



Llywodraeth Cymru
Welsh Government

Canllawiau ar ddiogelu gwybodaeth i ysgolion



Canllawiau

Dogfen ganllawiau: rhif 206/2016

Dyddiad cyhoeddi: Awst 2016

Yn disodli dogfen ganllawiau: rhif 186/2015

Canllawiau ar ddiogelu gwybodaeth i ysgolion

Cynulleidfa

Staff, llywodraethwyr a dysgwyr ysgolion a gynhelir gan gynnwys unedau cyfeirio disgyblion.

Trosolwg

Nod y ddogfen hon yw rhoi cyngor a chanllawiau i ysgolion ynglŷn â chadw gwybodaeth ar blatfform Hwb (sy'n cynnwys Microsoft Office 365).

Camau i'w cymryd

Dim – er gwybodaeth yn unig.

Rhagor o wybodaeth

Dylid cyfeirio ymholiadau am y ddogfen hon at:

Yr Uned Dysgu Digidol

Y Gyfarwyddiaeth Gweithrediadau

Llywodraeth Cymru

Parc Cathays

Caerdydd

CF10 3NQ

Ffôn: 0845 010 4400 (ymholiadau yn Gymraeg)

0845 010 3300 (ymholiadau yn Saesneg)

e-bost: hwb@cymru.gsi.gov.uk

Copïau ychwanegol

Mae'r ddogfen hon ar gael o wefan Llywodraeth Cymru yn

www.llyw.cymru/addysgasiliau

Cynnwys

1.	Cyflwyniad	2
2.	Diogelu gwybodaeth	3
3.	Data personol	4
4.	Dosbarthu data	5
5.	Cyngor cyffredinol	6
6.	Hwb	7
7.	Hwb+	8
8.	HwbCloud	9
	Atodiad A: Diffiniadau diogelu data	14
	Atodiad B: Crynodeb o reolaethau HwbCloud	15

1. Cyflwyniad

Hwb yw adnodd dysgu digidol Llywodraeth Cymru ar gyfer ysgolion.

Mae'r diagram isod yn dangos gwahanol agweddau Hwb.



Hwb⁺



Mae'r ddogfen hon yn disgrifio'r rheolaethau sydd ar gael ar draws yr ystod o offer digidol yn Hwb a sut y gellir defnyddio'r offer hyn i alluogi ysgolion i gynnal diogelwch y wybodaeth y maent yn ei defnyddio.

Mae'r canllawiau a roddir yn gyffredinol eu natur ond maent yn adlewyrchu defnydd ysgol nodweddiadol yn seiliedig ar wybodaeth o gyfarfodydd ag ystod o randdeiliaid gan gynnwys athrawon, staff cymorth ac awdurdodau lleol.

2. Diogelu gwybodaeth

Bwriad diogelu gwybodaeth yw cynnal y nodweddion canlynol:

- Cyfrinachedd – sicrhau bod gwybodaeth yn aros yn gyfrinachol;
- Cywirdeb – sicrhau cywirdeb gwybodaeth; ac
- Argaeledd – sicrhau y gellir cael gafael ar wybodaeth pan fydd ei hangen.

Yn ogystal â'r priodoleddau allweddol hyn, ceir sefyllfaoedd lle bydd nodweddion eraill yn bwysig, er enghraifft: atebolrwydd, arddel gwybodaeth a dibynadwyedd.

3. Data personol

Data personol yw gwybodaeth am unigolion y gellir eu hadnabod, ac mae'r Ddeddf Diogelu Data (y Ddeddf) yn diffinio'r gofynion cyfreithiol sy'n berthnasol i'r defnydd o ddata personol.

Mae diffiniad y Ddeddf o ddata personol wedi'i gynnwys yn Atodiad A.

Mae'r rhagofalon y dylid eu cymryd yn berthnasol waeth pa fath o gyfrwng sydd dan sylw. Er enghraifft, gall mesurau diogelu fod yn ofynnol ar gyfer pob un o'r isod os ydynt yn cynnwys data personol:

- e-byst;
- lluniau;
- dogfennau electronig; a
- nodiadau a ysgrifennwyd â llaw.

