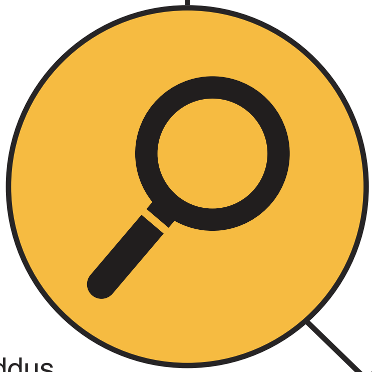
DIOGELU EICH PREIFATRWYDD AR-LEIN

Cynnwys

Preifatrwydd	3
Pwysigrwydd Preifatrwydd	4
Eich Cyd-gyfrifoldeb	4
Risgiau i Ddiogelwch Data	5
Gweithio o gartref	6
Defnyddio eich offer TG eich hun	6
Rhwydweithiau Wi-Fi heb eu diogelu	7
Storfa Cwmwl	7
Rhwydweithio Cymdeithasol	8
Sicrhau Preifatrwydd Ar-lein	10
Cefnogaeth arall i Aelodau NASUWT	12
Atodiad	13

Mae rhwydweithiau diwifr wedi gweddnewid y ffordd y gallwn ddefnyddio cyfrifiaduron a dyfeisiau symudol yn y cartref, yn y gweithle a phan fyddwn allan, gan gynnig hyblygrwydd i ni gyfathrebu gyda phobl eraill, i gael gafael ar wybodaeth, i brosesu data ac i wneud trafodion unrhyw amser o'r dydd a'r nos.



Mae cyfrifiaduron a nifer o ddyfeisiau eraill, gan gynnwys llechi (e.e. iPad), gliniaduron a ffonau clyfar, yn gallu cysylltu â'r we yn ddiwifr gan ddefnyddio rhwydweithiau Wi-Fi. Mae rhwydweithiau diwifr y cartref a'r swyddfa yn ei gwneud hi'n haws i ddefnyddio'r we ac anfon a derbyn e-byst mewn unrhyw ystafell yn yr adeilad ac hyd yn oed tu allan. Mae rhwydweithiau neu fannau poeth diwifr cyhoeddus yn galluogi unigolion hefyd i wneud eu gwaith yn unrhyw le, gan gynnwys mannau megis caffis, gwestai ac hyd yn oed ar y stryd. Mae ategion band eang symudol (y 'dongl') yn rhoi hyd yn oed fwy o hyblygrwydd i ni, gan adael i unigolion weithio ar-lein lle mae cysylltiad 3G neu 4G cellog.

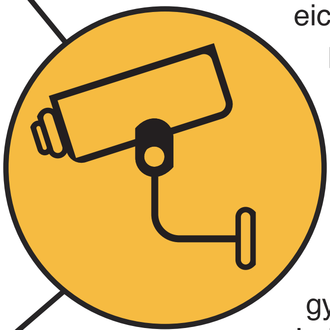
Fodd bynnag, mae materion pwysig yn ymwneud â'ch preifatrwydd a'ch diogelwch y mae angen i chi fel aelodau eu hystyried wrth ddefnyddio rhwydweithiau Wi-Fi ac wrth dderbyn, storio neu drosglwyddo data neu wybodaeth ar-lein.

Y risg i ddiogelwch sy'n gysylltiedig â defnyddio unrhyw system sydd wedi'i seilio ar y we neu sy'n defnyddio'r we yw y gallai pobl heb awdurdod dorri i mewn i'r hyn a wnewch ar-lein. Gallai hyn gynnwys cael gafael ar eich cyfrineiriau a darllen eich deunyddiau preifat a chyfrinachol..

Preifatrwydd

Mae'n hanfodol eich bod yn cynnal preifatrwydd pan fyddwch ar-lein er mwyn rhwystro unrhyw un rhag dwyn eich hunaniaeth neu'ch cofnodion personol, ac i atal ymddygiad twyllodrus.

Fodd bynnag, mae'n rhyfeddol o hawdd rhoi eich gwybodaeth bersonol i bobl eraill ar-lein heb wybod eich bod wedi gwneud hynny. Gallai hyn gael goblygiadau difrifol i chi, yn cynnwys dwyn eich hunaniaeth, colli arian, colli enw da, blacmel neu gribddeiliaeth.



