Sgiliau Digidol ar gyfer Treftadaeth:

Preifatrwydd a diogelwch ar-lein

Cynhyrchwyd gan Naomi Korn Associates ar gyfer Cronfa Dreftadaeth y Loteri Genedlaethol

CRONFA DREFTADAETH HERITAGE FUND

naomi korn ASSOCIATES

Sgiliau Digidol ar gyfer Treftadaeth

Cyflwyniad

Mae sefydliadau treftadaeth bellach yn gweithio'n fwyfwy ar-lein, ac mae'r pandemig coronafeirws (COVID-19) presennol wedi gwneud hyn yn fwy angenrheidiol nag erioed o'r blaen. Mae diogelu preifatrwydd pobl yn y sector treftadaeth, a chadw gwybodaeth yn ddiogel, yn arbennig o bwysig wrth i ni addasu i ffyrdd newydd o weithio o bell.

Mae'r canllaw yma'n edrych ar rai o'r gweithgareddau ar-lein a gynhelir gan sefydliadau treftadaeth y DU, ac yn ymdrin ag amrywiaeth o faterion y maen nhw'n debygol o ddod ar eu traws. Mae'n cynnwys rhestrau gwirio, cyngor ymarferol ac adnoddau i helpu i ddeall a rheoli gweithgaredd ar-lein. Defnyddiwch y canllaw yma'n unol ag anghenion eich sefydliad i'ch helpu chi, a'r cymunedau rydych chi'n eu cefnogi, i aros yn ddiogel.

Preifatrwydd a diogelwch ar-lein

Mae staff a gwirfoddolwyr sy'n gweithio ar draws y sector treftadaeth yn cefnogi ac yn cysylltu ag ystod amrywiol o gymunedau. Rydym yn casglu, yn diogelu ac yn darparu mynediad at ystod o wrthrychau, adeiladau a mannau. Rydym hefyd yn cynhyrchu gwybodaeth, adnoddau a gweithgareddau, gan gynnwys adnoddau digidol a gweithgareddau sy'n digwydd ar-lein. Mae gwneud defnydd o dechnoleg yn ein galluogi i:

- gweithio o gartref ac o bell
- cyfathrebu a chydweithio gyda chyd-weithwyr a gwirfoddolwyr
- ymgysylltu â chynulleidfaoedd ac ateb cwestiynau
- cadw mewn cysylltiad ag aelodau a noddwyr
- darparu mynediad i adnoddau ac adeiladau

> **"Er nad yw cyfreithiau diogelu data sy'n berthnasol i bobl nad ydynt bellach yn fyw, bydd rhywfaint o ddata personol yn dal i fod yn eich system rheoli casgliadau ac mae angen i chi ei gadw'n ddiogel. Mae bod yn ymwybodol o'r data personol rydych chi'n ei ddal – seiberddiogelwch, diogelwch cyfrinair ac ati – i gyd yn hanfodol.**
>
> Gordon McKenna,
> Rheolwr Safonau,
> Collections Trust

Rheoliadau preifatrwydd a data

Mae'n rhaid i sefydliadau treftadaeth gydymffurfio ag ystod o gyfrifoldebau cyfreithiol ar-lein. P'un a yw'n aelod o'r bwrdd, yn gyflogai neu'n wirfoddolwr, mae gennym i gyd gyfrifoldeb i sicrhau ein bod yn cydymffurfio â'r polisïau diogelwch, diogelu data a phreifatrwydd yn ein sefydliadau. Mae'r polisïau hyn yn esbonio sut mae'r cyfrifoldebau cyfreithiol sy'n ymwneud â diogelwch data personol ac ymddygiad ar-lein derbyniol yn cael eu rheoli. Mae Deddf Diogelu Data 2018 sy'n ymgorffori'r Rheoliad Diogelu Data Cyffredinol (GDPR) yn darparu'r fframwaith ar gyfer y cyfrifoldebau a'r dyletswyddau hyn a chyfeirir atynt yn gyffredinol fel 'deddfwriaeth diogelu data'.

Efallai bod safonau cydnabyddedig y DU neu ryngwladol eraill y mae sefydliadau yn dewis eu mabwysiadu a chydymffurfio â hwy yn eu polisïau mewnol, e.e. y safon rheoli casgliadau SPECTRUM ar gyfer amgueddfeydd.

Beth bynnag yw maint eich sefydliad, rhaid i bawb barchu gwybodaeth bersonol pobl eraill a'i chadw'n ddiogel. Dylai pob sefydliad nodi eu dull o weithredu yn eu Hysbysiad Preifatrwydd, sy'n un o ofynion allweddol y ddeddfwriaeth diogelu data. Y datganiad sy'n wynebu'r cyhoedd sy'n esbonio sut mae'r sefydliad yn diogelu data personol ac yn cymryd ei gyfrifoldebau o ddifrif. Data personol yw unrhyw wybodaeth a all ei hun neu sydd wedi'i chyfuno â gwybodaeth arall nodi person byw. Yn ogystal â'r cyfeiriad e-bost amlwg neu'r enw, gall hyn fod yn ddelwedd CCTV, rhif plât car neu rhif gyfeirnod sy'n cysylltu â chyfrif neu restr bostio.

Ystyrir bod peth gwybodaeth yn arbennig o sensitif a bod ganddi ofynion diogelwch ychwanegol ar gyfer ei thrin os caiff ei chasglu:

- ethnigrwydd
- crefydd
- hanes meddygol
- rhywioldeb
- safbwyntiau gwleidyddol

Mae'r risg o beidio â chydymffurfio os caiff data o'r fath ei golli, ei ddwyn neu ei gamddefnyddio, naill ai drwy ddamwain neu'n fwriadol, yn golygu risg i enw da eich sefydliad a'r potensial ar gyfer cosbau neu ddirwyon.

Mae'r canllaw yma gan Gymdeithas yr Amgueddfeydd Annibynnol (AIM) yn crynhoi sut y gall amgueddfeydd reoli rheoliadau preifatrwydd a data. Bydd yn berthnasol i'r rhan fwyaf o sefydliadau treftadaeth.

Gall deall yr hyn a olygir wrth 'data' fod yn gymhleth. Drwy siartiau llif a chyfnodau syml, mae Swyddfa'r Comisiynydd Gwybodaeth (ICO) wedi darparu canllaw manwl.