Mae'r canllawiau yn y ddogfen hon yn gyfyngedig i'r rheolaethau sy'n berthnasol i fathau electronig o ddata. Os yw'r wybodaeth yn cael ei hargraffu yna mae'n rhaid ei diogelu o hyd; dylai'r gweithdrefnau fod yn gyson â'r rhai sy'n berthnasol i ddogfennau electronig.

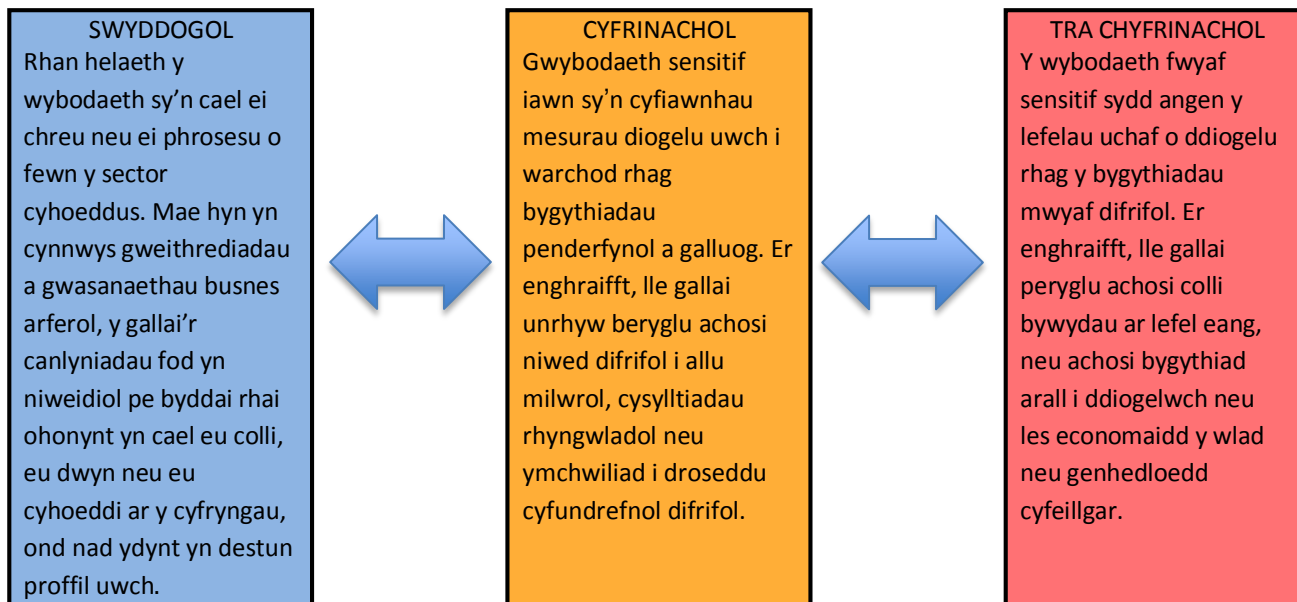
The Information Commissioner's Office (ICO) publishes guidance and codes of practice applicable to data protection and personal data on their website¹.

¹ www.ico.org.uk

4. Dosbarthu data

Bu i gynllun dosbarthu'r Llywodraeth newid ym mis Ebrill 2014 o gynllun marcio er diogelwch a oedd yn defnyddio pum categori (DIOGELU, CYFYNGEDIG, CUDD, CYFRINACHOL a TRA CHYFRINACHOL) i'r cynllun presennol a chanddo dri chategori (SWYDDOGOL, CYFRINACHOL a TRA CHYFRINACHOL).

Diffinnir y categorïau newydd fel a ganlyn:



Bydd gwybodaeth a gaiff ei phrosesu o fewn amgylchedd yr ysgol yn perthyn i'r categori SWYDDOGOL.

Ar gyfer data SWYDDOGOL dylai'r canlyniadau diogelu gwybodaeth:

- warchod rhag peryglu bwriadol gan ymosodiad awtomataidd neu fanteisgar; a
- cheisio canfod achos o beryglu gwirioneddol neu ymgais i beryglu ac ymateb iddo.

Mae'r manylion llawn ar gael yn nogfennau perthnasol Swyddfa'r Cabinet².

