Page

Preifatrwydd a diogelwch ar-lein

14/07/2020

14/07/2020

See all updates

Cyngor ac adnoddau ar gyfer sefydliadau treftadaeth - cadw gwybodaeth yn ddiogel a diogelu preifatrwydd pobl wrth weithio ar-lein.

Atodiad	Maint
Digital guide: Online privacy and security	234.98 KB
Canllaw Digidol: Preifatrwydd a diogelwch ar-lein (Fersiwn Cymraeg)	251.76 KB

Cynhyrchwyd y canllaw yma gan Naomi Korn Associates ar gyfer Cronfa Dreftadaeth y Loteri Genedlaethol. Mae'n rhan o'n Cynllun Sgiliau Digidol ar gyfer Treftadaeth, a gynlluniwyd i wella sgiliau digidol a hyder ar

draws holl sector treftadaeth y DU.

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

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.

"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

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

“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

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

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.

Rhestr wirio gweithio gartref ac o bell

1. A ydych chi'n gwybod sut i gadw'ch meddalwedd a'ch systemau wedi'u diweddaru?
2. A ydych chi'n gwybod sut i gadw'ch dyfeisiau a'r data personol rydych chi'n eu defnyddio'n ddiogel?
3. A ydych chi'n defnyddio cyfrineiriau diogel?
4. A ydych chi'n gwirio cyn agor negeseuon e-bost oddi wrth gysylltiadau anghyfarwydd?
5. A ydych chi'n gwybod pa ddata personol rydych chi'n ei storio, pam, ble ac am ba hyd?
6. A allwch chi nodi ac a ydych chi'n gwybod sut i ymateb i doriad data?
7. 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?
8. A ydych wedi gofyn am ganiatâd gan eich defnyddwyr i bostio rhestri a chylchlythyrau?
9. A all defnyddwyr ddad-danysgrifio o'ch rhestrau postio a'ch cylchlythyrau yn hawdd?

Adnoddau defnyddiol

- Mae Learn My Way, gan y Good Things Foundations 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.

Defnyddio WI-FI cyhoeddus yn ddiogel

Mae WI-FI yn cyfeirio at gr?p 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 si?r 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.

"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

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.

"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 McLeod, Rheolwraig Archif a Chofnodion

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.

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 si?r 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)

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 si?r 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 si?r 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 si?r, 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 gr?p 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 si?r 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.

Rhestr wirio

1. A ydych wedi darllen drwy'r datganiad diogelwch a phreifatrwydd a ddarparwyd gan y gwasanaeth yr ydych yn ei ddefnyddio?
2. A oes gennych god ymddygiad ar waith, ac a ydych yn gwybod sut y byddwch yn ei rannu â chyfranogwyr?
3. A yw'r gwesteiwr yn rheoli'r nodweddion a'r rheolaethau?
4. Os ydych yn mynd i recordio'r sesiwn, a gawsoch ganiatâd gan y rhai sy'n cymryd rhan, gan gynnwys unrhyw siaradwyr?
5. 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.
6. A oes gennych gynllun ar waith rhag ofn y bydd cynnwys neu ymddygiad tramgwyddus neu anghyfreithlon yn amharu ar eich digwyddiad?
7. A ydych wedi trin unrhyw ddata y gallech fod wedi'i gasglu yn unol â'ch cyfrifoldebau diogelu data?

Adnoddau defnyddiol

- Canllawiau NCSC ar gynadledda fideo
- Canllawiau'r ICO ar gynadledda fideo

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.

“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

- Gwnewch yn si?r 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 h?n 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

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.

