

CYNGOR SIR YNYS MÔN / ISLE OF ANGLESEY COUNTY COUNCIL

Cyfarfod:	Pwyllgor Llywodraethu ac Archwilio
Dyddiad:	8 Chwefror 2024
Teitl yr Adroddiad:	Llywodraethu Gwybodaeth – Adroddiad Blynyddol yr Uwch Berchennog Risg Gwybodaeth (SIRO) ar gyfer y cyfnod 1 Ebrill 2022 – 31 Mawrth 2023
Pwrpas yr Adroddiad:	Hysbysu Aelodau am Lefel y Gydymffurfiaeth a'r Risg
Adroddiad gan:	SIRO/Swyddog Monitro Est. 2586 lynnball@ynysmon.llyw.cymru
Swyddog Cyswllt:	SIRO/Swyddog Monitro Est. 2586 lynnball@ynysmon.llyw.cymru

Pwrpas yr adroddiad hwn

Rhannu'r materion Llywodraethu Gwybodaeth (LIG) allweddol ar gyfer y cyfnod 1 Ebrill 2022 hyd at 31 Mawrth 2023 a chrynhofi'r risgiau Llywodraethu Gwybodaeth cyfredol.

1.0 Cyflwyniad

Mae'r adroddiad hwn yn darparu datganiad a throsolwg yr Uwch Berchennog Risg Gwybodaeth o sut mae'r Cyngor yn cydymffurfio â gofynion cyfreithiol ar gyfer trin gwybodaeth gorfforaethol, gan gynnwys cydymffurfio â Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (GDPR y DU); Deddf Diogelu Data 2018; Deddf Rhyddid Gwybodaeth 2000; Deddf Rheoleiddio Pwerau Ymchwilio 2000 (Gwylidwriaeth) a chodau ymarfer perthnasol.

Mae'r adroddiad yn darparu gwybodaeth am gyswllt y Cyngor â rheoleiddwyr allanol ac mae'n darparu gwybodaeth hefyd am ddigwyddiadau diogelwch, achosion o dorri cyfrinachedd, neu "ddigwyddiadau ond y dim" yn ystod y cyfnod.

Rhoddir data allweddol am weithdrefnau llywodraethu gwybodaeth yn y Cyngor yn Atodiadau 1 - 7 isod.

2.0 Datganiad yr Uwch Berchennog Risg Gwybodaeth

Fel Uwch Berchennog Risg Gwybodaeth rwyf yn gwneud yr argymhellion canlynol:

- i. bod adroddiad yr Uwch Berchennog Risg Gwybodaeth yn cael ei dderbyn fel adlewyrchiad cywir o faterion Llywodraethu Gwybodaeth y Cyngor ar gyfer y cyfnod perthnasol;
- ii. bod y Pwyllgor yn caniatáu i'r Uwch Berchennog Risg Gwybodaeth ofyn i'r Tîm Arweinyddiaeth i:-
 - (i) asesu defnydd y Cyngor o TCC a'i ddefnydd, os o gwbl, o dechnoleg dronau;

- (ii) asesu'r risgiau diogelu data yn gysylltiedig â gweithio mewn partneriaeth, ynghyd â'r bygythiadau seiber yn gysylltiedig â rheoli contractau / caffael o fewn y Cyngor;
- (iii) rhoi trefniadau ar waith i sicrhau bod y Tîm Arweinyddiaeth yn derbyn gwybodaeth ddigonol fel eu bod yn ymwybodol o'r bygythiadau seiber sy'n wynebu'r Cyngor a'r mesurau lliniaru.

Atodiad 1. Nifer y digwyddiadau diogelwch data a gofnodwyd gan y Cyngor yn ystod y flwyddyn.

Digwyddiadau diogelwch data (22/23): 22 digwyddiad

Digwyddiadau Lefel 0 – Lefel 1 (digwyddiadau “ond y dim” neu ddigwyddiadau a gadarnhawyd fel digwyddiadau diogelwch data ond **nad oes** angen rhoi gwybod amdanynt i Swyddfa'r Comisiynydd Gwybodaeth a rheoleiddwyr eraill) = 21

Digwyddiadau Lefel 2 (digwyddiadau diogelwch data y mae'n **rhaidd** rhoi gwybod amdanynt i Swyddfa'r Comisiynydd Gwybodaeth oherwydd y risg sy'n gysylltiedig â'r digwyddiadau) = 1

Categori Lefel 0 -1	Nifer
Datgelu trwy gamgymeriad	19
Colli data / caledwedd	2
Datgelu heb awdurdod	0
Colli wrth gael eu cludo	0
Arall	0
Categori 2	Nifer
Datgelu trwy gamgymeriad	0
Datgelu heb awdurdod	1
Methiant technegol	0
Arall	0

Atodiad 2. Camau a gytunwyd yn dilyn digwyddiadau diogelwch data.