Rheoli diogelwch ar-lein a phreifatrwydd

Mae cadw staff, gwirfoddolwyr, a chymunedau - gan gynnwys plant, pobl ifanc a'r rhai sy'n agored i niwed - yn ddiogel mewn mannau ffisegol ac ar-lein yn bwysig i bob sefydliad treftadaeth. Mewn mannau digidol, gellir cynnal diogelwch drwy reoli diogelwch a phreifatrwydd ar-lein yn effeithiol.

Fel gweithwyr a gwirfoddolwyr sy'n gyfrifol am gasglu data personol, mae angen i chi wybod sut i gofnodi'r hyn yr ydych yn ei gasglu, ble mae'n cael ei gadw a sut i'w gadw'n ddiogel ar-lein ac all-lein. Dylid trin cadw data ar bapurau anffurfiol fel rotâu neu rifau cyswllt ar gyfer gwirfoddolwyr gyda'r un gofal â thaenlen ffurfiol gan fod pob risg yn torri preifatrwydd personol os ydynt yn cael eu gadael heb eu goruchwylio neu eu cam-osod. Mae'r canllaw yma'n darparu awgrymiadau er mwyn i chi allu bod yn hyderus mai dim ond am gyhyd ag sydd ei angen y byddwch yn cadw'r wybodaeth ac yna ei dileu ar yr adeg iawn. Mae angen i bob sefydliad gael prosesau clir ar waith i helpu cyflogeion a gwirfoddolwyr i wybod beth i'w wneud.

Mae rheoli preifatrwydd a diogelwch ar-lein i'r safon gorau hefyd yn bwysig oherwydd ei bod yn bwysig i bobl allu ymddiried ynddoch chi. Mae enw da sefydliadau treftadaeth yn dibynnu ar y rhai yr ydym yn gweithio gyda hwy yn hyderus ein bod yn cymryd ein cyfrifoldebau cyfreithiol a phroffesiynol o ddifrif.

> **Mae diogelu preifatrwydd arlein yn hollbwysig. Nid yn unig y mae'n sicrhau bod hawliau unigolion sy'n ymgysylltu â sefydliadau yn cael eu parchu, a bod eu gwybodaeth yn cael ei diogelu rhag mynediad a chamfanteisio anawdurdodedig, mae hefyd yn amddiffyn y sefydliadau eu hunain. Ni fydd neb am ymgysylltu â sefydliad sy'n ddiofal o'i wybodaeth.**
>
> Jon Card, Cyfarwyddwr Gweithredol,
> Swyddog Casgliadau, Llywodraethu a Diogelu Data,
> Imperial War Museums

Adnoddau Defnyddiol

Canllawiau defnyddiol ar egwyddorion cydymffurfio sylfaenol â rheoliadau diogelu data gan Swyddfa'r Comisiynydd Gwybodaeth.

Cyngor ar ddiogelwch ar-lein a diogelwch y Ganolfan Seiberddiogelwch Genedlaethol (NCSC).

Gweithio gartref ac o bell

Mae'r symudiad i weithio gartref oherwydd coronafeirws (COVID-19) wedi cyflymu'r defnydd o offer a gwasanaethau ar-lein gan bob un ohonom. Yn ogystal â dyfeisiau a meddalwedd a allai gael eu darparu gan eich sefydliad treftadaeth, mae llawer ohonom yn defnyddio ein dyfeisiau personol ein hunain gan gynnwys cyfrifiaduron, tabledi a ffonau symudol. Gallem hefyd ddefnyddio gwasanaethau rhad ac am ddim ar y we ar gyfer gwaith a gyflawnir gennym ar gyfer sefydliadau neu brosiectau treftadaeth, gan gynnwys:

- cynadledda fideo
- e-bost
- storio ar-lein
- offer cydweithio
- llwyfannau cyfryngau cymdeithasol

Cadw offer y saff

Cadwch gofnod o ba **ddyfeisiau** sy'n cael eu defnyddio gan yr holl staff a gwirfoddolwyr sy'n gweithio i'ch sefydliad, gan gynnwys sut mae'r ddyfais, y rhifau enghreifftiol a'r codau trefniadaethol unigryw. Ar gyfer asedau sy'n perthyn i'r sefydliad, bydd y wybodaeth hon yn eich helpu i olrhain eich dyfeisiau rhag ofn iddynt gael eu colli neu eu dwyn a nodi unrhyw ddyfeisiau sy'n gofyn am ddiweddariadau a meddalwedd ychwanegol i ddiogelu rhag unrhyw broblemau seiber-ddiogelwch posibl.

Lle mae dyfeisiau personol yn cael eu defnyddio naill ai yn y gweithle neu ar gyfer gweithio gartref, sicrhewch fod yr un safonau diogelwch yn cael eu dilyn fel nad yw data'r sefydliad mewn perygl. Dim ond at y diben yma y dylid defnyddio unrhyw fanylion a gofnodir am ddefnyddio dyfeisiau personol, a'u dileu pan nad oes angen i'r busnes fodoli mwyach.

Deg cam ar gyfer gwell diogelwch rhwydwaith gan yr NCSC.

Mae gan yr ICO ganllawiau defnyddiol ar eich gofynion cyfreithiol a'r camau nesaf wrth weithio o ddyfais bersonol.

> **Mae defnyddio llwyfannau digidol i ennyn diddordeb ein cynulleidfaoedd yn ystod y cyfnod cloi wedi bod yn hanfodol i ni. Rydym yn ei ddefnyddio fel ffordd o rannu'r casgliad, gan amlygu sut y gall y casgliad daflu goleuni ar y llu o faterion mae Cymdeithas yn ymgodymu â nhw heddiw ac yn cynnal casglu cyfoes. Mae ein dibyniaeth gynyddol ar ddigidol fel ffordd o gadw mewn cysylltiad â chymunedau lleol a byd-eang hefyd wedi ein harwain at well dealltwriaeth o faterion sy'n ymwneud â diogelwch ar-lein a phreifatrwydd.**
>
> Kylea Little,
> Ceidwad Hanes,
> Tyne & Wear Archives & Museums

Meddalwedd ac apiau

Dylai meddalwedd ac apiau gael eu diweddaru'n rheolaidd ar bob dyfais a ddefnyddir at ddibenion gwaith, p'un a ydynt yn perthyn i'r sefydliad neu a ydynt yn eiddo personol i chi. Bydd hyn yn helpu i sicrhau bod unrhyw ddata sensitif yn parhau'n ddiogel. Bydd cwmnïau meddalwedd yn diweddaru rhaglenni pan ganfyddir materion diogelwch, i'w cadw'n ddiogel. Er y bydd rhai meddalwedd yn diweddaru'n awtomatig, efallai y byddwch yn cael hysbysiadau ar eich dyfais i'w ddiweddaru eich hun - er enghraifft, mae hysbysiad sy'n dweud wrthych fod diweddariad ar gael ar gyfer ap penodol. Efallai na fydd rhai meddalwedd yn darparu awgrymiadau. Mae'n arfer da i wybod beth rydych chi wedi'i osod ar eich dyfais a chwilio am ddiweddariadau fel mater o drefn.