Expand All accordions

Online privacy and security

Staff and volunteers working across the heritage sector support and connect with a diverse range of communities. We collect, preserve and provide access to a range of objects, buildings and spaces. We also produce information, resources and activities, including digital resources and activities that take place online. Making use of technology enables us to:

- work from home and at distance
- communicate and collaborate with co-workers and volunteers
- engage with audiences and answer questions
- keep in touch with members and patrons
- provide access to resources and buildings

Privacy and data regulations

Heritage organisations must comply with a range of legal responsibilities in this online space. Whether board member, employee or volunteer, we all have a responsibility to make sure we comply with the security, data protection and privacy policies in our organisations. These policies explain how the legal responsibilities relating to the security of personal data and acceptable online behaviour are managed. The Data Protection Act 2018 incorporating the General Data Protection Regulation (GDPR) provides the framework for these responsibilities and duties and is commonly referred to as 'data protection legislation'.

There may be other recognised UK or international standards that organisations choose to adopt and comply with in their internal policies, eg the SPECTRUM collection management standard for museums.

Whatever the size of your organisation, everyone must respect others' personal information and keep it secure. Each organisation should set out their approach in their Privacy Notice, which is a key requirement of the data protection legislation. It is the publicly facing statement that explains how the organisation protects personal data and takes its responsibilities seriously. Personal data is any information that by itself or when combined with other information can identify a living person. As well as the obvious email address or name, this can be a CCTV image, car number plate or reference number that links to an account or mailing list.

Some information is regarded as particularly sensitive and has additional security requirements for its handling if it is collected:

- ethnicity
- religion
- medical history
- sexuality
- political views

The risk of non-compliance if such data is lost, stolen or misused, either by accident or deliberately, means reputational risk for your organisation and the potential for sanctions or fines.

- This guide from The Association of Independent Museums (AIM) summarises how museums can manage privacy and data regulations. It will be relevant to most heritage organisations.
- Understanding what is meant by 'data' can be complex. Through flowcharts and simple stages the Information Commissioner's Office (ICO) has provided a detailed guide.

> *"Although data protection laws don't apply to people who are no longer alive, there will still be a surprising amount of personal data in your collections management system and you need to keep it safe. Being aware of what personal data you do hold – cybersecurity, password protection and so on – are all crucial."*
>
> *Gordon McKenna, Standards Manager, Collections Trust*

Managing online security and privacy

Keeping staff, volunteers, and communities – including children, young people and the vulnerable – safe in both physical and online spaces is important to all heritage organisations. In digital spaces, safety can be maintained through effective management of online security and privacy.

As employees and volunteers responsible for collecting personal data, you need to know how to record what you collect, where it is held and how to keep it safe both online and offline. Holding onto informal paper lists of rotas or contact numbers for volunteers needs to be treated with the same care as a formal spreadsheet because each risks breaching personal privacy if left unattended or mislaid. This guide provides pointers so you can be confident that you hold the information only for as long as it is needed and then delete it at the right time. Each organisation needs to have clear processes in place to help employees and volunteers know what to do.

Managing online privacy and security well is also important because trust matters. The reputation of heritage organisations depends upon those we work with having confidence that we take our legal and professional responsibilities seriously.

> *"Protecting privacy online is crucial. Not only does it ensure individuals who engage with organisations have their rights respected and their information secured from unauthorised access and exploitation, it also protects the organisations themselves. No one will want to engage with an institution that is careless with their information."*
>
> *Jon Card, Executive Director, Collections and Governance and Data Protection Officer, Imperial War Museums*

Useful resources

- Helpful guidance on the basic principles of data protection compliance from the ICO
- The National Cyber Security Centre (NCSC) advice on online safety and security

Expand All accordions

Home and remote working

The shift to homeworking due to coronavirus (COVID-19) has accelerated the use of online tools and services by all of us. As well as devices and software that might be provided by your heritage organisation, many of us are using our own personal devices including computers, tablets and mobile phones. We might also use free and low cost web-based services for work we carry out for heritage organisations or projects, including:

- video conferencing
- email
- online storage
- collaboration tools
- social media platforms