Mae nifer o ysgolion/golegau'n defnyddio systemau TG i storio cofnodion staff a disgyblion. Bydd llawer o'r systemau hyn yn cynnwys gwybodaeth bersonol a sensitif am unigolion. Mae rhai cyflogwyr, er enghraifft, yn defnyddio systemau TG wedi'u lleoli yn y cwmwl i storio a rhoi mynediad i chi at wybodaeth sydd ar y gyflogres, gan gynnwys rhoi hysbysiadau am gyflog i staff ar ddiwedd bob mis. Mae ysgolion/colegau (sef 'rheolwyr data') yn gyfrifol am sicrhau bod data o'r fath yn cael eu rheoli'n ddiogel drwy unrhyw systemau TG y maent yn eu defnyddio ac maent yn gyfrifol hefyd am sicrhau diogelwch data personol a phreifat. Fodd bynnag, dylai aelodau fod yn glir hefyd ynglŷn â pha wybodaeth sydd wedi'i storio amdanynt neu sy'n cael ei drosglwyddo ar-lein a gweithredu'n briodol i sicrhau nad yw diogelwch a phreifatrwydd yr wybodaeth bersonol a sensitif amdanoch chi eich hun neu am bobl eraill yn cael ei beryglu.

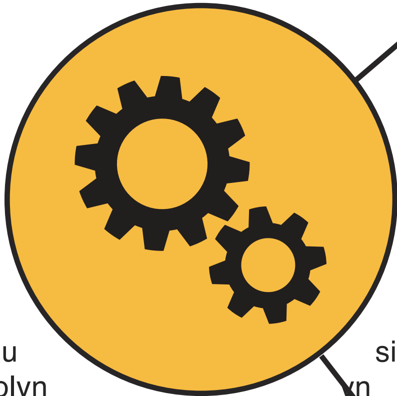
Pwysigrwydd Preifatrwydd

Lle bynnag y mae gwybodaeth yn cael ei storio, mae angen i unigolion a sefydliadau gofio pwysigrwydd preifatrwydd a diogelwch y data.

Mae Deddf Diogelu Data 1998 yn darparu fframwaith cyfreithiol o gyfrifoldebau ar sefydliadau (gan gynnwys ysgolion a cholegau) a chyflogwyr, a hawliau i unigolion (gan gynnwys athrawon) mewn perthynas â sicrhau preifatrwydd a chyfrinachedd. Mae'r Ddeddf yn gofyn i sefydliadau brosesu data personol yn deg ac yn gyfreithlon, ar sail wyth egwyddor (gwelwch yr Atodiad), i ddiogelu budd yr unigolion y mae eu data personol yn cael ei brosesu.

Mae ysgolion, colegau a sefydliadau eraill wedi'u diffinio o dan y Ddeddf fel 'rheolwyr data' a thrwy hynny maent yn gyfrifol am sicrhau diogelwch a chywirdeb y data personol sydd ganddynt neu y maent yn eu prosesu. Mae'r Ddeddf yn rhoi dyletswydd ar ysgolion a cholegau i gymryd camau priodol i atal prosesu data personol heb awdurdod neu'n anghyfreithlon ac i ddiogelu yn erbyn colli, dinistrio neu niweidio data personol yn ddamweiniol. Beth bynnag fo'r trefniadau neu'r dull o storio, prosesu neu drosglwyddo data personol, mae'r ysgol/coleg, fel y rheolydd data, yn gyfrifol am gydymffurfio â darpariaethau'r Ddeddf Diogelu Data.

Eich Cyd-gyfrifoldeb



Dylai aelodau gydnabod eu cyfrifoldeb i osgoi cyfathrebu, trosglwyddo, dileu neu bostio data personol am bobl eraill ar-lein yn anfwriadol.

Gallai unigolion dorri'r gyfraith wrth bostio ar-lein os ydynt yn postio gwybodaeth sy'n achosi camdriniaeth neu aflonyddwch i eraill. Gellir erlyn unigolion drwy'r llysoedd troseddol a gallent gael eu siwio am iawndal mewn llys sifil. Mewn agwedd amhersonol, lle mae unigolyn yn cynrychioli sefydliad (e.e. ysgol, coleg neu undeb llafur) dylai'r unigolyn a'u sefydliad gydymffurfio ag egwyddorion diogelu data'r Ddeddf Diogelu Data.

Risgiau i Ddiogelwch Data

Mae datblygiadau mewn technoleg wedi galluogi sefydliadau i brosesu mwy a mwy o ddata personol, a rhannu gwybodaeth yn haws. Er bod nifer o fanteision i hyn, mae hefyd yn achosi mwy o risgiau diogelwch. O'i roi yn syml, po fwyaf o gronfeydd data sy'n cael eu sefydlu a pho fwyaf o wybodaeth sy'n cael ei chyfnewid, y mwyaf yw'r risg y bydd rhywfaint o'r data'n cael ei golli, ei gamddefnyddio neu ei lygru.