Mae gan NCSC gyngor ar gadw meddalwedd yn gyfredol a sicrhau eich dyfeisiau.

Wal Dân

System ddiogelwch yw wal dân sy'n rhwystro mynediad anawdurdodedig i rwydwaith preifat sydd wedi'i gysylltu â'r rhyngrwyd. Gall wal dân y caledwedd helpu i ddiogelu grwpiau o gyfrifiaduron mewn rhwydwaith, a gall wal dân meddalwedd ddiogelu dyfeisiau unigol. Os ydych chi'n defnyddio dyfais ar gyfer rheoli neu gyrchu gwybodaeth ar gyfer gwaith, dylech osod wal dân.

Mae rhagor o wybodaeth am waliau tân ar Get Safe Online.

Polisi Defnydd Derbyniol

Dylai sefydliadau treftadaeth sy'n darparu offer a systemau TG fod â Pholisi Defnydd Derbyniol – datganiad ynghylch sut rydych yn defnyddio'r cyfarpar a rheolau clir ynghylch sut y gellir neu na ellir defnyddio rhwydwaith, gwefan neu system eich sefydliad, gan gynnwys WI-FI.

Gweler trosolwg defnyddiol yr ICO ar gyfer sefydliadau ynghylch diogelwch TG, gan gynnwys rhestr wirio ddefnyddiol o ofynion.

Cadw data'n ddiogel

Dim ond data sydd ei angen arnoch ar gyfer eich gwaith y dylech ei gasglu, a dylech sicrhau eich bod yn gwybod beth sy'n cael ei gasglu a sut y caiff ei ddefnyddio, fel y nodir yn Hysbysiad Preifatrwydd eich sefydliad.

Os cesglir data personol at ddibenion gwaith, er mwyn cydymffurfio â'r ddeddfwriaeth diogelu data, mae angen i chi wybod:

- pa ddata personol rydych yn ei gasglu a pham
- ble rydych chi'n ei storio
- sut rydych yn diogelu'r data ac am ba mor hir

Mae deddfwriaeth diogelu data yn ei gwneud yn ofynnol i chi gadw data personol dim ond cyhyd ag y bo ei angen. Bydd hyn yn dibynnu ar nifer o ffactorau, gan gynnwys diben y data ac unrhyw ofynion cyfreithiol sy'n ymwneud â faint o amser y mae'n rhaid cadw mathau penodol o ddata. Er enghraifft, mae rheoliadau ariannol yn ei gwneud yn ofynnol i gadw data sy'n gysylltiedig â phensiwn cyhyd ag y bo gweithiwr yn fyw, pa un a yw'n dal i weithio i'ch sefydliad ai peidio. Efallai mai ychydig iawn o ddefnydd a wneir o ddata personol a gesglir, fel gwybodaeth sy'n ymwneud â chyfranogwyr sy'n mynychu digwyddiad penodol. Yn yr achos yma, heb ganiatâd ychwanegol i gysylltu â chyfranogwyr yn y dyfodol, byddai angen i chi ddileu'r data yma ar ôl y digwyddiad unwaith y bydd yr angen busnes wedi'i gwblhau.

Mae'r ICO yn darparu canllawiau ar ba mor hir y dylid cadw data personol.

Achosion o dorri data

Mae toriad data yn digwydd pan fydd data personol yn cael ei golli, ei gyfaddawdu neu ei ddwyn, boed yn fwriadol neu drwy ddamwain. O dan ddeddfwriaeth diogelu data, mae dyletswydd i hysbysu'r ICO o doriad data **o fewn 72 awr o ddod yn ymwybodol o'r toriad** os effeithir ar ddata personol a gedwir gan eich sefydliad a bod y person dan sylw yn cael ei effeithio.

> Gweler gwybodaeth yr ICO am achosion o dorri data personol, gan gynnwys rhestrau gwirio ar gyfer paratoi ar gyfer toriad ac ymateb iddo.

Copi wrth gefn o'ch data

Gallwch ddiogelu rhag colli data yn anfwriadol neu'n ddamweiniol drwy gadw copi ychwanegol, neu gopi wrth gefn, o ddata. Mae nifer o ffyrdd y gallwch wneud hyn. Bydd rhai gwasanaethau yn cadw copi ychwanegol yn awtomatig i chi. Dylech bob amser sicrhau bod gennych chi gwybodaeth wrth gefn priodol yn ei le. Gallai rhywfaint o'r data a gasglwch fod yn anadferadwy – er enghraifft cyfweliadau hanesion llafar. Gallai mathau eraill o ddata fod yn rhy ddrud neu'n cymryd llawer o amser i'w disodli.

> Canllaw i gefnogi eich data o'r NCSC

Gweithio'n ddiogel gyda data

- Sicrhewch nad yw pobl nad oes ganddynt ganiatâd i weld data cyfrinachol, masnachol, personol neu ddata sensitif arall yn gallu edrych ar hyn pan fyddwch yn ei weld ar eich sgrin.
- Caewch eich sgrin bob amser os ydych i ffwrdd o'ch cyfrifiadur.
- Gwnewch ddefnydd o nodweddion diogelwch fel cyfrinair neu ddiogelwch cod PIN.
- Gosodwch seibiau awtomatig ar eich dyfais.
- Cofiwch allgofnodi o sesiynau os ydych yn gadael eich dyfais heb oruchwyliaeth neu pan fyddwch yn gadael cyfrifiadur a rennir.

Gwe-rwydo

Nod ymosodiadau gwe-rwydo yw twyllo unigolion i ddarparu mynediad at ddata neu ddarparu gwybodaeth yn uniongyrchol. Yn nodweddiadol, bydd y rhain ar ffurf negeseuon e-bost sy'n gofyn i chi glicio ar dolenni neu ffeiliau agored (sy'n caniatáu i sgamwyr osod maleiswedd ar eich dyfais), neu ofyn i chi ddarparu gwybodaeth fel cyfrineiriau neu fanylion bancio. Gall ymosodiadau gael effaith fawr ar sefydliadau ac maent yn gyfystyr â thoriadau diogelwch difrifol, felly dylech fod yn ofalus bob amser.