> *"Using digital platforms to engage our audiences during lockdown has been critical to us. We use it as a way of sharing the collection, highlighting how the collection can shed light on the many issues society is grappling with today and carrying out contemporary collecting. Our increased reliance on digital as a means of keeping in touch with local and worldwide communities has also led us to a better understanding of issues around online security and privacy."*
>
> *Kylea Little, Keeper of History, Tyne & Wear Archives & Museums*

Keeping equipment safe

Keep a record of what devices are being used by all staff and volunteers working for your organisation, including the make of the device, model numbers and unique organisational codes. For assets belonging to the organisation, this information will help you trace your devices in case they are lost or stolen and identify any devices that require updates and extra software to protect against any potential cyber security issues.

Where personal devices are being used either in the workplace or for home working, ensure that the same security standards are being followed so that the organisation's data is not at risk. Any details captured about the use of personal devices should only be used for this purpose, and deleted when the business need no longer exists.

- Ten steps for better network security from the NCSC
- The ICO has useful guidance on your legal requirements and next steps when working from a personal device.

Software and apps

Software and apps should be updated regularly on all devices used for work purposes, whether they belong to the organisation or are personally owned by you. This will help ensure any sensitive data remains secure. Software companies will update programmes when security issues are discovered, to keep them secure. While some software will update automatically, you might get notifications on your device to manually update – for example, a notice that tells you an update is available for a specific app. Some software may not provide prompts. It's good practice to know what you have installed on your device and routinely check for updates.

The NCSC has tips on keeping software up to date and securing your devices.

Firewalls

A firewall is a security system that prevents unauthorised access to a private network connected to the internet. A hardware firewall can help to protect groups of computers in a network, and software firewalls can protect individual devices. If you are using a device for managing or accessing information for work, you should install a firewall.

Further information about firewalls from Get Safe Online

Acceptable Use Policy

Heritage organisations that provide IT equipment and systems should have an Acceptable Use Policy – a statement about how you use the equipment and clear rules about how your organisation's network, website or system can or can't be used, including Wi-Fi.

See the ICO's helpful overview for organisations about IT security, including a handy checklist of requirements.

Keeping data secure

You should only collect data that you need for your work, and you should ensure that you know what is being collected and how it will be used, as set out in your organisation's Privacy Notice.

If personal data is collected for work purposes, in order to comply with the data protection legislation, you need to know:

- what personal data you are collecting and why
- where you are storing it
- how you are protecting the data and for how long

Data protection legislation requires you to retain personal data only for as long as it is needed. This will depend on a number of factors, including the purpose of the data and any legal requirements there are relating to the length of time specific types of data must be kept. For example, financial regulations require pension-related data to be kept for as long as an employee is alive, regardless of whether they are still working for your organisation.

Some personal data collected might have a very limited use, such as information relating to participants who are attending a specific event. In this case, without additional permissions to contact participants in future, you would need to delete this data after the event once the business need had completed.

The ICO provides guidance on how long personal data should be kept

Data breaches

A data breach occurs when personal data is lost, compromised or stolen, whether deliberately or by accident. Under data protection legislation, there is a duty to inform the ICO of a breach **within 72 hours of becoming aware of the breach** if personal data held by your organisation is affected and the subject concerned is potentially affected.

See the ICO's information about personal data breaches, including checklists for preparing for and responding to a breach.

Back up your data

You can guard against unintended or accidental loss of data by keeping an additional copy, or back-up, of data. There are a number of ways that you can do this. Some services will provide automatic back-ups for you. You should always make sure that you have an appropriate back-up in place. Some data you collect might be irreplaceable – for example oral history interviews. Other kinds of data might be prohibitively expensive or time-consuming to replace. The NCSC has a guide to backing up your data.

Work safely with data

- Ensure that people who don't have permission to view confidential, commercial, personal or other sensitive data aren't able to look at this when you are viewing it on your screen.
- Always close your screen if you are away from your computer.
- Make use of security features like password or PIN code protection.
- Set an automatic session time-out on your device.
- Manually log out of sessions if leaving your device unattended or when you leave a shared computer.