Camau Gweithredu

Yn dilyn achos o ddatgelu heb awdurdod pan gafodd llun o lythyr cyfrinachol gan yr ysbyty at ddefnyddiwr gwasanaeth ei atodi i neges e-bost ar gyfer Grŵp defnyddwyr mewnol nodwyd a chytunwyd ar dri cham gweithredu er mwyn lleihau'r tebygolrwydd o ddigwyddiad tebyg.

Atodiad 3. Digwyddiadau diogelwch data y rhoddwyd gwybod i'r Swyddfa'r Comisiynydd Gwybodaeth yn eu cylch.

- 1.0 Rhoddwyd gwybod i Swyddfa'r Comisiynydd Gwybodaeth am ddigwyddiad diogelwch data ym mis Medi 2022 wedi i lythyr cyfrinachol gan yr ysbyty at ddefnyddiwr gwasanaeth ei ddatgelu heb ganiatâd. Ni ofynnwyd i'r Cyngor gymryd unrhyw gamau pellach gan Swyddfa'r Comisiynydd Gwybodaeth.

2.0 Yn dilyn proses ymchwilio a gymerodd dros 20 mis i'w chwblhau, rhoddodd Swyddfa'r Comisiynydd Gwybodaeth adborth ar ddigwyddiad diogelwch data a adroddwyd yn ôl ym mis Mehefin 2021, ac a oedd yn ymwneud â diogelwch gweinyddion 5 ysgol uwchradd. Daeth y Cyngor i wybod am y digwyddiad wedi iddo sylwi ar lif traffig amheus drwy'r SMTP (protocol trosglwyddo post syml h.y. gweithgaredd e-bost amheus) ar rwydwaith yr ysgolion uwchradd. Roedd y gweinyddion a'r seilwaith TG wedi cael eu datblygu gan drydydd parti ar ran yr ysgolion a oedd hefyd yn gyfrifol am eu cynnal a'u cadw.

Ar ôl methu â dod o hyd i'r rheswm dros y gweithgarwch amheus, penderfynwyd rhoi peiriannau rhithiol ac unrhyw ddyfeisiadau rhwydwaith a chyfrifon defnyddwyr y 5 ysgol uwchradd a allai fod dan fygythiad mewn cwarantîn. Cyflwynwyd adroddiad i Swyddfa'r Comisiynydd Gwybodaeth gan Swyddog Diogelu Data'r Cyngor, ac yna gan yr ysgolion fel rheolyddion y data. Cynhaliwyd ymchwiliad gan *NCC Group*, sef y prif sefydliad ymgynghorol ar fygythiadau seiber yn y DU a sefydlwyd Tîm Rheoli Digwyddiad gan y Cyngor.

Yn ystod yr ymchwiliad canfuwyd bod y systemau'n cynnwys nifer o wendidau hysbys, ac felly roeddent yn agored i ymosodiadau. Daeth *NCC Group* o hyd i nifer o faterion yn gysylltiedig â chyflwr gwael yr ystâd yn gyffredinol o ran diogelwch. Canfuwyd bod systemau allweddol yn dal i gael eu defnyddio heb eu cefnogi wedi iddynt gyrraedd diwedd eu hoes, Systemau Gweithredu etifeddol. Bu i *NCC Group* hefyd nodi bod diffyg cofnodi ar draws yr ystâd wedi effeithio'n sylweddol ar eu hymchwiliad.

Er bod yr ymchwiliad wedi dod i'r casgliad nad oedd unrhyw dystiolaeth o ymosodiad, roedd nifer o elfennau cydymffurfiaeth allweddol ar goll ac roedd Swyddfa'r Comisiynydd Gwybodaeth yn gefnogol o'r cynllun gweithredu a gafodd ei ddatblygu a'i weithredu gan y Cyngor i sicrhau bod modd i ysgolion brosesu data personol yn ddiogel ac yn unol â deddfwriaeth diogelu data'r DU.