> Gweler canllawiau'r NCSC ar ymdrin â gwe-rwydo.

- Peidiwch byth â chlicio ar gysylltiadau anghyfarwydd neu amheus mewn negeseuon e-bost, a gwirio i weld o ble daw'r e-bost. Gallwch wneud hyn drwy glicio ar y botwm dde neu hofran dros gyfeiriad e-bost. Gweler canllawiau'r NCSC ar ddelio â negeseuon e-bost amheus.
- Os credwch eich bod wedi bod yn destun ymosodiad gwe-rwydo a allai fod wedi peryglu'r data personol sydd gennych ar gyfer eich sefydliad, dilynwch y camau a amlinellwyd gan yr ICO cyn gynted â phosibl.

Cyfrineiriau

Mae modd lleihau'r risg o fynediad anawdurdodedig (cael eich 'hacio ') a chadw eich data yn ddiogel drwy osgoi cyfrineiriau rhagweladwy a newid cyfrineiriau bob tro.

Os ydych yn cael trafferth cofio cyfrineiriau lluosog, peidiwch â'u hysgrifennu i lawr! Defnyddiwch rheolwr cyfrinair yn lle hynny. Gall y ceisiadau hyn gynhyrchu cyfrineiriau unigryw, cymhleth, sy'n hawdd eu newid ar gyfer yr holl gyfrifon ar-lein a'r storfa ddiogel wedi'i hamgryptio o'r cyfrineiriau hynny.

> Mae'r NCSC yn darparu cyngor ar ddefnyddio cyfrineiriau cryf a rheolwyr cyfrinair.

Cofrestrwyr rhestrau postio a chylchlythyrau

Mae rhestrau postio ar-lein a chylchlythyrau digidol yn ffordd effeithlon i sefydliadau treftadaeth barhau i fod yn gysylltiedig â'u cymunedau. Mae'n rhaid i bobl roi caniatâd i chi gasglu eu data personol, gan gynnwys enwau a chyfeiriadau e-bost, a chytuno i chi ddal eu data at y diben hwnnw. Ni allwch ddefnyddio eu data at unrhyw ddiben arall na rhannu'r data hwnnw gydag eraill hyd yn oed o fewn eich sefydliad eich hun. Dylai pobl hefyd allu tynnu eu caniatâd yn ôl yn hawdd, neu ddad-danysgrifio, ar unrhyw adeg. Dim ond am gyhyd ag sydd ei angen y mae'n rhaid cadw'r data yma.

> Mae'r ICO yn darparu canllawiau ar ddefnyddio rhestrau marchnata a'r defnydd o gwcis.

Adnoddau defnyddiol:

Mae Learn My Way, gan y Good Things Foundation yn cynnwys cyrsiau lefel mynediad ar gadw eich dyfais yn ddiogel a chadw'n ddiogel ar-lein.

Rhif Ffôn Cymorth ICO am ragor o wybodaeth ynghylch preifatrwydd ar-lein.

Canllaw ymarferol yr ICO i ddiogelwch ar-lein.

Bydd y prawf NCSC yma yn eich helpu i ddeall a yw eich sefydliad bach neu ganolig yn meddu ar y diogelwch sylfaenol sydd ei angen arno.

Mae'r canllaw yma ar gyfer cadw plant a phobl ifanc yn ddiogel ar-lein gan Childnet International ar gyfer Cronfa Dreftadaeth y Loteri Genedlaethol yn cwmpasu amrywiaeth o faterion sy'n effeithio ar bawb.

Mae gan arweiniad CILIP ac Ymddiriedolaeth Carnegie ar gyfer llyfrgelloedd cyhoeddus wrth reoli preifatrwydd data awgrymiadau defnyddiol hefyd sy'n berthnasol i sefydliadau treftadaeth.

Rhestr wirio gweithio gartref ac o bell:

- [ ] A ydych chi'n gwybod sut i gadw'ch meddalwedd a'ch systemau wedi'u diweddaru?
- [ ] A ydych chi'n gwybod sut i gadw'ch dyfeisiau a'r data personol rydych chi'n eu defnyddio'n ddiogel?
- [ ] A ydych chi'n defnyddio cyfrineiriau diogel?
- [ ] A ydych chi'n gwirio cyn agor negeseuon e-bost oddi wrth gysylltiadau anghyfarwydd?
- [ ] A ydych chi'n gwybod pa ddata personol rydych chi'n ei storio, pam, ble ac am ba hyd?
- [ ] A allwch chi nodi ac a ydych chi'n gwybod sut i ymateb i doriad data?
- [ ] A ydych yn cadw'r wybodaeth ddiweddaraf am eich cyfrifoldebau diogelwch ar-lein a phreifatrwydd ac yn cyfleu hyn i bobl yr ydych yn gweithio gyda hwy a'u cefnogi?
- [ ] A ydych wedi gofyn am ganiatâd gan eich defnyddwyr i bostio rhestri a chylchlythyrau?
- [ ] A all defnyddwyr ddad-danysgrifio o'ch rhestrau postio a'ch cylchlythyrau yn hawdd?

Defnyddio WI-FI cyhoeddus yn ddiogel

Mae WI-FI yn cyfeirio at grŵp o dechnolegau sy'n caniatáu i ddefnyddwyr lluosog gyrchu'r rhyngrwyd a rhwydweithiau yn ddi-wifr. Efallai y byddwch yn defnyddio cysylltiad WI-FI preifat yn y cartref, neu gysylltiad preifat yn y gwaith y gall aelodau o'ch sefydliad ei gyrchu yn unig. Mae WI-FI cyhoeddus yn cyfeirio at gysylltiad rhwydwaith sydd ar gael i unrhyw un gysylltu ag ef, naill ai gyda chyfrinair neu hebddo, sydd ar gael fel arfer mewn mannau cyhoeddus fel bwytai, siopau a meysydd awyr.

Cymerwch ofal wrth rannu eich cyfrinair WI-FI cartref

Gallai'r rhai sy'n cael mynediad anawdurdodedig i'ch systemau a'ch data fod yn camddefnyddio eich cysylltiad â'r rhwydwaith, neu'r rhai a allai ddefnyddio eich WI-FI ar gyfer gweithgareddau anghyfreithlon fel lawrlwytho cynnwys amhriodol neu anghyfreithlon.

