
Dyddiad Adolygu'r Polisi: Medi/Hydref 2023

Atodiad 1

Cynllun Ymateb i Achos - y PCI

Mewn ymateb i achos posibl o dorri rheolau data sy'n ymwneud â Safon Diogelwch Data (taliadau â cherdyn) y PCI, bydd y Tîm Ymateb i Achos o Dorri Rheolau Data yn cysylltu ar unwaith â Swyddog Rheoli Trysorlys y Cyngor neu â Phennaeth y Gwasanaethau Ariannol a fydd yn gorfod gwneud y canlynol:

- Sicrhau bod unrhyw systemau sydd wedi'u peryglu yn cael eu hynysu oddi wrth y rhwydwaith;

- Casglu, adolygu a dadansoddi cofnodion a gwybodaeth gysylltiedig o systemau diogelu a mesurau diogelwch amrywiol, yn ganolog a lleol.

- Dadansoddi'n fforensig unrhyw systemau sydd wedi'u peryglu;

- Cysylltu â'r adrannau a'r cyrff perthnasol, yn fewnol ac yn allanol;

- Cysylltu â'r Heddlu a/neu swyddogion diogelwch perthnasol y diwydiant cardiau, a darparu cofnodion a manylion fforensig iddynt yn ôl yr angen;

- Cynorthwyo'r Heddlu a swyddogion diogelwch perthnasol y diwydiant cardiau gyda'r broses ymchwilio, gan gynnwys erlyniadau;

- Cysylltu â'r cwmni cardiau perthnasol a chyflawni gofynion penodol y cwmni wrth riportio achosion tybiedig neu sicr o ryddhau data deiliaid cardiau talu.