**Polisi Tor Diogelwch Data**

**Prifysgol Cymru Y Drindod Dewi Sant**

Cynnwys

[1. Rhagarweiniad 3](#_Toc196309852)

[2. Diffiniadau 3](#_Toc196309853)

[3. Pwrpas y polisi hwn 3](#_Toc196309854)

[4. Hysbysu am dor diogelwch data personol 4](#_Toc196309855)

[5. Rheoli achosion o dorri 4](#_Toc196309856)

[6. Achosion o dorri diogelwch data personol yn sgil digwyddiadau seiberddiogelwch 6](#_Toc196309857)

[7. Gwerthuso a ‘gwersi a ddysgwyd’ 6](#_Toc196309858)

# Rhagarweiniad

* 1. Mae Grŵp Prifysgol Cymru Y Drindod Dewi Sant a Phrifysgol Cymru (“y Brifysgol”) yn casglu, prosesu a chadw data er mwyn cyflawni eu hamcanion gweithredol a strategol ac i gefnogi eu swyddogaethau busnes.
	2. Wrth brosesu data personol, mae gan y Brifysgol rwymedigaeth gyfreithiol i sicrhau ei bod yn cydymffurfio â’r gofynion a wnaed yn Rheoliad Cyffredinol y DU ar Ddiogelu Data (GDPR y DU), Deddf Diogelu Data 2018 (DPA 2018) ac unrhyw ddeddfwriaeth gysylltiedig arall, gan gynnwys GDPR yr UE os yw’n berthnasol.
	3. Yn rhan o’r rhwymedigaethau cyfreithiol hynny, rhaid i’r Brifysgol sicrhau bod dulliau diogelu priodol yn bodoli er mwyn diogelu data personol.
	4. Os bydd y dulliau diogelu hyn yn methu, mae gan y Brifysgol ddyletswydd gyfreithiol i gynnal prosesau ar gyfer canfod a rheoli digwyddiadau’n ymwneud â thorri diogelwch data personol, ac adrodd amdanynt.

# Diffiniadau

* 1. At ddibenion y polisi hwn, diffinnir ‘data personol’ fel gwybodaeth yn ymwneud â phersonau naturiol:
		+ y gellir eu hadnabod neu sy’n adnabyddadwy yn uniongyrchol o’r wybodaeth dan sylw, neu
		+ y gellir eu hadnabod yn anuniongyrchol o’r wybodaeth honno ar y cyd â gwybodaeth arall.
	2. Mae’r polisi hwn yn berthnasol i ddata personol y mae’r Brifysgol yn rheolydd data cofrestredig ar ei gyfer ac mae hefyd yn berthnasol pan fydd parti allanol yn prosesu data o’r fath.
	3. Diffinnir ‘Tor diogelwch data’ fel digwyddiad lle bu tor diogelwch yn ymwneud â data personol, sydd yn ei dro wedi arwain at ddinistrio, colli, addasu damweiniol neu anghyfreithiol, neu ddatgelu neu fynediad heb awdurdod i ddata personol a gaiff ei drosglwyddo, ei storio neu ei brosesu fel arall.

# Pwrpas y polisi hwn

* 1. Mae’r polisi hwn yn manylu sut mae’r Brifysgol yn bodloni ei rhwymedigaethau cyfreithiol ynghylch hysbysu am achosion o dorri diogelwch data personol, a’u rheoli, trwy:
		+ manylu’r weithdrefn y mae’n rhaid i staff ei dilyn i roi gwybod i’r Swyddog Diogelu Data (DPO) dynodedig am achosion o dorri diogelwch data; a
		+ cadarnhau dyletswydd staff i gynorthwyo’r DPO a’i staff mewn perthynas â thrin achosion o dorri diogelwch data personol; ac
		+ amlinellu’r ffactorau y mae’n rhaid eu hystyried wrth asesu risg effaith a difrifoldeb tor diogelwch data personol; a
		+ sefydlu’r fframwaith sefydliadol y mae’n rhaid ei ddefnyddio i reoli a hysbysu am achosion o dorri diogelwch data, er mwyn lleihau’r effaith, y difrifoldeb a’r risg yn gysylltiedig ag achosion o dorri diogelwch data.