Pryd bynnag y bydd gwybodaeth yn cael ei storio neu ei ledaenu gan ddefnyddio systemau TG a rhwydweithiau ar-lein, bydd risg i breifatrwydd a diogelwch data. Y risg i ddiogelwch sy'n gysylltiedig â defnyddio unrhyw system sydd wedi'i seilio ar y we neu sy'n defnyddio'r we yw y gallai pobl heb awdurdod efallai dorri i mewn i'r hyn yr ydych yn ei wneud ar-lein. Gallai hyn gynnwys cael gafael ar gyfrineiriau unigol a darllen deunyddiau preifat a chyfrinachol heb awdurdod.

Mae rhwydweithiau diwifr yn y cartref neu yn yr ysgol/coleg yn ei gwneud hi'n haws i ni ddefnyddio'r we ac anfon a derbyn e-byst. Mae rhwydweithiau neu fannau poeth diwifr cyhoeddus yn galluogi unigolion hefyd i wneud eu gwaith yn unrhyw le y dewisent. Fodd bynnag, dylid rhoi ystyriaeth wrth ddefnyddio rhwydweithiau diwifr sy'n gallu ei gwneud hi'n haws i hacwyr gael gafael ar ffeiliau preifat neu wybodaeth breifat neu'n haws i eraill fynd i mewn i'ch cysylltiad â'r we yn eich cartref neu yn yr ysgol/coleg mewn ffyrdd a allai fod yn niweidiol i chi'n bersonol neu'n broffesiynol.

Mewn rhai achosion, gallai dolenni at wefannau ffug sy'n cael eu hanfon ar yr ebost neu drwy gyfrifon cyfryngau cymdeithasol megis Facebook neu Twitter gael eu defnyddio hefyd i gael gafael ar wybodaeth bersonol, breifat a sensitif. Mae rhai sgamwyr hefyd yn defnyddio galwadau ffôn i ofyn i unigolion gadarnhau gwybodaeth amdanynt eu hunain er mwyn iddynt allu gwneud pethau twyllodrus a throseddol.

Cyfrifoldeb yr ysgol/coleg yw hi i sicrhau bod ganddynt systemau ar waith i sicrhau diogelwch yr holl ddata personol y maent yn ei gasglu ac yn ei ddal, lle bynnag y mae'r wybodaeth wedi'i storio – e.e. ar weinydd neu wedi'i gadw ar go bach. Dylai'r rheolydd data (yr ysgol/coleg) sicrhau'r canlynol o leiaf:

- mai dim ond pobl sydd wedi'u hawdurdodi sy'n gallu mynd i mewn i, newid, datgelu neu ddinistrio data personol;
- nad ydy'r bobl yma'n gweithredu y tu allan i gwmpas eu hawdurdod;
- os bydd data personol yn cael ei golli, ei addasu neu ei ddinistrio'n ddamweiniol, bod modd ei adfer i atal unrhyw niwed neu drallod i'r unigolion perthnasol.

Os bydd diogelwch data wedi'i dorri, mae gan yr ysgol/coleg gyfrifoldeb i roi gwybod am hyn i Swyddfa'r Comisiynydd Gwybodaeth.

Lle mae unigolyn yn drwgdybio bod rhywbeth wedi peryglu diogelwch data (p'un a yw'r data'n ddata personol iddyn nhw neu i rywun arall), dylid rhoi gwybod am hyn ar frys i'r unigolyn sy'n gyfrifol am faterion diogelu data.

Dylai aelodau NASUWT gysylltu â'r Undeb ar unwaith os ydynt yn credu bod eu data personol eu hunain wedi'i beryglu.

Gweithio o gartref

Dylai aelodau sy'n dewis gweithio gartref gydnabod mai eu cyfrifoldeb nhw yw hi i gael caniatâd gan eu cyflogwr cyn prosesu neu gadw data personol gartref, gan gynnwys data personol a sensitif sy'n ymwneud ag aelodau unigol o'r staff neu'r disgyblion. Mae hyn yn bwysig lle mae ffeiliau sy'n cynnwys data o'r fath yn cael eu cymryd allan o'r gweithle (e.e. ar gerdyn cof / co bach) neu lle'r eir i mewn iddynt ar-lein, p'un a ydych yn bwriadu cael gafael ar neu ddefnyddio unrhyw ddata a allai fod yn bersonol neu'n sensitif.