Phishing

Phishing attacks are designed to trick individuals into providing access to data or providing information directly. Typically, these will be in the form of emails which ask you to click on links or open files (which allow scammers to install malware on your device), or ask you to provide information like passwords or banking details. Attacks may have a big impact on organisations and constitute serious security breaches, so you should always be careful. See the NCSC's guidance on dealing with phishing.

- Never click on unfamiliar or suspicious links in emails, and check to see if emails are really from who they say they are. You can do this by right-clicking or hovering over an email address. See the NCSC's guidance on dealing with suspicious emails.
- If you think you have been the subject of a phishing attack which might have compromised the personal data that you hold for your organisation, follow the steps outlined by the ICO as soon as possible.

Passwords

Reduce the risk of unauthorised access (being 'hacked') and keep your data safe by avoiding predictable passwords and always changing default passwords.

If you have trouble remembering multiple passwords, don't write them down! Use a password manager instead. These applications can generate unique, complex, easily changed passwords for all online accounts and the secure encrypted storage of those passwords.

The NCSC provides advice on using strong passwords and password managers.

Mailing lists and newsletter sign-ups

Online mailing lists and digital newsletters are an efficient way for heritage organisations to stay connected with their communities. People must give consent for you to collect their personal data, including names and email addresses, and agree to you holding their data for that purpose. You cannot use their data for any other purpose or share that data with others even within your own organisation. People should also be able to easily withdraw their consent, or unsubscribe, at any point. This data must only be held for as long as it is required.

The ICO provides guidance on using marketing lists and the use of cookies.

Home and remote working checklist

1. Do you know how to keep your software and systems updated?
2. Do you know how to keep your devices and the personal data you are accessing secure?
3. Are you using secure passwords?
4. Do you check before opening emails from unfamiliar contacts?
5. Do you know what personal data you are storing, why, where and for how long?
6. Can you identify and do you know how to respond to a data breach?
7. Are you keeping updated about your online security and privacy responsibilities and communicating this to people you work with and support?
8. Have you sought consent from your users to mailing lists and newsletters?
9. Can users unsubscribe from your mailing lists and newsletters easily?

Useful resources

- Learn My Way, by the Good Things Foundation includes entry-level courses on keeping your device safe and keeping safe online.
- ICO helpline for further assistance regarding privacy
- ICO practical guide to online security
- This NCSC test will help you understand whether your small- or medium-sized organisation has the basic security it needs in place.
- This guide for keeping children and young people safe online by Childnet International for The National Lottery Heritage Fund covers a range of issues that affect everyone.
- CILIP and the Carnegie Trust's guide for public libraries in managing data privacy has useful pointers also applicable to heritage organisations.

Expand All accordions

Using public Wi-Fi safely

Wi-Fi refers to a group of technologies that allow multiple users to access the internet and networks wirelessly. You may use a private Wi-Fi connection at home, or a private connection at work that can only be accessed by members of your organisation. Public Wi-Fi refers to a network connection that is available for anyone to connect to, either with or without a password, typically available in public places like restaurants, shops and airports.

Take care when sharing your home Wi-Fi password

Your network connection could be misused by those gaining unauthorised access to your systems and data, or those who may use your Wi-Fi for illegal activities such as downloading inappropriate or illegal content.

People using guest Wi-Fi should have to agree to an Acceptable Use Policy (AUP)

An AUP sets out what users can and can't do while using your network so that their activity doesn't compromise your organisation's online security. This can be a simple click to understand the requirements but it puts them on notice about acceptable use. Some larger organisations will have filters that provide alerts about inappropriate use.

Always treat public Wi-Fi as being less secure than private networks

Services that don't require registration or passwords should be avoided and regarded as insecure.