Dylai pobl sy'n defnyddio WI-FI gwadd orfod cytuno ar Bolisi Defnydd Derbyniol (AUP)

Mae AUP yn nodi'r hyn y gall defnyddwyr ei wneud wrth ddefnyddio eich rhwydwaith fel nad yw eu gweithgarwch yn peryglu diogelwch ar-lein eich sefydliad. Gall hyn fod yn glic syml i ddeall y gofynion ond mae'n eu rhoi ar rybudd ynghylch defnydd derbyniol. Bydd gan rai sefydliadau rhagor o hidlyddion sy'n rhoi rhybuddion am ddefnydd amhriodol.

Cofiwch drin wi-fi cyhoeddus bob amser fel ei fod yn llai diogel na rhwydweithiau preifat

Dylid osgoi gwasanaethau nad oes angen eu cofrestru neu gyfrineiriau, a dylid ystyried nad yw'n ddiogel.

Cynghorion ar gyfer defnyddio WI-FI cyhoeddus yn ddiogel:

- Defnyddio cyfrifiadur gyda wal dân a meddalwedd gwrth-firws diweddaraf i ddiogelu eich cyfrifiadur a'i ddata. Mae'r canllawiau hyn gan NCSC yn egluro beth yw meddalwedd gwrth-firws.
- Dylech osgoi anfon negeseuon e-bost cyfrinachol, er enghraifft, rhai sy'n cynnwys data personol neu sensitif, nes y gallwch gysylltu â system fwy diogel.
- Cyfyngu ar rannu ffeiliau.
- Amgryptio ffeiliau sy'n cynnwys data cyfrinachol, personol neu sensitif.
- Cyfyngu ar fewnbynnu gwybodaeth ariannol neu bersonol drwy wefannau oni bai eich bod yn siŵr bod y gwefannau rydych yn ymweld â nhw yn ddiogel. Bydd hyn yn cael ei nodi gan arwydd clo yng nghyfeiriad gwe pob tudalen o wefannau rydych yn ymweld â nhw.

Fideo-gynadledda ar-lein

Mae defnyddio llwyfannau fideo-gynadledda wedi dod yn rhan o'r drefn ddyddiol i lawer o bobl sy'n gorfod gweithio gartref. Mae gwasanaethau poblogaidd yn cynnwys Zoom, Face Time, Microsoft Teams, a GoToMeeting. Gellir defnyddio'r llwyfannau hyn i gynnal cyfarfodydd ffurfiol neu anffurfiol, gweminarau, cyfweliadau, sesiynau addysgu neu ddigwyddiadau.

Erbyn hyn, mae llawer o sefydliadau treftadaeth yn gwneud defnydd rheolaidd o fideo-gynadledda. Ym mis Rhagfyr 2019, roedd gan Zoom 10 miliwn o ddefnyddwyr ac roedd gan Microsoft Teams 32 miliwn o ddefnyddwyr ledled y byd. Erbyn dechrau Mai 2020, oherwydd y cyfyngiadau symud a oedd yn angenrheidiol o ganlyniad i'r pandemig a'r newid i weithio gartref, amcangyfrifodd Zoom fod 300 miliwn o ddefnyddwyr yn cymryd rhan yn ddyddiol a bod gan Microsoft Teams 75 miliwn o ddefnyddwyr gweithredol yn fyd-eang. I lawer ohonom, mae fideo-gynadledda wedi dod yn rhywbeth rydym yn ei ddefnyddio'n rheolaidd i gadw mewn cysylltiad â ffrindiau a theulu ac i weithio. Mae llwyfannau fideo-gynadledda yn ein galluogi i gydweithio mewn amser real a rhannu ffeiliau.

Peryglon posibl fideo-gynadledda

Heb ddefnyddio diogelwch synhwyrol wedi'i ymgorffori yn y llwyfannau, mae gan gyfarfodydd fideo-gynadledda y potensial i gael eu herwgipio gan unigolion neu grwpiau o bobl. Gelwir hyn weithiau'n 'Zoom bombing', ar ôl un o'r llwyfannau mwyaf poblogaidd. Mae'n bosibl bod pobl sy'n bwriadu tarfu ar sesiynau wedi cofrestru i fynychu'r digwyddiad ac mae'n ymddangos eu bod yn gyfranogwyr dilys. Gall ymosodiadau gynnwys rhannu cynnwys amhriodol neu anghyfreithlon, neu ddangos delweddau neu fideo yn y ffenestr cyfranogwr. Gellir camddefnyddio offer cydweithredol - er enghraifft, drwy ddefnyddio bwrdd gwyn neu drwy anodi sleidiau i dynnu testun neu luniau tramgwyddus. Mae ymddangos mewn mannau sgwrsio drwy gopïo a chludo testun tramgwyddus neu anghyfreithlon hefyd yn dacteg gyffredin. Gellir defnyddio sain i ddarlledu synau uchel neu sylwadau ffiaidd. Mae hyn yn brin ac ni ddylai rwystro rhag y manteision sydd gan fideo-gynadledda i'w cynnig.

> **Gyda mwy na 100 o safleoedd treftadaeth a phum swyddfa, roedd rhai staff yn treulio oriau yn teithio bob wythnos. Mae fideo-gynadledda yn golygu y gallwn gwrdd â chydweithwyr o bob cwr o'r Alban heb orfod teithio. Mae hyn wedi gwneud y sefydliad yn fwy cynhyrchiol yn ogystal â lleihau ein hôl troed carbon.**
>
> Susanna Hillhouse,
> Pennaeth Gwasanaethau Casgliadau,
> Ymddiriedolaeth Genedlaethol yr Alban

Dewis llwyfan fideo-gynadledda

Os nad yw eich sefydliad yn darparu llwyfan cynadledda fideo penodol, bydd angen i chi benderfynu pa wasanaeth sy'n gweithio orau i chi. Darllenwch delerau ac amodau'r llwyfan cyn i chi benderfynu ac edrych ar adolygiadau defnyddwyr neu gymuned.

Sicrhewch eich bod yn deall sut bydd y cynnwys a/neu'r data rydych yn ei bostio ar y platfform yn cael eu defnyddio, eu storio a'u rhannu. Gallwch ddod o hyd i'r wybodaeth yma yn nhelerau ac amodau'r gwasanaeth – dylai fod gan bob gwasanaeth bolisi preifatrwydd.