Bydd angen i aelodau gymryd rhagofalon digonol i sicrhau na all unrhyw drydydd parti sydd heb awdurdod, gan gynnwys aelodau eu teulu, eu ffrindiau neu bobl eraill, gael gafael ar ddata personol am y staff neu'r disgyblion. Dylai ffeiliau gael eu diogelu gan gyfrinair bob amser, a dylid cymryd camau hefyd i ddefnyddio dyfeisiau diogel, gan gynnwys storfa cyfrifiadur/dyfais, storfa Wi-Fi ddiogel a storfeydd cyfryngau (e.e. cardiau cof, co bach USB).

Gallai cyfnewid dyfeisiau storio data megis cardiau cof rhwng cyfrifiaduron a dyfeisiau'r gwaith neu'r cartref, gyfaddawdu diogelwch systemau TG yr ysgol/coleg hefyd a diogelwch eich system bersonol eich hun, yn arbennig os yw dyfeisiau data'n cynnwys maleiswedd neu firysau a allai gasglu neu ddinistrio data. Mae'n bwysig cofio bod colli data'n drosedd hefyd o dan y Ddeddf Diogelu Data. Byddai disgwyl i reolydd data (yr ysgol/coleg) a'r defnyddiwr data (yr athro/athrawes) esbonio'r amgylchiadau ar gyfer unrhyw golled a dangos bod cymryd data oddi ar y wefan yn gyfiawn a bod y risgiau sy'n gysylltiedig â gwneud hyn wedi'i reoli'n briodol.

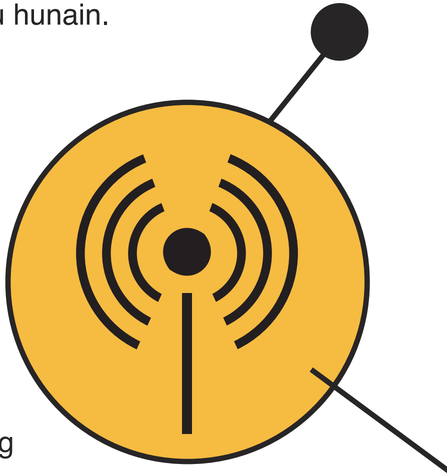
Defnyddio eich offer TG eich hun

Dylai aelodau osgoi defnyddio eu hoffer/dyfeisiau TG eu hunain (gan gynnwys cyfrifiaduron, llechi, ffonau clyfar, cardiau cof, ac ati), p'un a yw hynny yn y gweithle neu'n rhywle arall, i bwrpasau sy'n ymwneud â gwaith, heb ganiatâd ysgrifenedig gan y cyflogwr. Lle mae gofyn i aelodau ddefnyddio offer TG i bwrpasau gwaith, dylai'r cyflogwr ddarparu'r offer/dyfeisiau. Mae'n bwysig bod unrhyw ddyfeisiau a ddarperir gan y cyflogwr yn cael eu defnyddio yn gyfan gwbl yn unol â darpariaethau Polisi Defnydd Derbyniol y cyflogwr, ac ni ddylid eu defnyddio i'ch pwrpasau personol eich hun.

Mae'n bwysig cadw dyfeisiau a systemau sy'n ymwneud â gwaith ar wahân i ddyfeisiau a ddefnyddir i bwrpasau personol/preifat bob amser. Mae hyn yn golygu, er enghraifft, sicrhau bod gennych gyfrifiaduron/dyfeisiau annibynnol/unswydd i'ch gweithgareddau ar-lein personol eich hun.

Er bod defnyddio offer TG personol yn cael ei ganiatáu o fewn Polisi Defnydd Derbyniol y cyflogwr, bydd angen i ysgol/coleg sicrhau nad yw'r dyfeisiau y mae unigolyn yn bwriadu eu defnyddio'n cyfaddawdu diogelwch data o fewn yr ysgol/coleg. O ganlyniad felly, efallai y bydd gofyn i gyflogwr fonitro a gwirio'r defnydd o gyfrifiadur neu ddyfeisiau'r cyflogai unigol ei hun i sicrhau eu bod yn cydymffurfio â'r Polisi Defnydd Derbyniol. Gallai hyn gael goblygiadau i breifatrwydd unrhyw ddata, deunyddiau neu hanes ar-lein a allai gael eu hadnabod o ddefnydd unigolion o'u cyfrifiaduron/dyfeisiau eu hunain.