Yn sgil y camau adferol a gymerwyd gan y Cyngor er mwyn diogelu systemau digidol a phrosesau llywodraethu gwybodaeth yr ysgolion llwyddwyd i wella diogelwch a chydymffurfiaeth yn sylweddol ac ar unwaith ac o ganlyniad i hyn, yn fwy na dim byd arall, ni chymerodd Swyddfa'r Comisiynydd Gwybodaeth unrhyw gamau pellach yn erbyn y Cyngor a'r ysgolion. Mae'r elfennau diogelu data o'r gwaith hwn yn parhau i fod ar y gweill gan y Gwasanaeth Dysgu.

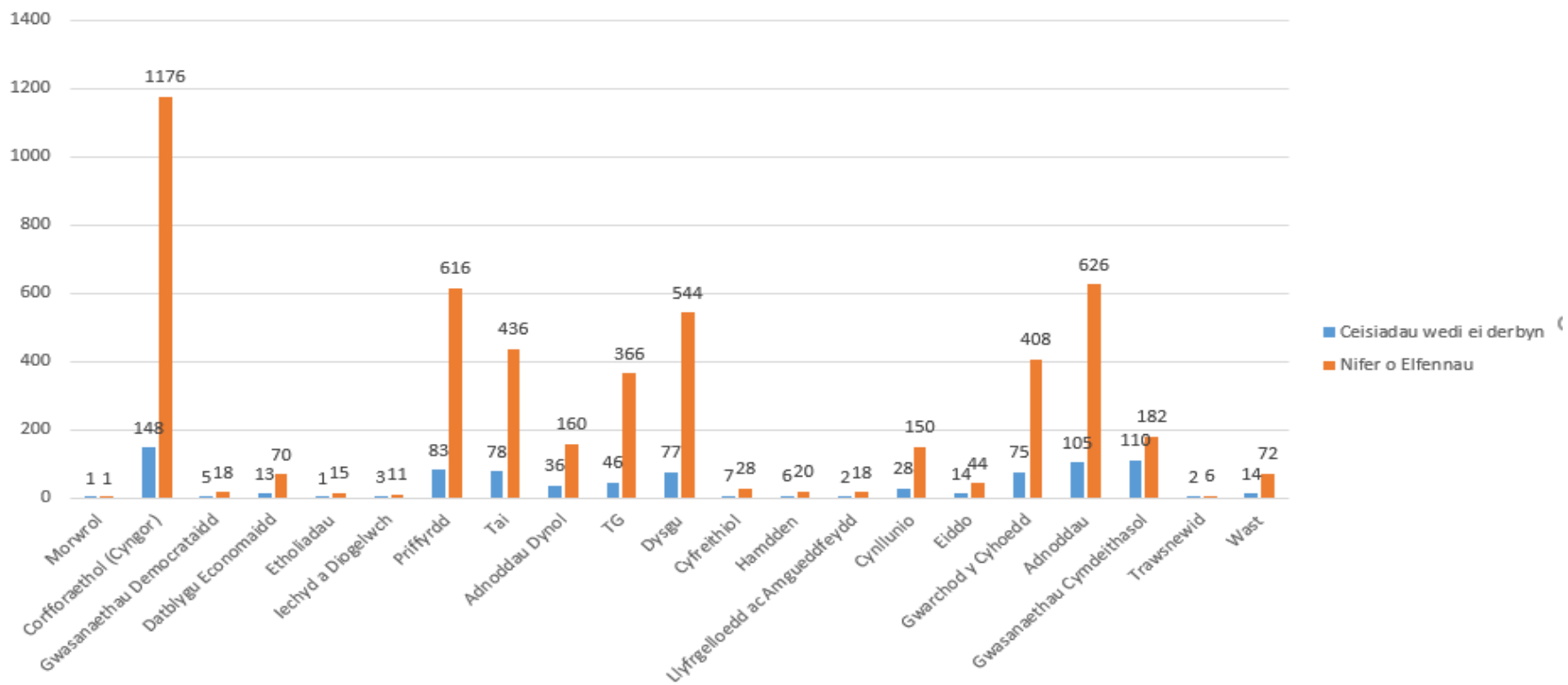
Atodiad 4. Gwybodaeth am geisiadau a chwynion Deddf Rhyddid Gwybodaeth 2000