Darganfyddwch sut y bydd recordiadau a data, gan gynnwys cynnwys y cyfleuster sgwrsio, yn cael eu cadw'n ddiogel a pha weithdrefnau sydd gan y llwyfan i roi gwybod i chi am unrhyw achosion o dorri data.

Gallwch hefyd ddod o hyd i gymariaethau o nodweddion diogelwch a phreifatrwydd llwyfannau cynnal fideo ar-lein. Mae'r rhain yn tueddu hyd yn hyn fod yn gyflym gan fod gwasanaethau'n cael eu diweddaru'n gyson, felly gwnewch yn siŵr eich bod yn gwirio dyddiad y cymariaethau. Gwiriwch fod y gymhariaeth yn dod o drydydd parti gwrthrychol.

Efallai bydd gan eich sefydliad bolisïau sy'n cyfyngu neu'n penderfynu ar y platfform a ddefnyddiwch, neu reolau preifatrwydd a all eich helpu i benderfynu.

Casglu data cyfranogwyr

Os ydych yn cynnal cyfarfod neu weithgaredd sy'n agored i'r cyhoedd, gofynnwch i bobl gofrestru ymlaen llaw. Bydd hyn yn eich galluogi i ddarparu unrhyw wybodaeth am y cyfarfod, a chael cytundeb am yr ymddygiad a ddisgwylir a'r caniatâd ar gyfer unrhyw gofnodion sy'n cael eu cynnal. Gallwch ddewis darparu dolenni logio i mewn i'r gweminar neu gyfarfod er mwyn cael mwy o ddiogelwch.

Cofiwch, fel gyda phob data personol, mae'n rhaid i chi gadw enwau, cyfeiriadau e-bost a theitlau swydd yn unig at ddibenion y cyfarfod, a rhaid eu dileu ar ôl y cyfarfod. Rhaid i chi gael caniatâd gan fynychwyr i ddal eu data at unrhyw ddiben arall, ee rhybuddion i ddigwyddiadau tebyg.

Cyn i'ch cyfarfod ddechrau

Polisïau gofod cyfeillgar

Mae gan lawer o sefydliadau bolisïau lle cyfeillgar neu godau ymddygiad y maent yn gofyn i bobl gytuno iddynt cyn mynchu digwyddiadau ar-lein. Mae'r rhain yn sicrhau bod pobl yn glir ynghylch y mathau o ymddygiad a ddisgwylir gan gyfranogwyr, a beth yw canlyniadau peidio â chadw at safonau cymunedol. Mae'n dda gofyn i gyfranogwyr ddarllen y rhain cyn cyfarfodydd, a nodi bod presenoldeb yn cael ei gymryd fel arwydd bod y cyfranogwr yn cytuno i'r rhain.

Mae codau ymddygiad yn ffordd y gall sefydliadau ddangos eu bod yn gwerthfawrogi cyfranogiad pob aelod o'u cymuned, gan sicrhau bod pawb yn teimlo bod croeso iddynt. Os yn bosibl dylech ddatblygu eich cod mewn ymgynghoriad â'ch cymuned.

Mae Sefydliad Wikimedia wedi rhannu eu camau gweithredu a rhai cytundebau enghreifftiol.

Pethau y dylech neu na ddylech eu gwneud ar-lein gan Childnet.

Enghraifft o god ymddygiad ar gyfer digwyddiadau ar-lein (NSCS).

> **Mae fideo-gynadledda wedi bod yn adnodd hanfodol ym mhecyn archifydd yn ystod y cyfyngiadau – sy'n ein galluogi i barhau i hyfforddi, hogi ein sgiliau, a chadw mewn cysylltiad â'n sefydliadau a'n gwirfoddolwyr, yn ogystal ag ateb ymholiadau. Fodd bynnag, fel gweithwyr gwybodaeth proffesiynol, rhaid cydbwyso'r defnyddioldeb anhygoel yma yn erbyn ystyriaeth uchel i gydymffurfiaeth GDPR a diogelwch data.**
>
> Faye McCleod,
> Rheolwraig Archif a Chofnodion

Recordio cyfarfodydd

A ydych yn bwriadu cofnodi'r cyfarfod, neu arbed y sgwrs destun o'r cyfarfod, neu'r ddau?

Er enghraifft, a fydd y sgwrs testun yn cael ei gipio gan y fideo, neu a fyddwch chi'n ei gadw fel ffeil testun? Os felly, bydd angen i chi ofyn am ganiatâd gan y cyfranogwyr ymlaen llaw a'u hatgoffa yn ystod y cyfarfod. Byddant hefyd yn gweld yr arwydd recordio ar y sgrin, a fydd yn gweithredu fel rhybudd.

Fyddwch chi'n ffrydio'n fyw y cyfarfod drwy lwyfan arall fel YouTube?

Edrychwch ar delerau ac amodau'r platfform rydych chi'n ei ddefnyddio a gwnewch yn siŵr eich bod yn cael caniatâd eich cyfranogwyr os ydych chi'n eu cynnwys a/neu'n rhoi sylwadau am gyfleuster sgwrsio. Gwiriwch nad yw defnyddio unrhyw lwyfannau ychwanegol yn peryglu diogelwch eich prif lwyfan, neu gyflwyno materion diogelwch ychwanegol y mae angen i chi fod yn ymwybodol ohonynt.

A fyddwch yn postio'r recordiad yn gyhoeddus ar ôl y digwyddiad? A fyddwch yn cyhoeddi sgyrsiau sgwrs testun a gynhaliwyd yn ystod y cyfarfod?

Bydd angen i chi ofyn am ganiatâd gan gyfranogwyr ymlaen llaw.

Am ba hyd rydych chi'n bwriadu cadw copi o'r recordiad ar gyfer defnydd mewnol eich sefydliad? Os postiwch fideo yn gyhoeddus, a wnewch chi ei dynnu i lawr rywbryd?

Gwnewch yn siŵr bod eich cyfranogwyr yn ymwybodol o hyn fel y gallant roi caniatâd, ac mae hyn wedi'i nodi yn eich polisi mewnol ynghylch storio data.

Offer rheoli ystafelloedd cyfarfod

- Ystyriwch sut y gallech reoli rhyngweithiadau eich cyfranogwyr yn y cyfarfod ar-lein. Bydd y rhan fwyaf o lwyfannau fideo-gynadledda yn gadael i chi ddewis a ydych yn caniatáu i gyfranogwyr ddefnyddio cyfleuster sgwrsio ac a allant rannu eu sgriniau. Bydd y cyfarfod yn gallu tawelu microffonau'r cyfranogwyr a rheoli p'un a yw cyfranogwyr yn gallu defnyddio eu camerâu.