Rhwydweithiau Wi-Fi heb eu diogelu



Y brif risg i ddiogelwch sy'n gysylltiedig â defnyddio eich dyfais eich hun mewn mannau cyhoeddus yw'r posibilrwydd nad yw'r rhwydwaith Wi-Fi wedi'i ddiogelu, gan alluogi i bobl heb awdurdod dorri ar draws unrhyw beth yr ydych yn ei wneud ar-lein. Gallai hyn gynnwys cipio eich cyfrineiriau neu eich dogfennau/deunyddiau preifat a chyfrinachol. Mae rhwydweithiau Wi-Fi heb eu diogelu hefyd yn rhoi eich hunaniaeth mewn perygl o gael ei ganfod, gan gynnwys eich manylion ariannol neu fancio. Gallai risg godi i breifatrwydd a diogelwch unigolion os bydd y cysylltiad rhwng eu cyfrifiadur a'u ffôn clyfar a'r signal Wi-Fi heb ei amgryptio, neu os bydd rhywun yn creu man poeth Wi-Fi ffug sy'n honni bod yn gyfreithlon.

Lle defnyddir rhwydweithiau Wi-Fi heb eu diogelu yn ystod gwaith bob dydd, mae gan hyn hefyd y potensial i roi diogelwch data'r ysgol/coleg mewn perygl.

Storfa Cwmwl

Mae rhai ysgolion/colegau'n symud eu systemau TG o systemau storio data ffisegol i ddulliau storio ar-lein neu yn y cwmwl. Mae storfa cwmwl yn cyfeirio at storio data ar blatfformau ar-lein sydd wedi'u rheoli gan sefydliad arall. Yn aml iawn mae'r atebion yma'n cael eu defnyddio gan sefydliadau i arbed costau sy'n gysylltiedig â storio data, neu i wella hygyrchedd data neu i gadw copi wrth gefn o ddata i ddiogelu yn erbyn colli data. Fodd bynnag, mae storio data yn y cwmwl yn creu risgiau sydd â goblygiadau i athrawon unigol.

Nid oes y fath beth â system gwmwl gwbl ddiogel. Pryd bynnag y mae data'n cael ei storio ar y we, mae mewn perygl o ddioddef ymosodiad seiber neu o gael ei 'hacio', yn arbennig os nad yw data wedi'i amgryptio, neu lle nad yw'r dull o fynd i mewn i'r system (e.e. cyfrifiadur neu rwydwaith) yn ddiogel.

Gallai graddfa'r effaith o dorri diogelwch data fod yn uwch hefyd lle mae data wedi'i storio yn y cwmwl. Os bydd diogelwch platfform cwmwl yn cael ei beryglu, gallai'r holl ddata sydd wedi'i storio gael ei golli neu ei gyfaddawdu. Gallai'r mynediad at ddata sy'n cael ei storio yn y cwmwl gael ei effeithio hefyd os bydd gweinydd ar-lein yn methu neu os na ellir mynd i mewn iddo am ryw reswm. Gallai hyn gael goblygiadau difrifol ar reoli systemau a phrosesau'r ysgol/coleg o ddydd i ddydd.

Mae'r darparwr trydydd parti, nid yr ysgol/coleg, yn rheoli'r gwaith o gynnal a diogelu'r data sydd wedi'i storio yn y system gwmwl. Mae hyn yn golygu bod trydydd parti, yn ei hanfod, yn gallu mynd i mewn i ddata personol unigolion, gan greu haen ychwanegol o risg i breifatrwydd a diogelwch data.

Felly dylai ysgolion a cholegau ystyried yn ofalus pa ddata fyddai'n elwa o gael ei storio yn y cwmwl. Efallai nad yw storfa cwmwl yn ateb da i bob ffurf o ddata, yn enwedig os yw'r risgiau sy'n gysylltiedig â defnyddio atebion o'r fath yn methu cael eu rheoli'n effeithiol.

Dylai ysgolion a cholegau hefyd ystyried bod darparwyr storfeydd cwmwl eisiau prosesu'r data personol sydd wedi'i storio weithiau i'w pwrpasau marchnata uniongyrchol eu hunain. Mae hwn yn fater i'r ysgol/coleg fel y rheolydd data gytuno iddo neu beidio. Ond, mae'n rhaid i unigolion y cedwir eu data gan ddarparwr storfa cwmwl gael yr hawl i atal i'w data personol gael ei ddefnyddio i bwrpasau marchnata uniongyrchol. Mae gan ysgolion a cholegau ddyletswydd i esbonio i'r staff, y rhieni a/neu'r disgyblion pa ddata personol fydd yn cael ei ddal amdanynt, sut y bydd yn cael ei gasglu a'i storio, sut y bydd yn cael ei ddefnyddio a gan bwy, a pha hawliau sydd ganddynt ynglŷn â defnyddio eu data personol.

Dylai'r ysgol/coleg sicrhau ei fod yn gweithredu diwydrwydd dyladwy wrth ddethol darparwr gwasanaeth cwmwl er mwyn ateb eu dyletswydd o dan y Ddeddf Diogelu Data.