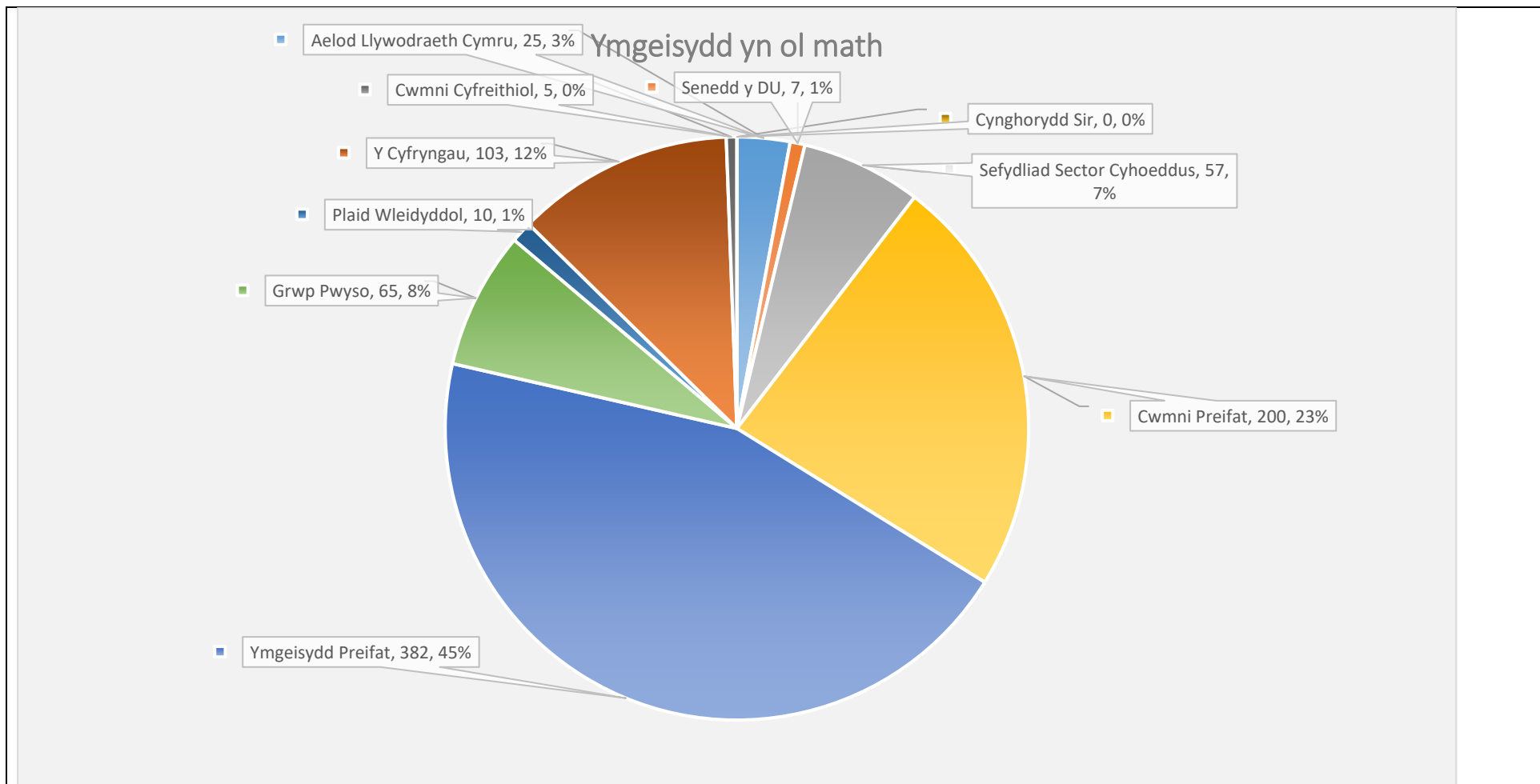
Ceisiadau Deddf Rhyddid Gwybodaeth 2000 ac Adolygiadau Mewnol

Yn ystod y cyfnod 1 Ebrill 2022 i 31 Mawrth 2023 derbyniodd y Cyngor 854 o geisiadau am wybodaeth yn cynnwys 4967 o gwestiynau unigol.

Cyfanswm Nifer y Ceisiadau a Dderbyniwyd 854
 Cyfanswm Nifer y Cwestiynau a Dderbyniwyd 4967

Ceisiadau a Dderbyniwyd fesul Gwasanaeth a Chwestiynau o fewn Ceisiadau





O'r 854 o geisiadau, arweiniodd 2 at Adolygiad Mewnol o ymatebion y Cyngor. Mae'r canlyniadau fel a ganlyn:

- Cadarnhawyd y penderfyniad gwreiddiol yn y naill achos;

Atodiad 5. Gwybodaeth am nifer y cwynion diogelu data a wnaed i'r Cyngor yn ystod y flwyddyn gan unigolion ynghylch y modd y proseswyd eu gwybodaeth bersonol.