# Hysbysu am dor diogelwch data personol

* 1. Pan ddaw staff yn ymwybodol o dor diogelwch data personol posibl, rhaid iddynt roi gwybod i’r DPO am y tor yn syth.
	2. Wrth hysbysu am dor, mae’n ofynnol i staff ddarparu’r wybodaeth ganlynol i’r DPO:
		+ disgrifiad o’r data personol yr effeithir arno;
		+ esboniad o’r digwyddiad, sut y digwyddodd a phryd;
		+ y mathau a’r nifer bras o wrthrychau’r data dan sylw;
		+ y categorïau a’r nifer bras o gofnodion data personol dan sylw;
		+ canlyniadau tebygol y tor diogelwch data personol;
		+ unrhyw ymdrechion uniongyrchol i leihau effaith y tor.
	3. Gofynnir i staff lenwi’r Ffurflen Adroddiad Gwerthuso Digwyddiad Data (“DIERF”) ynghlwm yn Atodiad A. Ni chaiff diffyg eglurder ynghylch yr amgylchiadau’n ymwneud â’r tor posibl oedi hysbysu’r DPO am achosion o dorri.
	4. Rhaid i staff gynorthwyo’r DPO yn brydlon mewn perthynas ag unrhyw ymholiadau a godir gan y DPO yn ystod yr ymchwiliad a/neu ymchwiliadau cysylltiedig.
	5. Gall y Brifysgol benodi proseswyr allanol i brosesu data ar ei rhan. Rhaid i unrhyw gontract cysylltiedig ei wneud yn ofynnol i’r prosesydd hysbysu DPO y Brifysgol heb oedi am unrhyw dor diogelwch data personol posibl sy’n effeithio ar ddata a reolir gan y Brifysgol.
	6. Os daw aelod o staff yn y Brifysgol yn ymwybodol fod prosesydd neu is-brosesydd wedi profi tor diogelwch data personol, rhaid iddo roi gwybod i’r DPO yn yr un modd ag y byddai am unrhyw achos arall o dorri.
	7. Rhaid i’r DPO gymryd camau rhesymol i sicrhau bod yr holl staff yn ymwybodol o’r mecanwaith hysbysu sydd wedi’i gynnwys yn yr adran hon.

# Rheoli achosion o dorri

* 1. Pan fydd yn derbyn y DIERF, bydd y DPO yn asesu a yw’r tor posibl yn debygol o arwain at risg sylweddol i hawliau a rhyddid gwrthrychau’r data dan sylw.
	2. Os bydd y DPO o’r farn y byddai’r tor posibl yn arwain at risg sylweddol tebygol i hawliau a rhyddid gwrthrych y data, bydd yn hysbysu Ysgrifennydd y Brifysgol am y tor cyn gynted ag y bo’n ymarferol ac yna i Swyddfa’r Comisiynydd Gwybodaeth (ICO) cyn pen 72 awr i PCYDDS ddod yn ymwybodol o’r tor. Bydd Ysgrifennydd y Brifysgol wedyn yn adrodd am y tor ac ymateb yr ICO i CCAUC a’r Pwyllgor Archwilio a Risg gan ddefnyddio’r protocol sefydledig ar gyfer adrodd, a bydd yn cysylltu â Chadeiryddion y Pwyllgor Archwilio a Risg a’r Cyngor i benderfynu a ddylid gwneud adroddiad i’r Comisiwn Elusennau.
	3. Pan nad ystyrir fod tor neu dor posibl yn hysbysadwy, bydd y DPO yn diffinio’r tor neu’r tor posibl fel ‘digwyddiad diogelwch data’ neu ‘dor diogelwch data nad yw’n hysbysadwy’ ac yn hysbysu Ysgrifennydd y Brifysgol am y mater. Caiff y tor ei gofnodi yn “log achosion o dorri” y Brifysgol.
	4. Wrth asesu’r risg a grëir i wrthrychau’r data gan y tor, dylai’r DPO ystyried y ffactorau canlynol:
		+ y math o dor;
		+ natur, sensitifrwydd a maint y data personol;
		+ rhwyddineb adnabod unigolion;
		+ difrifoldeb y canlyniadau i unigolion;
		+ nodweddion arbennig yr unigolion yr effeithir arnynt;
		+ nifer yr unigolion yr effeithir arnynt.
	5. Pan fo diffyg manylion ynghylch achosion ac effaith bosibl tor, dylai’r DPO gynnwys hynny fel ffactor wrth asesu’r risg cyffredinol.
	6. Lle bu tor difrifol yr ystyrir ei fod yn hysbysadwy i’r ICO (a bod y DPO wedi nodi risg uchel i wrthrychau’r data) bydd y DPO yn cysylltu â gwrthrychau’r data dan sylw heb oedi gormodol, ac yn rhoi gwybod iddynt am y canlynol, man lleiaf:
		+ disgrifiad o natur y tor;
		+ enw a manylion cyswllt y DPO a/neu gysylltiadau perthnasol eraill;
		+ disgrifiad o ganlyniadau tebygol y tor;
		+ disgrifiad o’r mesurau a gymerwyd neu y cynigiwyd eu cymryd gan y rheolydd i fynd i’r afael â’r tor, gan gynnwys, lle bo hynny’n briodol, mesurau i leihau ei effeithiau andwyol posibl.
	7. Bydd y DPO yn ymchwilio i bob achos o dorri.
	8. Bydd y DPO yn cynghori ac yn cynorthwyo’r adran hysbysu i gymryd camau i ffrwyno unrhyw dor posibl, lleihau unrhyw risgiau sy’n deillio ohono a rhoi dulliau unioni ar waith er mwyn lleihau effaith unrhyw dor posibl ar wrthrych/gwrthrychau’r data dan sylw.
	9. Os bydd y DPO, yn ystod yr ymchwiliad, yn darganfod gwybodaeth bellach sy’n newid natur mân dor diogelwch data fel ei fod yn ymddangos bod y tor yn hysbysadwy, bydd y DPO yn ymgynghori ag Ysgrifennydd y Brifysgol i gadarnhau’r camau i’w cymryd.
	10. Bydd y DPO/y Brifysgol yn cynorthwyo’r ICO wrth arfer ei bwerau statudol yn ymwneud ag achosion o dorri diogelwch data sy’n hysbysadwy a bydd yn ystyried unrhyw gyngor a roddir gan yr ICO ynghylch rheoli tor diogelwch data yr hysbyswyd amdano.
	11. Bydd y DPO yn cynnal log o bob achos o dorri (y log achosion o dorri), rhai hysbysadwy yn ogystal â mân achosion, yn ogystal â chofnod o’r holl gamau gweithredu a phenderfyniadau a wnaed gan y Swyddog Diogelu Data o ran rheoli’r tor hwnnw.