Rhwydweithio Cymdeithasol

Mae rhwydweithio cymdeithasol ar-lein yn rhan o fywyd pob dydd llawer o athrawon erbyn hyn. Mae gwefannau rhwydweithio cymdeithasol amrywiol yn offer gwerthfawr hefyd a ddefnyddir gan lawer o athrawon, ac yn cael eu hannog gan rai cyflogwyr a chyrff datblygiad proffesiynol. Fodd bynnag, mae defnyddio gwefannau rhwydweithio cymdeithasol yn cario rhywfaint o risg i breifatrwydd a diogelwch.

P'un a ydyw'r platfformau a'r fforymau rhwydweithio cymdeithasol megis Facebook, Twitter, TES, LinkedIn ac eraill yn cael eu defnyddio dim ond i gysylltu â phobl eraill, rhannu gwybodaeth, postio lluniau o gyfarfodydd, gwyliau neu ddigwyddiadau pwysig, mae hynny'n debygol o gynnwys cyfnewid o leiaf rhywfaint o wybodaeth bersonol amdanoch chi eich hun neu am bobl eraill a allai achosi risg i'ch preifatrwydd neu hyd yn oed eich diogelwch personol.

Mae'r rhan fwyaf o wefannau rhwydweithio cymdeithasol yn caniatáu i ddefnyddwyr osod gosodiadau preifatrwydd i reoli pa mor gyhoeddus neu breifat y bydd yr wybodaeth y maent yn ei phostio ar-lein. Cyn postio gwybodaeth neu luniau ar wefannau rhwydweithio cymdeithasol:

- gwiriwch y gosodiadau preifatrwydd a'u haddasu i sicrhau nad ydych yn risgio rhannu gwybodaeth amdanoch chi eich hun neu am bobl eraill (e.e. eich teulu, eich cydweithwyr ac ati) gyda phobl nad ydych eisiau ei rannu â nhw;
- adolygwch eich gosodiadau preifatrwydd yn rheolaidd;
- cofiwch, ar rai gwefannau rhwydweithio cymdeithasol, bydd pobl nad ydynt ar eich rhestr o 'ffrindiau' cymeradwy yn dal i allu gweld rhywfaint o'r wybodaeth a bostiwch ar-lein;
- defnyddiwch gyfrineiriau a mewngofnodion cryf i atal mynediad heb awdurdod i'ch cyfrifon rhwydweithio cymdeithasol a'ch gosodiadau preifatrwydd;
- dewiswch enw defnyddiwr nad yw'n cynnwys unrhyw wybodaeth bersonol;
- osgowch bostio gwybodaeth bersonol amdanoch chi eich hun – naill ai yn eich proffil neu yn eich pyst (e.e. rhifau ffôn, lluniau o'ch cartref, eich gweithle neu'ch ysgol, cyfeiriad cartref, pen-blwydd, cynlluniau gwyliau) – a allai eich gwneud yn agored i dwyll hunaniaeth, lladrad neu niwed;
- meddyliwch yn ofalus cyn postio gwybodaeth y gallai pobl eraill fynd i mewn iddo a'i ddefnyddio yn eich erbyn – er enghraifft, eich cyflogwr neu gyflogwr posibl, neu gydweithiwr, rhiant neu ddisgybl;
- gofynnwch am ganiatâd gan bobl eraill (yn arbennig gydweithwyr, rhieni a disgyblion), cyn llwytho eu lluniau neu eu gwybodaeth bersonol i fyny;
- cadwch gyfrifon rhwydweithio cymdeithasol ar wahân i'ch gwaith a'ch gweithgareddau personol ar-lein;
- byddwch yn ochelgar rhag sgamiau 'gwe-rwydo', gan gynnwys ceisiadau gan ffrindiau ffug a physt gan unigolion neu sefydliadau yn eich gwahodd i ymweld â thudalennau gwe neu wefannau eraill;
- gwnewch yn siŵr bod gennych feddalwedd gwrth-firws/gwrth-ysbïwedd effeithiol ac wedi'i ddiweddaru a mur gwarchod cyn i chi fynd ar-lein.

Sicrhau Preifatrwydd Ar-lein

Sicrhewch fod gennych bob amser feddalwedd gwrth-firws/gwrth-ysbïwedd effeithiol ac wedi'i ddiweddaru ar eich cyfrifiadur.

Defnyddiwch rwydweithiau Wi-Fi diogel yn unig, a sicrhewch fod eich rhwydwaith cartref wedi'i ddiogelu hefyd.