² <https://www.gov.uk/government/publications/government-security-classifications>

5. Cyngor cyffredinol

Dylai pob defnyddiwr (staff ysgolion a dysgwyr) ddilyn rheolau diogelwch cyffredinol sylfaenol; yn gyffredinol, mae'r rhain yn gymwys i unrhyw system TG ac yn cynnwys:

- peidiwch byth â gadael i unrhyw un arall ddefnyddio eich cyfrif Hwb;
- peidiwch byth â defnyddio cyfrif Hwb rhywun arall;
- byddwch yn ofalus wrth ddefnyddio eich cyfrif Hwb mewn man cyhoeddus – gwnewch yn siŵr na ellir eich gwyllo yn ei ddefnyddio, yn enwedig wrth ichi gofnodi eich cyfrinair;
- peidiwch â defnyddio eich cyfrif Hwb at ddibenion ar wahân i fusnes sy'n ymwneud â'r ysgol;
- gwnewch yn siŵr bob amser fod manylion derbynnydd yr e-bost yn gywir cyn ei anfon;
- rhowch wybod bob amser am bryderon ynghylch defnydd anaddas – dylid dilyn gweithdrefnau lleol fel y bo angen; ac
- osgowch ddefnyddio dyfeisiau / systemau cyhoeddus, personol neu rai a rennir ar gyfer data sensitif neu bersonol.

Bydd defnyddio dyfeisiau personol, y cyfeirir ato'n aml fel 'dod â'ch dyfais eich hun' ('Bring Your Own Device'/BYOD), bron yn bendant yn cyflwyno risgiau i'r wybodaeth a gaiff ei phrosesu arnynt; penderfyniad rheoli risg i bob ysgol yw hwn. Mae'r ICO wedi cyhoeddi canllawiau penodol ynghylch dod â'ch dyfais eich hun a diogelu data .

Ar hyn o bryd nid yw Hwb wedi'i ffurfweddu i reoli na gwirio'r dyfeisiau sy'n cael mynediad i Hwb; yn hytrach, dibynnir ar ddefnyddwyr i ddilyn y polisiau lleol sy'n berthnasol iddynt.

6. Hwb

Hwb yw'r llwyfan dysgu digidol a ariennir yn ganolog, â'r nod o ddarparu mynediad i ystod o gynnwys ac offer digidol.



Yn ogystal â darparu mynediad i adnodd ehangach Hwb, mae hefyd yn borth i wasanaethau cynnwys ychwanegol, a cheir enghreifftiau o'r rhain isod:



Dyluniwyd Hwb yn bennaf i storio cynnwys addysgol y gellir ei rannu ag unrhyw ddefnyddiwr Hwb arall.

Er mai dim ond defnyddwyr Hwb cofrestredig sy'n gallu cael mynediad i blatfform Hwb, nid ar gyfer storio data sensitif y'i bwriadwyd. Pan fydd angen i ysgolion ymdrin â data sensitif, dylid gwneud hyn trwy gyfrwng HwbCloud fel yr amlinellir isod.

7. Hwb+

Hwb+ yw'r amgylchedd dysgu rhithiwr a gynlluniwyd ac a grëwyd i ddarparu amgylchedd dysgu ar-lein diogel i athrawon a dysgwyr ac sy'n galluogi cydweithredu gan ddefnyddio adnoddau digidol.



Nod pennaf Hwb+ yw ei ddefnyddio ar gyfer gweithgarwch addysgu mewn ysgolion o ddydd i ddydd, lle gellir cynnwys data personol cyffredinol perthnasol, yn yr un modd ag y byddai data personol yn cael eu defnyddio yn yr ystafell ddosbarth.