- Gwnewch yn siŵr, fel gwesteiwr, eich bod yn gwybod sut i droi fideo i ffwrdd, tawelu cyfranogwyr, dileu cynnwys ystafell sgwrsio, a chael gwared ar y cyfranogwyr.

- Gosodwch gyfrinair neu gyfleuster ystafell aros ar gyfer cyfarfodydd sy'n cynnwys pobl o'r tu allan i'ch sefydliad. Gosodwch bob cyfarfod gyda chyfrinair newydd a'i rannu dim ond gyda chyfranogwyr rydych chi'n eu hadnabod sy'n ymuno â chi.

- Mae'r opsiwn o ddefnyddio ystafell aros yn golygu y gallwch roi mynediad penodol i bobl yn y sesiwn. Mae hyn yn rhoi mwy o reolaeth i chi dros bwy sydd yn yr ystafell, ond mae'n cymryd mwy o amser, felly nid yw bob amser yn opsiwn ymarferol ar gyfer cyfarfodydd mawr.

- Wrth gofnodi unrhyw rai o'r cyfranogwyr (gan gynnwys siaradwyr allanol) a/neu unrhyw rai yn eu sgwrs fyw, gofalwch eich bod yn cael y caniatâd priodol i'w recordio ac yna i ddarlledu neu gyhoeddi'r darllediad. Mae'n arbennig o bwysig eich bod yn ceisio caniatâd rhieni neu warcheidwaid plant ac oedolion sy'n agored i niwed. Gweler canllaw ICO i geisio a rheoli caniatâd.

Dechrau eich cyfarfod

- Os oes gennych y cyfleuster galluogi sgwrsio, eglurwch i gyfranogwyr sut i'w ddefnyddio, sy'n galluogi ac yn atal i eraill weld y negeseuon y maent yn eu hanfon at ei gilydd, ac a ellir gweld negeseuon preifat gan safonwyr.

- Atgoffwch eich cyfranogwyr os ydych yn bwriadu recordio'r cyfarfod, os byddwch yn recordio neu'n arbed unrhyw sgwrs gyhoeddus, a beth fyddwch chi'n ei wneud gydag unrhyw recordiadau neu gopïau.

- O dan ddeddfwriaeth diogelu data, mae gofynion ychwanegol yn berthnasol i gyfranogwyr sy'n agored i niwed gan ddefnyddio gwasanaethau ar-lein neu adnoddau addysgol. Os bydd unrhyw aelodau o'ch grŵp o dan 13 oed, yna mae angen mesurau diogelu ychwanegol i reoli eu data personol, gan gynnwys cyfarwyddiadau sy'n briodol i'w hoedran, a chynllun a chydsyniad rhieni. Mae'r ICO yn darparu gwybodaeth am reoli eich data.

- Atgoffwch eich cyfranogwyr am yr ymddygiad yr ydych yn ei ddisgwyl ganddynt ac amlygwch gofynion allweddol a amlinellir yn eich cod ymddygiad, e.e . peidio â chaniatáu i eraill gymryd drosodd y sgriniau heb ganiatâd.

Yn ystod y cyfarfod

- Gall cael pobl eraill i helpu i gymedroli a rheoli digwyddiad ar-lein helpu pethau i redeg yn fwy llyfn, ac mae'n sicrhau, os bydd rhywbeth yn mynd o'i le, fod pobl wrth law i sylwi arno a delio ag ef yn gyflym. Os ydych yn galluogi sgwrsio yn ystod y cyfarfod, gwnewch yn siŵr bod gennych o leiaf un person arall gyda chi i gadw golwg arno.

- Dylid ymdrin ag unrhyw ymddygiad sy'n groes i'ch cod ymddygiad yn brydlon. Lle bo angen, dylid dileu cyfranogwyr sy'n torri rheolau ymddygiad o'r cyfarfod.

- Os ydych yn cofnodi'r cyfarfod, diffoddwch y swyddogaeth recordio cyn ac yn ystod unrhyw egwyliau. Atgoffwch y cyfranogwyr ar ôl unrhyw seibiannau bod y recordiad wedi ailddechrau.

Ar ôl y cyfarfod

- Dilëwch unrhyw ddata cofrestru am y cyfranogwyr, oni bai bod gennych ganiatâd i'w gadw, a rheswm clir dros barhau i'w gynnal.

- Dilëwch y recordiadau eu hunain pan nad oes eu hangen arnoch mwyach. Os yw'r recordiadau'n cynnwys unrhyw gynnwys sy'n torri preifatrwydd (er enghraifft, delweddau o blant na cheisiwyd caniatâd gan rieni neu warcheidwaid ar eu cyfer) neu sy'n torri hawlfraint, neu unrhyw gynnwys sy'n anghyfreithlon, bydd yn rhaid i chi dynnu'r adran honno o'r recordiad. Os nad yw hyn yn bosibl, ni fyddwch yn gallu postio'r recordiad.

Adnoddau defnyddiol:

Canllawiau NCSC ar gynadledda fideo

Canllawiau'r ICO ar gynadledda fideo

Rhestr wirio:

- [ ] A ydych wedi darllen drwy'r datganiad diogelwch a phreifatrwydd a ddarparwyd gan y gwasanaeth yr ydych yn ei ddefnyddio?
- [ ] A oes gennych god ymddygiad ar waith, ac a ydych yn gwybod sut y byddwch yn ei rannu â chyfranogwyr?
- [ ] A yw'r gwesteiwr yn rheoli'r nodweddion a'r rheolaethau?
- [ ] Os ydych yn mynd i recordio'r sesiwn, a gawsoch ganiatâd gan y rhai sy'n cymryd rhan, gan gynnwys unrhyw siaradwyr?
- [ ] A ydych chi'n gwybod sut mae'r holl nodweddion diogelwch a phreifatrwydd yn gweithio, a sut i sefydlu'r rhain cyn y cyfarfod? Er enghraifft, cyfrinair yn diogelu eich sesiwn neu'n defnyddio ystafell aros.
- [ ] A oes gennych gynllun ar waith rhag ofn y bydd cynnwys neu ymddygiad tramgwyddus neu anghyfreithlon yn amharu ar eich digwyddiad?
- [ ] A ydych wedi trin unrhyw ddata y gallech fod wedi'i gasglu yn unol â'ch cyfrifoldebau diogelu data?