Peidiwch â gadael eich cyfrifiadur, eich ffôn clyfar neu'ch llechen heb neb yn edrych ar eu hôl mewn mannau cyhoeddus.

Os ydych yn defnyddio eich cyfrifiadur, eich ffôn clyfar neu'ch llechen mewn mannau cyhoeddus, cofiwch y bydd pobl eraill o'ch cwmpas sydd efallai'n gwylio'r hyn yr ydych yn ei wneud ar-lein.

Heblaw eich bod yn defnyddio gwefan ddiogel, peidiwch ag anfon neu dderbyn gwybodaeth breifat wrth ddefnyddio rhwydweithiau Wi-Fi cyhoeddus.

Os oes gennych chi un, defnyddiwch 'ddongl' neu ategyn tebyg sy'n rhoi cysylltiad diogel i chi.

Dim ond gwefannau diogel y dylech eu defnyddio wrth wneud trafodion ar-lein, gan gynnwys wrth fancio ar-lein, gwirio cofnodion gwybodaeth bersonol, neu wrth adolygu unrhyw wybodaeth breifat, sensitif neu gyfrinachol ar-lein.

Allgofnodwch o wefannau diogel gynted ag y byddwch wedi cwblhau trafodyn a chyn i chi allgofnodi neu ddiffodd eich cyfrifiadur/dyfais bob tro. Efallai na fydd cau'r ffenestr neu gau eich cyfrifiadur yn eich allgofnodi'n awtomatig o'r wefan yr ydych wedi ymweld â hi ac a allai wneud eich gwybodaeth yn hygyrch i rywun arall sydd efallai'n defnyddio'r un cyfrifiadur/dyfais.

Defnyddiwch gyfrineiriau cryf bob amser (cymysgedd o lythrennau bach a phriflythrennau a rhifau) a newidiwch eich cyfrineiriau'n rheolaidd. Ni ddylech byth ddatgelu eich cyfrinair i unrhyw un arall.

Cadwch gyfrineiriau a chodau Wi-Fi yn ddiogel fel nad yw pobl eraill yn gallu mynd i mewn iddynt neu eu defnyddio.

Gwiriwch pa ddata sy'n cael ei storio amdanoch, yn cynnwys data amdanoch chi gan ddefnyddio storfa cwmwl. Canfyddwch pa reolyddion sydd ar waith i sicrhau diogelwch a chywirdeb y data amdanoch chi.

Gwiriwch a allai'r wybodaeth a ddelir amdanoch chi gael ei ddefnyddio i bwrpasau marchnata uniongyrchol. Os oes gennych unrhyw bryderon, mae gennych yr hawl i atal eich gwybodaeth rhag cael ei chasglu neu ei phasio i sefydliadau eraill i bwrpas marchnata uniongyrchol.

Defnyddiwch beiriannau chwilio (e.e. Google, Bing) i chwilio am unrhyw wybodaeth sydd efallai wedi'i bostio ar-lein amdanoch chi. Cysylltwch â'r awdur, gweinyddwr y wefan neu ddarparwr y peiriant chwilio i dynnu unrhyw wybodaeth anghywir neu faleisus.

Peidiwch â defnyddio cyfeiriad e-bost gwaith at ddefnydd personol. Mae'n llawer gwell cael cyfeiriad e-bost preifat ar wahân at ddefnydd preifat. Lle mae gwybodaeth bersonol yn cael ei throsglwyddo gan ddefnyddio cyfeiriad ebost gwaith neu ar gyfrifiadur/ddyfais neu rwydwaith a ddarperir gan eich cyflogwr, gallai eich cyflogwr fynd i mewn iddo unrhyw bryd.

Defnyddiwch unrhyw gyfrifiaduron/dyfeisiau a roddir i chi gan eich cyflogwr yn unol â darpariaethau Polisi Defnydd Derbyniol y cyflogwr yn unig, ac nid at eich pwrpasau personol eich hun.

Cadwch ddyfeisiau a systemau sy'n ymwneud â gwaith ar wahân i ddyfeisiau a ddefnyddir i bwrpasau personol/preifat bob amser.

Osgowch gyfnewid perifferolion storio data rhwng cyfrifiaduron/dyfeisiau gwaith a phersonol, yn enwedig heb wneud gwiriad gwrth-firws priodol.

Peidiwch â defnyddio dolenni at wefannau ffug neu anhysbys, neu agor negeseuon e-bost o ffynonellau drwgdybus neu anhysbys.

Peidiwch â darparu gwybodaeth bersonol neu breifat mewn ymateb i alwadau ffôn digymell.