# Achosion o dorri diogelwch data personol yn sgil digwyddiadau seiberddiogelwch

* 1. Mewn amgylchiadau lle bo diogelwch data personol wedi’i beryglu gan seiberddigwyddiad, yn hytrach na thor diogelwch data penodol, bydd y DPO yn cysylltu ag uwch gydweithwyr ym maes Gwasanaethau Digidol y Brifysgol, yn unol â’r Cynllun Ymateb i Ddigwyddiad TG, gan sicrhau fod y seiberddigwyddiad yn cael ei reoli yn unol â’r gofynion a wnaed yn y polisi hwn a pholisïau eraill. Rhoddir y wybodaeth ddiweddaraf i Ysgrifennydd y Brifysgol ar bob adeg.

# Gwerthuso a ‘gwersi a ddysgwyd’

* 1. Unwaith y bydd y tor diogelwch data personol wedi’i ffrwyno a chamau adferol wedi’u cwblhau, bydd y DPO yn adolygu achosion y tor diogelwch data personol ac ymateb y Brifysgol i’r tor.
	2. Bydd gwerthusiad y DPO yn cael ei gyfleu i uwch reolwyr y Brifysgol o’r maes gweithredol lle digwyddodd y tor.
	3. Bydd y gwerthusiad hefyd yn cael ei gyfleu i Ysgrifennydd y Brifysgol i sicrhau bod dull ‘gwersi a ddysgwyd’ yn cael ei ymgorffori yn y broses tor diogelwch data.
	4. Bydd y DPO yn cynnwys ystadegau a chrynodebau perthnasol ynghylch achosion o dorri diogelwch data yn ei adroddiadau rheolaidd i Ysgrifennydd y Brifysgol ar gyfer prosesau adrodd.