Tips for using public Wi-Fi safely:

- Use a computer with a firewall and up to date anti-virus software to protect your computer and its data. This guidance from NCSC explains what anti-virus software is.
- Avoid sending confidential emails, for example those including personal or sensitive data, until you can connect to a more secure system.
- Limit file sharing.
- Encrypt files that contain confidential, personal or sensitive data.
- Limit inputting financial or personal information via any websites unless you are sure that the websites that you visit are secure. This will be indicated by a padlock sign in the web address of all the pages of websites that you visit.

Expand All accordions

Online video conferencing

Using video conferencing platforms has become part of the daily routine for many people having to work from home. Popular services include Zoom, Face Time, Microsoft Teams, and GoToMeeting. These platforms can be used to host formal or informal meetings, webinars, interviews, teaching sessions or events.

> *"With over 100 heritage sites and five offices some staff were spending hours on the road each week. Video conferencing means we can meet colleagues from all over Scotland without the need to travel. This has made the organisation more productive as well as reducing our carbon footprint."*
>
> *Susanna Hillhouse, Head of Collections Services, National Trust for Scotland*

Many heritage organisations are now routinely making use of video conferencing. In December 2019, Zoom had 10 million users and Microsoft Teams had 32 million users worldwide. By the beginning of May 2020, due to the lockdown made necessary by the pandemic and the shift to homeworking, Zoom estimated that it had 300 million participant users daily and Microsoft Teams had 75 million active users globally. For many of us, video conferencing has become something we use regularly to stay in touch with friends and family

and to work. Video conferencing platforms enable us to collaborate in real time and share files.

> *“Video conferencing has been an essential tool in the archivist’s kit during lockdown – allowing us to continue to train, hone our skills, and keep in touch with our organisations and volunteers, as well as answer queries. However, as information professionals, this incredible usefulness must be balanced against a high regard for GDPR compliance and data security.”*
>
> *Faye McLeod, Archivist and Records Manager*

Potential risks of video conferencing

Without using sensible security built into the platforms, video conference meetings have the potential to be hijacked by individuals or groups of people. This is sometimes called ‘Zoom bombing’, after one of the most popular platforms. People planning to disrupt sessions may have signed up to attend the event and appear to be legitimate participants. Attacks may include sharing inappropriate or illegal content, or showing images or video in the participant window. Collaborative tools may be misused - for example, using a whiteboard or annotating slides to draw offensive text or pictures. Flooding chat spaces by copying and pasting offensive or illegal text is also a common tactic. Audio can be used to broadcast loud noises or obscene comments. This is rare and should not deter from the benefits that video conferencing has to offer.

Choosing a video conferencing platform

- If your organisation doesn’t provide a specific video conferencing platform, you will need to decide which service works best for you. Read the platform’s terms and conditions before you decide and look at user or community reviews.
- Make sure that you understand how the content and/or data you post on the platform will be used, stored and shared. You can find this information in the service terms and conditions – all services should have a privacy policy.
- Find out how recordings and data, including chat facility content, will be kept secure and what procedures the platform has in place to tell you about any data breaches.
- You can also find comparisons of video hosting platforms security and privacy features online. These tend to date very quickly as services are updated constantly, so be sure to check the date of the comparisons. Check that the comparison comes from an objective third party.
- Your organisation might have policies that restrict or determine the platform you use, or privacy rules that can help you decide.

Collecting participant data

If you are hosting a meeting or activity that is open to the public, ask people to sign up in advance and register. This will enable you to provide any information about the meeting, and get agreement for expected behaviour and consent for any recording taking place. You can choose to provide individual log-in links to the webinar or meeting for additional security.

Remember, as with all personal data you must only keep names, email addresses and job titles for the purposes of the meeting, and it must be deleted after the meeting. You must obtain permission from attendees to hold their data for any other purpose, eg alerts to similar events.

Before your meeting starts

Friendly space policies

Many organisations have friendly space policies or codes of conduct that they ask people to agree to before attending in-person and online events. These make sure people are clear about the kinds of behaviours that are expected from participants, and what the consequences of not adhering to community standards are. It's good to ask participants to read these before meetings, and state that attendance is taken as a sign that the participant agrees to these.