Gwiriwch osodiadau preifatrwydd a'u haddasu i sicrhau nad ydych mewn perygl o rannu gwybodaeth amdanoch chi eich hun neu am bobl eraill (e.e. eich teulu, eich cydweithwyr ac ati) gyda phobl nad ydych eisiau gwneud hynny â nhw.

Peidiwch â defnyddio rhwydweithiau Wi-Fi heb eu diogelu p'un a ydyw hynny yn eich cartref, swyddfa neu pan fyddwch allan.

Sicrhewch fod eich llwybrydd/ategyn diwifr/hyb yn ddiogel fel nad yw pobl eraill yn gallu cael gafael yn hawdd ar wybodaeth sensitif yr ydych efallai'n ei anfon neu'n ei dderbyn ar-lein. Mae hwn yn rhagofal pwysig pan fyddwch yn gweithio ac yn defnyddio eich offer eich hun i gyfathrebu ar-lein. Yn syml iawn, chwiliwch am rwydweithiau diwifr sydd ar gael, a bydd y rheiny sydd wedi'u sicrhau yn dangos symbol clo.

Gwiriwch nad yw eich dyfais yn cysylltu'n awtomatig at signalau Wi-Fi. Os yw eich dyfais wedi'i osod i gysylltu'n awtomatig at rwydweithiau Wi-Fi agored sydd ar gael, yna rydych mewn perygl o gysylltu'n awtomatig at rwydweithiau anhysbys a allai fod yn beryglus. Dylech ddiffodd y cysylltu-awtomatig drwy dudalen osodion y ddyfais.

Cefnogaeth arall i Aelodau NASUWT

Mae NASUWT yn cydnabod bod cyfrifiaduron a dyfeisiau, megis llechi (e.e. iPad) a ffonau clyfar, yn ddefnyddiol i alluogi unigolion a sefydliadau i gyfathrebu, cadw mewn cysylltiad a rhannu gwybodaeth. O ran cyflogaeth, gall athrawon elwa'n aml iawn o allu rheoli eu gwaith mewn ffordd ac ar amser sy'n addas iddyn nhw. Ond, mae perygl hefyd y gallai hyblygrwydd o'r fath gynyddu'r llwyth gwaith ac y gallai unigolion wynebu gofynion afrealistig ac afresymol.

NASUWT yw'r unig undeb sy'n ystyried gweithredu diwydiannol i amddiffyn athrawon a phrifathrawon rhag llwyth gwaith gormodol sy'n gysylltiedig â defnyddio systemau e-bost a systemau cyfathrebu ar-lein eraill.

I gael rhagor o wybodaeth am weithredu diwydiannol NASUWT, ewch i www.nasuwt.org.uk/IndustrialAction.

Lle bynnag y bydd aelodau'n wynebu problemau neu bryderon ynglŷn â defnyddio data personol, dylent gysylltu â NASUWT i gael cymorth a chyngor.

NASUWT CYMRU
Undeb yr Athrawon The Teachers' Union

E-bost: rc-wales-cymru@mail.nasuwt.org.uk
Ffôn: 029 2054 6080

ATODIAD

Deddf Diogelu Data 1998 – Wyth Egwyddor Diogelu Data

1. Prosesu data personol yn deg ac yn gyfreithlon.

2. Casglu data personol dim ond at ddiben neu ddibenion penodol a chyfreithlon, a pheidio prosesu'r data ymhellach mewn unrhyw ffordd sy'n anghydnaws â'r diben hwnnw neu'r dibenion hynny.

3. Sicrhau fod data personol yn ddigonol, yn berthnasol ac nid yn ormodol o ran diben neu ddibenion eu prosesu.

4. Sicrhau fod data personol yn gywir a, lle bo angen, yn cael ei ddiweddaru.

5. Peidio â chadw data personol a brosesir at unrhyw ddiben neu ddibenion am gyfnod hirach nag sydd ei angen ar gyfer y diben hwnnw neu'r dibenion hynny.

6. Prosesu data personol yn unol â hawliau gwrthrychau'r data o dan y Ddeddf.

7. Cymryd camau technegol a threfniadol priodol yn erbyn prosesu data personol heb awdurdod neu'n anghyfreithlon ac yn erbyn colli, dinistrio neu niweidio data personol yn ddamweiniol.

8. Peidio â throsglwyddo data personol i wlad neu diriogaeth y tu allan i'r Ardal Economaidd Ewropeaidd oni bai bod y wlad neu'r diriogaeth honno'n sicrhau lefel ddigonol o ddiogelwch i hawliau a rhyddid gwrthrychau'r data mewn perthynas â phrosesu data personol.

NASUWT CYMRU
Undeb yr Athrawon
The Teachers' Union

16/07064 Cymru