**Atodiad 1**

 **Ffurflen Adroddiad Gwerthuso Digwyddiad Data**

1. **Dyddiad ac amser y Digwyddiad (a phryd y daeth i’ch sylw)**
2. **Disgrifiwch y digwyddiad (beth a ddigwyddodd, sut y digwyddodd, pa gamau a gymerwyd gennych i leihau’r golled, er enghraifft adalw e-bost a anfonwyd ar gam)**
3. **Rhowch fanylion y data a’r nifer o bobl y gallai’r digwyddiad/tor diogelwch data effeithio arnynt**

**Enw…………………………………………………………………………………**

**Dyddiad ac Amser……………………………………………………………….**

**Sicrhewch fod y wybodaeth a ddarperir mor llawn â phosibl a chysylltwch â Swyddog Diogelu Data’r Brifysgol cyn gynted â phosibl i roi gwybod am y tor.**

Awdur(on) y polisi:

Paul Osborne – Swyddog Diogelu Data

Rheoli fersiynau’r ddogfen

|  |  |  |  |
| --- | --- | --- | --- |
| Rhif y Fersiwn: | Rheswm dros newid: | Awdur: | Dyddiad y newid: |
| 0.1 | Crëwyd y polisi | PO | 1af Chwef 2024 |
| 0.2 | Adolygwyd y polisi gan Ddirprwy Ysgrifennydd y Brifysgol ac ychwanegwyd at y templed corfforaethol | RD a CG | 28ain Chwef 2024 |
|  | Cymeradwywyd gan UDA |  | 8fed Tachwedd 2024 |
|  |  |  |  |

Statws presennol y Polisi: cytunwyd gan UDA

A yw’r Polisi’n berthnasol i**:** / AB ac AU fel ei gilydd\*

Dyddiad cadarnhau: 8/11/24

Dyddiad dod i rym: 8/11/24

Dyddiad adolygu’r polisi: 7/11/25

I’w gyhoeddi**:** ar / MyDay /

### *Cymeradwyo*

*Caiff y polisi ei ystyried a’i gymeradwyo’n ffurfiol yn unol â Chylch Gorchwyl y Pwyllgor a amlinellwyd yn y Llawlyfr Ansawdd Academaidd.*

*Os yw’r polisi’n effeithio ar staff, dylid ceisio cyngor gan AD o’r cychwyn i ganfod a oes angen ymgynghoriad yn y JCC. Yn ogystal, bydd AD yn darparu cyngor ar y cam mwyaf priodol i ymgynghori â JCC ac a oes angen cymeradwyaeth y Cyngor.*

*Rhaid i BOB polisi a gyflwynir i’w gymeradwyo ddod gyda’r canlynol wedi’u cwblhau:*

* *[Asesiad o’r Effaith ar Gydraddoldeb a’r Gymraeg](https://uowtsd.sharepoint.com/%3Aw%3A/r/corporate-services/Shared%20Documents/Policies%20%26%20Strategies/Guidance%20and%20Templates/1.3%20UWTSD%20Equality%20and%20welsh%20language%20Impact%20Assessment%20March%202022%20v2.dot?d=w108478d73dff429290b3881e7312c242&csf=1&web=1&e=ieoDH6)*
* [*Asesiad Effaith Sefydliadol*](https://uowtsd.sharepoint.com/%3Aw%3A/r/corporate-services/Shared%20Documents/Policies%20%26%20Strategies/Guidance%20and%20Templates/1.4.%20UWTSD%20Institutional%20Impact%20Assessment%20-%20Oct%202017.dotx?d=wa000b736a38941ff992940a724f79bce&csf=1&web=1&e=dMgUao)
* [*Asesiad o’r Effaith ar Ddiogelu Data*](https://uowtsd.sharepoint.com/%3Aw%3A/r/corporate-services/Shared%20Documents/Policies%20%26%20Strategies/Guidance%20and%20Templates/Data%20Protection%20Impact%20Assessment%20template.dotx?d=w806d26e953bc46f5bc6c3243f4bed39a&csf=1&web=1&e=hyeTgg)

*Cyn cyflwyno i’r pwyllgor, gofynnir i awduron ymgynghori â’r Tîm Polisi a Chynllunio a fydd yn gwirio bod y ddogfen yn cydymffurfio â gofynion y Brifysgol. Bydd y Tîm Polisi a Chynllunio yn cwblhau’r adran isod.*

**I’w gwblhau gan ysgrifennydd y pwyllgor**

*Ticiwch i gadarnhau’r canlynol:*

*Mae Asesiad Effaith Sefydliadol wedi’i gwblhau ☒*

*Mae Asesiad o’r Effaith ar Gydraddoldeb a'r Gymraeg wedi'i gwblhau ☒*

*Mae DPIA wedi’i gwblhau ☒*

*Materion sydd angen eu hystyried gan y pwyllgor cymeradwyo:*