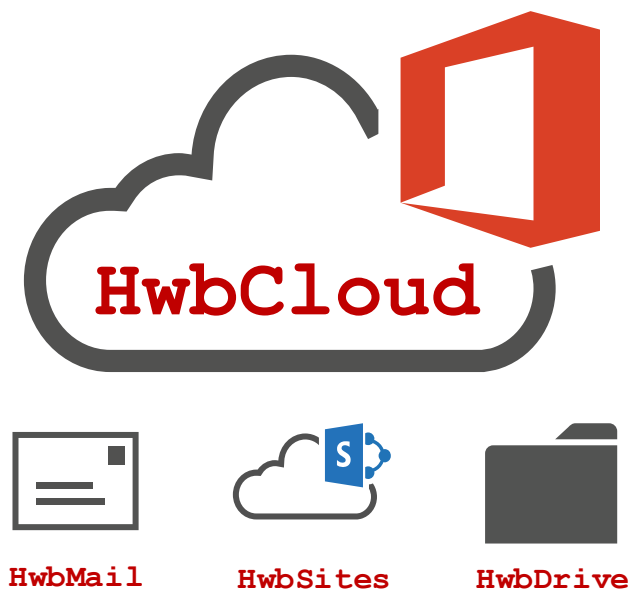
Er mai dim ond defnyddwyr cofrestredig Hwb sy'n gallu cael mynediad i Hwb+, nid ar gyfer storio data sensitif y'i bwriadwyd. Dylid gwneud hyn trwy gyfrwng HwbCloud fel yr amlinellir isod.

8. HwbCloud

HwbCloud yw'r arf mwyaf addas ar gyfer cyfnewid a storio gwybodaeth a dogfennau rheoli, gan gynnwys gwybodaeth am staff a dysgwyr.

Darperir y nodweddion yn HwbCloud gan Microsoft Office 365 ac felly mae'n elwa yn sgil y rheolaethau sydd wedi'u hymgorffori yn y gwasanaeth gan Microsoft.

Mae'r diagram isod yn dangos y gwasanaethau sydd ar gael yn HwbCloud ar hyn o bryd.



8.1 Office 365

Mae adnodd Office 365 Microsoft yn seiliedig ar set graidd o reolaethau sy'n ei wneud yn addas ar gyfer prosesu data SWYDDOGOL a phersonol. Cydnabuwyd hyn yn ffurfiol drwy:

- ardystio hyd at safonau diogelu gwybodaeth rhyngwladol;
- achredu ar draws llywodraethau; ac
- archwiliadau annibynnol sy'n parhau.

Mae Office 365 yn cynnig sawl opsiwn i ddefnyddwyr storio a rhannu gwybodaeth. Mae'r dewisiadau sydd ar gael yn amrywio o opsiynau hynod o hyblyg a chyfleus, i opsiynau diogel sy'n defnyddio amgryptio i roi sicrwydd y bydd y data'n aros yn gyfrinachol.

Mae Llywodraeth Cymru wedi adolygu'r opsiynau diogelwch sydd ar gael yn Office 365 ac wedi ffurfweddu HwbCloud â'r nod o ddarparu amgylchedd diogel sy'n addas ar gyfer y sefyllfaoedd defnydd nodweddiadol mewn ysgolion.

Nodyn: Mae effeithiolrwydd y rheolaethau yn HwbCloud yn gwbl ddibynnol ar fodolaeth polisïau a gweithdrefnau lleol addas. Mae angen i holl ddefnyddwyr HwbCloud fod yn ymwybodol o'r rhain a deall goblygiadau peidio â glynu at arferion gwaith diogel.

8.2 Diogelwch HwbCloud

Er na fydd angen i'r mwyafrif o ddefnyddwyr gyrchu neu gyfnewid gwybodaeth sensitif, cydnabyddir y bydd rhai defnyddwyr yn rheolaidd yn cyrchu gwybodaeth fwy sensitif sy'n cyfiawnhau lefel uwch o ddiogelu; felly, mae gwahanol lefelau o reolaeth ar gael.

Yn y ddogfen hon cyfeirir at y rheolaethau fel rhai safonol ac uwch – bydd holl ddefnyddwyr Hwb yn elwa yn sgil y rheolaethau safonol, tra bydd gofyn cael penderfyniad ffurfweddu penodol er mwyn defnyddio'r rheolaethau uwch, ac efallai y bydd gofyn i ddefnyddwyr ddewis yr opsiynau addas wrth storio neu anfon gwybodaeth.

Ar gyfer data personol, penderfyniad rheolwr y data fydd pryd i ddefnyddio rheolaethau uwch; mewn ysgolion, y pennaeth fydd y person hwn fel arfer. Fel y nodwyd yn gynharach yn y ddogfen hon, ceir cyngor ar wefan yr ICO i gynorthwyo penaethiaid i benderfynu pa lefel o reolaeth sy'n ofynnol.