Codes of conduct are a way that organisations can demonstrate that they value the participation of all members of their community, ensuring everyone feels welcome. If possible you should develop your code in consultation with your community.

- The Wikimedia Foundation have shared their implementation steps and some sample agreements.
- Some dos and don'ts of online behaviour from Childnet
- An example of a code of conduct for online events (NSCS)

Recording meetings

Are you planning on recording the meeting, or saving the text chat from the meeting, or both?

For example, will the text chat be captured by the video, or will you save it as a text file? If so, you will need to seek consent from participants in advance and remind them during the meeting. They will also see the recording sign on the screen, which will act as an alert.

Will you be live streaming the meeting via another platform such as YouTube?

Check the terms and conditions of the platform you are using and make sure that you have the consent of your participants if you are including them and/or chat facility comments. Check that use of any additional platforms doesn't compromise the security of your main platform, or present additional security issues you need to be aware of.

Will you be posting the recording in public after the event? Will you be publishing text chat conversations that took place during the meeting?

You will need to seek permission from participants in advance.

How long are you planning on keeping a copy of the recording for the internal use of your organisation? If you post a video publicly, will you take it down at some point?

Make sure your participants are aware of this so they can provide consent, and this is set out in your internal policy about storing data.

Meeting room management tools

- Consider how you might want to manage your participants' interactions in the online meeting. Most video conferencing platforms will let you choose whether you allow participants to use a chat facility and whether they can share their screens. The host of the meeting will be able to mute participants' microphones and control whether participants are able to use their cameras.

- Make sure, as host, that you know how to turn off video, mute participants, delete chatroom content, and eject participants.
- Set up a password or a waiting room facility for meetings involving people from outside your organisation. Set up each meeting with a new password and share it only with participants you know are joining you.
- Using a waiting room option means that you can manually let people into the session. This gives you greater control over who is in the room, but takes more time, so isn't always a practical option for big meetings.
- When recording any of the participants (including external speakers) and/or any of their live chat, ensure you have the appropriate consent to record them and then to broadcast or publish the broadcast. It is particularly important that you seek consent from parents or guardians of children and vulnerable adults. See the ICO guide to seeking and managing consent.

Starting your meeting

- If you have the chat facility enabled, explain to participants how to use it, who can and can't see messages they send to each other, and whether private messages can be viewed by moderators.
- Remind your participants if you are planning on recording the meeting, if you will be recording or saving any of the public chat, and what you will be doing with any recordings or copies.
- Under data protection legislation, additional requirements apply to vulnerable participants using online services or educational resources. If any members of your group are under 13 years old then additional safeguards are required to manage their personal data, including age-appropriate instructions and design and parental consent. The ICO provide information on managing children's data.
- Remind your participants about the behaviour you expect from them and highlight key requirements outlined in your code of conduct, eg not allowing others to take screenshots without permission.

During the meeting

- Having other people to help moderate and manage an online event can help things run more smoothly, and ensures that if anything goes wrong there are people on hand to spot it and deal with it quickly. If you enable chat during the meeting, make sure you have at least one other person with you to keep an eye on it.
- Any behaviour that is in breach of your code of conduct should be dealt with promptly. Where necessary, participants who breach behaviour rules should be removed from the meeting.
- If you are recording the meeting, switch off the recording functionality before and during any breaks. Remind participants after any breaks that the recording has resumed.

After the meeting

- Delete any registration data about the participants, unless you have permission from them to retain it and a clear reason to continue to hold it.
- Delete the recordings themselves when you no longer need them. If the recordings contain any content that breaches privacy (for example, images of children for which permission from parents or guardians has not been sought) or infringes copyright, or any content which is illegal, you will have to remove that section of the recording. If this is not possible, you will not be able to post the recording.