Mae deddfwriaeth diogelu data yn atgyfnerthu hawliau gwrthrych y data i gwyno am y modd y mae sefydliadau wedi defnyddio eu data personol, neu'n bwriadu ei ddefnyddio, neu sut y maent fel arall wedi amharu ar hawliau gwrthrych y data.

Cwynion a gyflwynwyd i'r Cyngor o dan y Ddeddf Diogelu Data

Derbyniwyd 3 o gwynion o dan y Ddeddf Diogelu Data,

- 1 yn ymwneud â chais i **gywiro data**
- 2 yn ymwneud â **gwrthwynebu** prosesu data personol gan y Cyngor

Ar ôl archwiliad gan y Swyddog Diogelu Data, **ni chafodd y cwynion eu cadarnhau.** Ystyriwyd bod gweithgareddau prosesu'r Cyngor yn gyfreithlon ac na chafodd hawliau gwrthrychau'r data eu cyfaddawdu.

Atodiad 6. Gwybodaeth am nifer y Ceisiadau Gwrthrych am Wybodaeth a chydymffurfiaeth y Cyngor.

Ceisiadau Gwrthrych am Wybodaeth a chydymffurfiaeth

Derbyniwyd 24 cais o'r fath a derbyniodd 50% (12) ymateb o fewn y terfyn amser statudol, h.y. o fewn mis.

Mae 10 wedi'u gohirio.

Roedd 2 gais yn gymhleth ac felly cafodd y terfyn amser statudol ei ymestyn i dri mis. Derbyniodd 1 o'r rhain ymateb o fewn y terfyn amser newydd ac mae'r llall yn dal i fod gyda'r Gwasanaethau Cymdeithasol.

7.1. Swyddfa'r Comisiynydd Pwerau Ymchwilio

Mae Swyddfa'r Comisiynydd Pwerau Ymchwilio (IPCO) yn goruchwyllo'r modd y mae awdurdodau cyhoeddus yn cynnal gwyliadwriaeth gudd a ffynonellau cudd-wybodaeth ddynol yn unol â Deddf yr Heddlu 1997, Deddf Diogelu Rhyddidau 2012 a Deddf Rheoleiddio Pwerau Ymchwilio 2000 (RIPA). Nod y gyfundrefn RIPA yw sicrhau bod gweithgareddau gwyliadwriaeth gyfeiriedig yn cael eu cynnal mewn ffordd sy'n cydymffurfio â hawliau dynol. Cyflawnir hyn trwy system o hunanawdurdodi gan uwch swyddogion sy'n gorfod bod yn fodlon bod y wylidwriaeth yn angenrheidiol ac yn gymesur; yna mae'n rhaid derbyn cymeradwriaeth gan farnwr i'r hunanawdurdodiad.

Mae Uwch Berchennog Risg Gwybodaeth y Cyngor hefyd yn Uwch Swyddog Cyfrifol ar gyfer cydymffurfiaeth y Cyngor â gweithdrefnau RIPA.

Archwiliwyd a diweddarwyd Polisi'r Cyngor yn ystod y cyfnod adrodd hwn. Fodd bynnag, ni chafodd unrhyw awdurdodiadau eu gwneud yn ystod y cyfnod adrodd hwn.

7.2 Y Comisiynydd Gwybodaeth

Mae'r Comisiynydd Gwybodaeth yn gyfrifol am orfodi a hyrwyddo cydymffurfiaeth â Deddf Diogelu Data 2018 a'r GDPR; Deddf Rhyddid Gwybodaeth 2000; y Rheoliadau Preifatrwydd a Chyfathrebiadau Electronig; y Rheoliadau Gwybodaeth Amgylcheddol; y Rheoliadau Ailddefnyddio Gwybodaeth Sector Cyhoeddus; y Rheoliadau INSPIRE. Mae gan y Comisiynydd Gwybodaeth y pŵer i asesu'r ffordd y mae unrhyw sefydliad wedi prosesu data personol yn erbyn safonau cyfredol 'arfer dda'.

Gwybodaeth am nifer y cwynion diogelu data a wnaed gan unigolion ynghylch y modd y bu i'r Cyngor brosesu eu gwybodaeth bersonol ac yr ymchwiliwyd iddynt gan Swyddfa'r Comisiynydd Gwybodaeth (SCG) yn ystod cyfnod yr adroddiad hwn.