Mae'r adrannau canlynol yn rhoi canllawiau ar sut y gellir defnyddio'r gwahanol raglenni o fewn Hwb365 i ymdrin â data personol yn ddiogel.

Mae'r tabl canlynol yn dangos sefyllfaoedd defnydd nodweddiadol. Mae'n debygol y bydd yna resymau dilys dros wyro oddi wrth y model hwn gan ddibynnu ar amgylchiadau penodol ysgol; bydd unrhyw wyro o'r fath yn benderfyniad rheoli risg lleol.

Nodyn: Rhaid defnyddio'r tabl hwn ar y cyd â'r siart lif dewis rheolaeth (a geir yn Atodiad B) sy'n gymwys i bob agwedd ar HwbCloud.

Sefyllfaoedd	Rheolaethau Safonol HwbCloud	Rheolaethau Uwch HwbCloud
Gwybodaeth ysgol gyffredinol gan gynnwys data cyrhaeddiad o SIMS, nad yw'n cynnwys gwybodaeth sensitif.	😊	😊
Gwybodaeth am ddysgwyr o'r system gwybodaeth reoli; er enghraifft, i'w defnyddio ar dripiâu ysgolion. Pan fydd gwybodaeth feddygol sensitif wedi'i chynnwys, dylid ystyried diogelwch uwch. Gall data AAA yn aml gynnwys gwybodaeth sensitif; dylid gwneud penderfyniad lleol yn seiliedig ar gyd-destun a chynnwys y data er mwyn pennu a ellir cyfiawnhau rheolaethau uwch.	😐	😊
Mae ymchwiliadau diogelwch plant yn tueddu i fod yn sensitif eu natur ac angen cyfrinachedd; bydd hyn fel arfer yn golygu bod angen rheolaethau uwch.	😞	😊

8.2.1 HwbMail

HwbMail yw'r system e-bost a ddarperir ar gyfer holl ddefnyddwyr Hwb. Mae'n system e-bost sy'n seiliedig ar safonau ac sy'n manteisio yn sgil nifer o opsiynau ffurfweddu a all ddarparu mesurau diogelu cadarn.

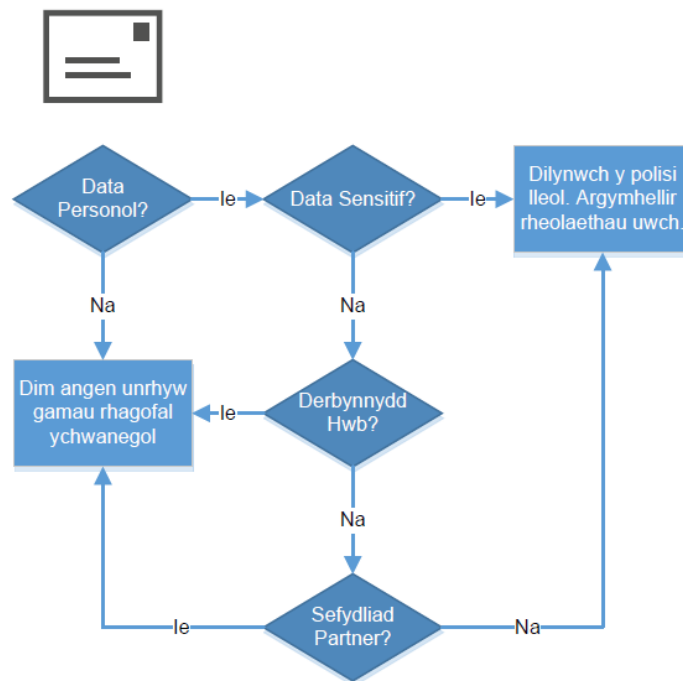
Mae ffurfweddiad diofyn HwbMail yn darparu ffordd ddiogel o anfon e-byst rhwng defnyddwyr HwbMail yn ogystal â rhai sefydliadau partner; mae'r rhestr gyfredol o sefydliadau partner sydd wedi'u dilysu ar gael ar [Hwb](#).

Mae'r rhestr o sefydliadau partner sydd wedi'u ffurfweddu i dderbyn e-byst diogel o Hwb wedi'i sefydlu ar y cyd â'r awdurdodau lleol a'r consortia addysg rhanbarthol.