Video conferencing checklist

1. Have you read through the security and privacy statement provided by the service you are using?
2. Do you have a code of conduct in place, and know how you will share this with participants?
3. Is the host in control of the features and controls?

4. If you are going to record the session, have you got consent from meeting participants, including any speakers?
5. Do you know how all the security and privacy features work, and how to set these up prior to the meeting? For example, password protecting your session or using a waiting room.
6. Do you have a plan in place in case your event is disrupted by offensive or illegal content or conduct?
7. Have you treated any data you may have collected in line with your data protection responsibilities?

Useful resources

- NCSC guidance on video conferencing
- ICO guidance on video conferencing

Expand All accordions

Social media

Social media platforms like Facebook, Twitter and Instagram enable individuals and organisations to communicate in real time to connect and engage with communities. They can be used to host educational events and talks and for marketing and promotional activities. They can be particularly useful when access to physical heritage spaces may be restricted.

It's important to know how much personal data we post, how we stay safe online and guard against cyber crime, and how we can protect the communities we support, particularly those that include children and vulnerable adults. In this way, we can get the most from social media, but reduce the risks on criminal activity and comply with our data protection and other legal responsibilities.

The National Lottery Heritage Fund/Childnet guide to working with children and young people online includes tips on working safely in social media environments. Even if your audience is primarily adults, you should be mindful that there might be young people across all public online spaces.

> *"Using social media has been a lifeline over the last few months. It has enabled me to connect directly and personally with established users and new audiences. Social media may be a rapid form of communication but you must always think, reread and consider the audience before posting!"*
>
> *Heather Dawson, Academic Support Librarian, LSE Library*

- Make sure you understand the privacy settings of any platforms you use, as well as how to report inappropriate or illegal content. The NCSC provides information about privacy settings across the most common platforms.
- Familiarise yourself with common privacy issues, for example, sharing personal details or photographs of others without their permission. The ICO has helpful guidance with examples on the use of social media and online platforms.
- Children aged 13 and over can create their own account on most mainstream social media platforms. See Childnet's guidance about young people using social media platforms.
- Many organisations have a social media policy which provides guidelines on what employees should be aware of, and what they should avoid doing, on social media.

- The National Council for Voluntary Organisations has provided guidance on creating a social media policy.
- The ICO's own social media policy provides a good template for organisations.
- Charity Comms, the membership network for UK charity communications professionals, also has a social media policy template.

> *"Visual images of participation in our work are key to social media. We always seek permission to use images of our participants at the outset of a project so we are confident we don't infringe their privacy and break data protection rules"*
>
> *Emma Larkinson, Operations and Development Manager, Craftspace*

Further resources

- ICO information on privacy and social networking sites
- Advice on parental controls from Internet Matters

Expand All accordions

Next steps: continuing to manage risk

Keep up to date about your responsibilities regarding privacy and online security by attending regular training and awareness sessions. Introduction to cyber security: stay safe online is a free online course from OpenLearn, developed by The Open University with support from the UK Government's National Cyber Security Programme.

Know how you can work from home and stay safe online. The Prince's Responsible Business Network's at-a-glance guide links to free cyber security e-learning, home working guidance and small business resources.

Sign up to the ICO newsletter and NCSC updates for the latest information about privacy and online security.

Regularly review your digital security and privacy arrangements, specifically how and where personal and sensitive data is stored in order to effectively assess and manage security risks.

Know what to do if you suspect a data loss and need to follow security breach procedures. This will enable you to respond quickly by alerting colleagues and where necessary reporting to the ICO within the required 72 hours.

Expand All accordions

Sharing this guide

Expand All accordions

Digital Skills for Heritage

The coronavirus (COVID-19) pandemic has made the need for organisations to understand and make use of digital more pressing than ever.

We are working with our partners to better meet the new and emerging needs of the heritage sector. We also want to help organisations develop the skills that will build their resilience long term.