Cyfryngau Cymdeithasol

Mae llwyfannau cyfryngau cymdeithasol fel Facebook, Twitter ac Instagram yn galluogi unigolion a sefydliadau i gyfathrebu mewn amser real i gysylltu ac ymgysylltu â chymunedau. Gellir eu defnyddio i gynnal digwyddiadau addysgol a sgyrsiau ac ar gyfer gweithgareddau marchnata a hyrwyddo. Gallant fod yn arbennig o ddefnyddiol pan fydd yn bosibl cyfyngu ar fynediad i fannau treftadaeth ffisegol.

Mae'n bwysig gwybod faint o ddata personol y byddwn yn ei bostio, sut rydym yn aros yn ddiogel ar-lein ac yn gochel rhag seiber-droseddu, a sut y gallwn ddiogelu'r cymunedau rydym yn eu cefnogi, yn enwedig y rhai sy'n cynnwys plant ac oedolion agored i niwed. Fel hyn, gallwn gael y gorau o'r cyfryngau cymdeithasol, ond lleihau'r risgiau ar weithgarwch troseddol a chydymffurfio â'n cyfrifoldebau diogelu data a chyfrifoldebau cyfreithiol eraill.

Mae canllaw Cronfa Dreftadaeth y Loteri Genedlaethol/Childnet i weithio gyda phlant a phobl ifanc ar-lein yn cynnwys cynghorion ar weithio'n ddiogel mewn amgylcheddau cyfryngau cymdeithasol.

Hyd yn oed os mai oedolion yw eich cynulleidfa yn bennaf, dylech gofio y gallai fod pobl ifanc ar draws yr holl fannau cyhoeddus ar-lein.

- Gwnewch yn siŵr eich bod yn deall gosodiadau preifatrwydd unrhyw lwyfannau rydych yn eu defnyddio, yn ogystal â sut i roi gwybod am gynnwys amhriodol neu anghyfreithlon.

Mae NCSC yn darparu gwybodaeth am osodiadau preifatrwydd ar draws y llwyfannau mwyaf cyffredin.

- Ymgyfarwyddwch â materion preifatrwydd cyffredin, er enghraifft, rhannu manylion personol neu ffotograffau o bobl eraill heb eu caniatâd. Mae gan yr ICO ganllawiau defnyddiol gydag enghreifftiau o'r defnydd o gyfryngau cymdeithasol a llwyfannau ar-lein.

- Gall plant 13 oed a hŷn greu eu cyfrif eu hunain ar y rhan fwyaf o lwyfannau cyfryngau cymdeithasol. Gweler canllawiau Childnet ynghylch pobl ifanc sy'n defnyddio llwyfannau cyfryngau cymdeithasol.

- Mae gan lawer o sefydliadau bolisi cyfryngau cymdeithasol sy'n rhoi canllawiau ar yr hyn y dylai cyflogeion fod yn ymwybodol ohono, a'r hyn y dylent osgoi ei wneud, ar y cyfryngau cymdeithasol.

Mae Cyngor Cenedlaethol Mudiadau Gwirfoddol wedi darparu Canllawiau ar greu polisi cyfryngau cymdeithasol.

Mae polisi cyfryngau cymdeithasol yr ICO ei hun yn dempled da i sefydliadau.

Mae gan Charity Comms, y rhwydwaith aelodau ar gyfer gweithwyr proffesiynol cyfathrebu elusennol y DU, hefyd dempled polisi cyfryngau cymdeithasol.

> **Mae delweddau gweledol o gyfranogiad yn ein gwaith yn allweddol i gyfryngau cymdeithasol. Rydym bob amser yn ceisio caniatâd i ddefnyddio delweddau o'n cyfranogwyr ar ddechrau prosiect, felly rydym yn hyderus nad ydym yn torri eu rheolau diogelu a thorri prefiatrwydd data**
>
> Emma Larkinson,
> Rheolwr Gweithrediadau a Datblygu,
> Craftspace

> **Mae defnyddio'r cyfryngau cymdeithasol wedi bod yn achubiaeth dros y misoedd diwethaf. Mae wedi fy ngalluogi i gysylltu'n uniongyrchol ac yn bersonol â defnyddwyr sefydledig a chynulleidfaoedd newydd. Gall y cyfryngau cymdeithasol fod yn ddull cyfathrebu cyflym ond rhaid i chi feddwl bob amser, ailddarllen ac ystyried y gynulleidfa cyn postio!**
>
> Heather Dawson,
> Llyfrgellydd Cymorth Academaidd,
> Llyfrgell LSE

Rhagor o adnoddau

Gwybodaeth gan yr ICO ar breifatrwydd a safleoedd rhwydweithio cymdeithasol

Cyngor ar reolaeth gan rieni o Faterion y Rhyngrwyd

Y camau nesaf: parhau i reoli risg

- Cadwch mewn cyswllt â'r wybodaeth ddiweddaraf am eich cyfrifoldebau o ran preifatrwydd a diogelwch ar-lein drwy fynychu sesiynau hyfforddi ac ymwybyddiaeth rheolaidd. Mae Cyflwyniad i seiberddiogelwch: aros yn ddiogel ar-lein yn gwrs ar-lein am ddim gan OpenLearn, a ddatblygwyd gan y Brifysgol Agored gyda chymorth rhaglen seiberddiogelwch genedlaethol Llywodraeth y DU.
- Gwybod sut y gallwch weithio o gartref ac aros yn ddiogel ar-lein. Mae'r The Prince's Responsible Business Network yn ganllaw cyflym sydd â chysylltiadau i e-ddysgu seiber-ddiogelwch, canllawiau gweithio gartref ac adnoddau busnes bach.
- Cofrestrwch i dderbyn cylchlythyr ICO a diweddariadau NCSC i gael y wybodaeth ddiweddaraf am breifatrwydd a diogelwch ar-lein.
- Adolygwch eich trefniadau diogelwch a phreifatrwydd digidol yn rheolaidd, yn benodol sut a lle y caiff data personol a sensitif ei storio er mwyn asesu a rheoli risgiau diogelwch yn effeithiol.
- Darganfod beth i'w wneud os ydych yn amau colli data a bod angen i chi ddilyn gweithdrefnau torri diogelwch. Bydd hyn yn eich galluogi i ymateb yn gyflym drwy rybuddio cydweithwyr a, lle bo angen, adrodd i'r ICO o fewn y 72 awr gofynnol.