Nodyn: Hyd nes bod sefydliad partner wedi'i ddilysu, dylid tybio na fydd e-byst yn ddiogel a dylid ystyried defnyddio rheolaethau uwch.

Mae gan HwbMail opsiynau ychwanegol ar gyfer amgryptio e-byst sensitif; dylid gofyn am ragor o ganllawiau gan eich pennaeth neu swyddog diogelu gwybodaeth eich awdurdod lleol os oes angen.

Mae'r siart lif isod yn rhoi cynrychiolaeth ar ffurf graffig o'r broses a argymhellir er mwyn penderfynu ar y dull amgryptio addas ar gyfer e-byst sy'n cynnwys data personol. Gellir defnyddio proses debyg ar gyfer mathau eraill o ddata sensitif.



8.2.2 HwbSites

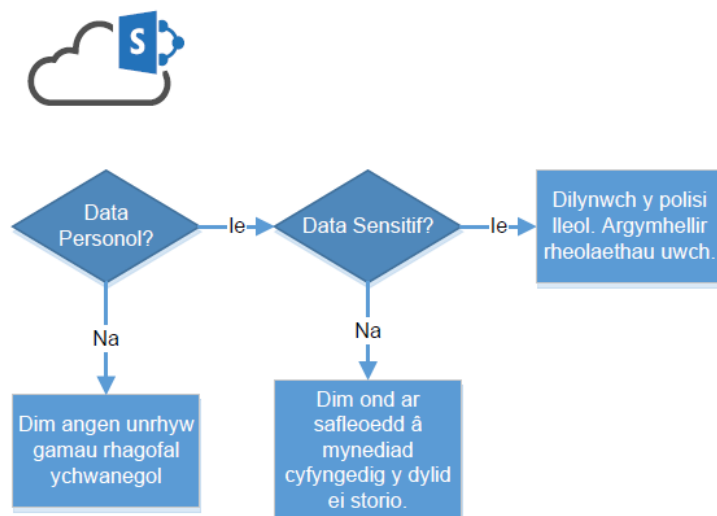
Mae HwbSites yn safleoedd gwaith ar-lein â'r nod o hwyluso rhannu gwybodaeth rhwng grwpiau o ddefnyddwyr a ddiffiniwyd yn ffurfiol.

Yn sgil natur gydweithredol HwbSites, dylid bod yn ofalus wrth storio data sensitif yn yr ardaloedd hyn. Gellir creu safleoedd penodol i gydweithredu'n ddiogel â data sensitif er mwyn helpu i sicrhau:

- bod mynediad yn cael ei gyfyngu i'r rhai sydd angen gwybod y wybodaeth yn unig; a
- diogelwch uwch i ddogfennau er mwyn lleihau'r risg o ryddhau gwybodaeth yn ddamweiniol.

Nodyn: Bydd y lefel uwch o ddiogelwch ar gyfer dogfennau yn golygu bod angen defnyddio'r fersiwn bwrdd gwaith o Microsoft Office i greu a golygu dogfennau.

I staff sydd â mynediad rheolaidd i'r data mwyaf sensitif, mae rheolaethau dilysu ychwanegol ar gael a dylid eu hystyried (er mwyn atal ymosodiadau ar sail cyfrineiriau).



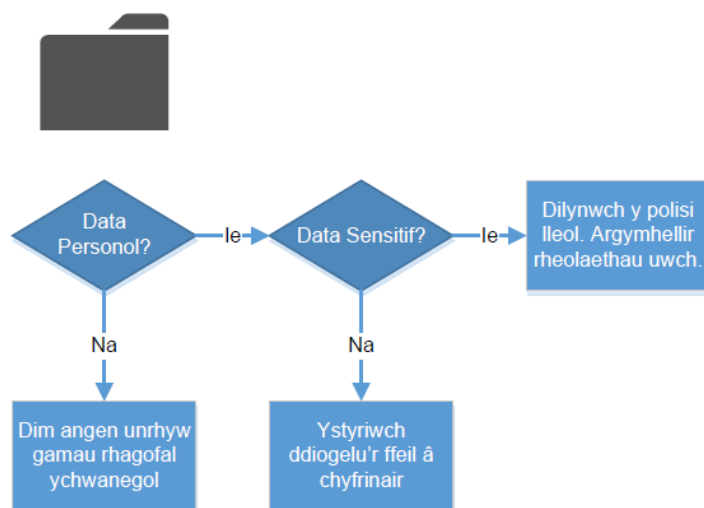
8.2.3 HwbDrive

HwbDrive yw'r ardal storio ffeiliau ar-lein bersonol ar gyfer defnyddwyr Hwb.