Gwybodaeth am nifer y cwynion diogelu data a wnaed gan unigolion ynghylch y modd y bu i'r Cyngor brosesu eu gwybodaeth bersonol ac yr ymchwiliwyd iddynt gan Swyddfa'r Comisiynydd Gwybodaeth (SCG) yn ystod cyfnod yr adroddiad hwn.

Dim.

Apeliadau Deddf Rhyddid Gwybodaeth i Swyddfa'r Comisiynydd Gwybodaeth

7.3. Y Comisiynydd Camerâu Gwyliadwriaeth

Mae Swyddfa'r Comisiynydd Biometreg a Chamerâu Gwyliadwriaeth yn goruchwyllo cydymffurfiaeth â'r Côt Ymarfer ar gyfer Camerâu Gwyliadwriaeth. Crëwyd swyddfa'r Comisiynydd o dan Ddeddf Diogelu Rhyddidau 2012 i reoleiddio systemau teledu cylch cyfyng (CCTV) ymhellach. Mae'r Comisiynydd Biometreg a Chamerâu Gwyliadwriaeth wedi ymgymryd â chyfrifoldebau'r Comisiynydd Camerâu Gwyliadwriaeth, rôl sydd bellach wedi dod i ben. Yn 2019 ysgrifennodd y Comisiynydd Camerâu Gwyliadwriaeth at Brif Weithredwyr awdurdodau lleol yn y DU yn gofyn iddynt benodi eu Swyddogion Diogelu Data i'r rôl Uwch Swyddog Cyfrifol CCTV.

Bu'r Cyngor yn defnyddio Asesiad o'r Effaith ar Ddiogelu Data y Comisiynydd Camerâu Gwyliadwriaeth mewn perthynas â theledu cylch cyfyng ers 2019-20 ac mae'r Cyngor yn ei ddefnyddio yn awr pryd bynnag y cynigir system teledu cylch cyfyng newydd. Er bod gwasanaethau'n derbyn cyngor ynglŷn â chydymffurfiaeth a llywodraethiant gan y Swyddog Diogelu Data ar gais ac er bod hyfforddiant wedi cael ei drefnu ar gyfer rheolwyr, nid oes rheidrwydd ar wasanaethau i fod yn rhagweithiol wrth rannu gwybodaeth â'r Swyddog Diogelu Data neu'r Un Pwynt Cyswllt CCTV ynglŷn â'u systemau CCTV. Mae'r gwaith a fu'n mynd rhagddo ers 2019 i geisio adolygu systemau CCTV y Cyngor wedi ennyn ymatebion amrywiol ac ansicr. Cydnabyddir bod defnydd y Cyngor o systemau CCTV yn llai ymwithiol na chynghorau eraill, sy'n gweithredu systemau mewn canol trefi, ond mae risg, yn enwedig oherwydd y cydweithio â'r Heddlu, y gallai prosesau llywodraethu gael eu herio.

Rwyf o'r fan bod gwybodaeth gorfforaethol ynglŷn â'r defnydd y mae gwasanaethau yn ei wneud o systemau CCTV yn dameidiog ac anghynhwysfawr. O ganlyniad, mae'n debyg nad oes gan y Cyngor oruchwyliaeth ddigonol o'i systemau ac na all nodi cydymffurfiaeth a bylchau o ran hyfforddiant. Rhaid i Uwch Dîm Arweinyddiaeth y Cyngor gymryd perchnogaeth dros y risgiau sy'n gysylltiedig â defnyddio systemau CCTV.

Rwyf yn ymwybodol bod gwasanaethau'n ystyried defnyddio technoleg Drôn a chamerâu corff ac er y gallai'r math yma o dechnoleg ddarparu gwasanaeth effeithiol, mae'r materion llywodraethiant a'r risgiau ychwanegol o ran cydymffurfiaeth yn gysylltiedig â'r math yma o dechnoleg yn golygu bod angen goruchwyllo cydymffurfiaeth a llywodraethiant ar lefel uwch drwy ddirprwyo'r dasg i'r Uwch Berchennog Risg Gwybodaeth i gefnogi rôl weithredol y Swyddog Un Pwynt Cyswllt CCTV.

Fel yr Uwch Berchennog Risg Gwybodaeth nodaf fod angen adolygu'r defnydd y mae'r Cyngor yn ei wneud o systemau teledu cylch cyfyng fesul gwasanaeth.