Os nad oes angen i lawer o ddefnyddwyr allu cyrchu dogfen gellir diogelu ffeiliau unigol â chyfrinair, a all fod yn ffordd effeithiol o sicrhau mai dim ond y defnyddiwr gwreiddiol sy'n gallu cyrchu'r cynnwys.

Ar gyfer data sy'n hynod o sensitif, diogelu ffeiliau unigol â chyfrinair yw'r dull rheoli mwyaf addas i roi sicrwydd o gyfrinachedd. Mewn sefyllfaoedd o'r fath dylid ceisio cyngor am gymhlethdod, hyd a dosbarthiad y cyfrinair.

Nodyn: Ar hyn o bryd dim ond ar y fersiwn bwrdd gwaith o Microsoft Office y mae diogelu â chyfrinair ar gael.



Atodiad A: Diffiniadau diogelu data

Mae Deddf Diogelu Data 1998 (y Ddeddf) yn diffinio data personol fel:

‘Data sy’n ymwneud ag unigolyn byw y gellir ei adnabod:

- a) o’r data hynny, neu;
- b) o’r data hynny a gwybodaeth arall sydd ym meddiant, neu sy’n debygol o ddod i feddiant, y rheolydd data,

ac yn cynnwys unrhyw farn am unigolyn ac unrhyw arwydd o fwriadau’r rheolydd data neu unrhyw berson arall mewn cysylltiad â’r unigolyn’

Mae’r Ddeddf yn diffinio data personol sensitif fel:

‘Yn cynnwys gwybodaeth sy’n ymwneud â:

- a) hil neu darddiad ethnig pwnc y data;
- b) ei safbwyntiau gwleidyddol,
- c) ei gredoau crefyddol neu gredoau eraill o natur debyg,
- d) a yw’n aelod o undeb llafur,
- e) ei gyflwr neu iechyd corfforol neu feddyliol,
- f) ei fywyd rhywiol,
- g) a yw wedi cyflawni neu honiad o gyflawni unrhyw drosedd neu
- h) unrhyw achosion ar gyfer unrhyw drosedd a gyflawnwyd neu a honnwyd a gyflawnwyd ganddo, canlyniad achos o’r fath neu ddedfryd unrhyw lys mewn achos o’r fath.’

Atodiad B: Crynodeb o reolaethau HwbCloud

Mae'r atodiad hwn yn crynhoi'r rheolaethau sydd ar gael yn HwbCloud.

B1 HwbMail

B1.1 STARTTLS Gorfodol

Caiff STARTTLS Gorfodol ei ffurfweddu gan dîm gweinyddol HwbCloud ac mae'n darparu gwasanaeth amgryptio e-byst wrth iddynt gael eu trosglwyddo drwy TLS ar gyfer e-byst a anfonir rhwng HwbCloud a sefydliadau partner sydd wedi'u dilysu.

Nid oes angen i'r defnyddiwr wneud dim byd; mae'n digwydd yn dryloyw gan ddilyn rheolau a ddiffiniwyd ymlaen llaw.

Bydd e-byst rhwng cyfrifon HwbMail yn cael eu hamgryptio gan ddefnyddio TLS yn rhan o ffurfweddiad diofyn Microsoft Office 365.

B1.2 S/MIME

Gall S/MIME gynnig dull o amgryptio e-byst wrth iddynt gael eu trosglwyddo a phan maent yn llonydd.

Mae hwn yn opsiwn sydd ar gael i unrhyw ddefnyddiwr Hwb; gellir ei ffurfweddu'n lleol ac ni fydd angen i dîm gweinyddol HwbCloud wneud unrhyw newidiadau i HwbCloud.

Rhaid i ddefnyddwyr sydd â S/MIME ddewis amgryptio e-byst yn Outlook (fel arall fe anfonir yr e-bost yn y dull arferol).

B1.3 Amgryptio Negeseuon Hwb (HME)

Mae Amgryptio Negeseuon Hwb yn ffordd o anfon e-byst fel bod y derbynnydd yn cyrchu'r cynnwys trwy gyfrwng porth diogel. Mae'n amgryptio e-byst wrth iddynt gael eu trosglwyddo ac oherwydd nad yw'r e-bost yn gadael y porth nid yw'n cael ei storio ar ddyfais y derbynnydd yn yr un modd ag e-bost arferol. Nid yw e-byst yn cael eu hamgryptio yn ffolder eitemau a anfonwyd yr anfonwr.

Mae Amgryptio Negeseuon Hwb wedi'i gyflunio i weithio'n awtomatig os yw defnyddiwr yn cynnwys y geiriau allweddol 'post diogel' neu 'secure mail' yn llinell bwnc yr e-bost.

Cyfeiriwch at ganllaw defnyddwyr Amgryptio Negeseuon Hwb ar Hwb am ragor o wybodaeth.

B2 HwbSites

Mae tîm Hwb wedi diffinio'r lefelau canlynol ar gyfer cyfuno rheolaethau uwch ar gyfer HwbSites. Disgrifir MFA ac IRM yn yr adrannau dilynol.

Disgwylir y defnyddir Lefel 3 ar gyfer mwyafrif HwbSites, gyda Lefelau 1 a 2 yn addas ar gyfer data personol gan ddibynnu ar ba mor sensitif yw'r wybodaeth.

Lefel	MFA	IRM	Rhannu	Nifer Disgwyliedig o Ddefnyddwyr
1	Oes	Oes	Na	Ychydig
2	Oes	Nac oes	Na	Ychydig
3	Nac oes	Nac oes	Na	Llawer
4	Nac oes	Nac oes	Ie	Ychydig

B2.1 Dilysu Aml-Ffactor (Multi-Factor Authentication/MFA)

Mae MFA yn HwbCloud wedi'i ffurfweddu fel y gellir ei gwneud yn ofynnol i ddefnyddwyr ddefnyddio cod o'r ap Azure Authenticator yn ogystal â'u henw defnyddiwr a'u cyfrinair.

Caiff yr ap Azure Authenticator ei osod ar ffôn clyfar a bydd yn helpu i atal ymosodiadau sy'n seiliedig ar gyfrineiriau, megis dyfalu cyfrinair neu wyllo person yn cofnodi cyfrinair.

Er mwyn i MFA fod yn effeithiol tybir na fydd staff a chanddynt fynediad i ddata sensitif yn rhannu eu ffonau clyfar ag eraill nac yn eu gadael heb eu cloi.

Nodyn: Er bod gan MFA opsiynau eraill yn Office 365, mae tîm Hwb wedi asesu mai ap Azure Authenticator yw'r unig opsiwn addas ar gyfer HwbCloud.

B2.2 Rheoli Hawliau Gwybodaeth (IRM)

Yn HwbCloud mae IRM yn fath ar reoli hawliau digidol a grëwyd gan Microsoft i ddarparu dull rheoli ychwanegol ar gyfer hawliau mynediad i ddogfennau, sy'n 'teithio' gyda'r ddogfen.

Yn HwbCloud mae'r defnydd o IRM wedi'i gyfyngu ar hyn o bryd i ategu rheolaethau mynediad presennol y rhwydwaith.

Bydd dogfen HwbCloud y mae IRM wedi'i chymhwyso iddi yn golygu bod angen i ddefnyddiwr ddarparu ei fanylion er mwyn cyrchu'r ddogfen, hyd yn oed pan fydd yn cyrchu'r ddogfen oddi allan i'r amgylchedd ar-lein.

B3 HwbDrive

B3.1 Dilysu Aml-Ffactor (Multi-Factor Authentication/MFA)

Gall HwbDrive fanteisio yn sgil MFA yn yr un modd â HwbSites; gweler yr adran berthnasol am ragor o wybodaeth.

B3.2 Diogelu â Chyfrinair ar Lefel Dogfen

Gellir defnyddio nodwedd diogelu â chyfrinair cynhenid Microsoft Office i ddiogelu dogfennau sy'n cynnwys data sensitif.