**Gweithdrefn Tor Diogelwch Data**

**1.0 Cyflwyniad**

1.1 Mae Prifysgol Metropolitan Caerdydd yn dal, yn prosesu ac yn rhannu llawer iawn o ddata personol a rhaid cymryd gofal i sicrhau ei bod wedi'i diogelu'n briodol er mwyn osgoi tor rheolau diogelu data yn ddamweiniol neu’n fwriadol.

1.2 Mae'n ofynnol o dan ddeddfwriaeth diogelu data i'r Brifysgol gael fframwaith sefydliadol wedi'i gynllunio i sicrhau diogelwch yr holl ddata personol trwy gydol ei gylch oes, gan gynnwys llinellau cyfrifoldeb clir.

1.3 Mae'r weithdrefn hon yn nodi sut i sicrhau bod camau effeithiol ac amlwg yn cael eu cymryd i reoli achos o dor diogelwch data neu ddigwyddiad diogelwch gwybodaeth ledled y Brifysgol.

**2.0 Cwmpas**

2.1 Dylid defnyddio'r Weithdrefn hon mewn perthynas â'r holl ddata categori personol a [chategori arbennig](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/) \* a gedwir gan y Brifysgol waeth beth fo'u fformat.

2.2 Mae'r Weithdrefn hon yn berthnasol i holl staff a myfyrwyr y Brifysgol. Mae hyn yn cynnwys staff dros dro, staff achlysurol neu staff a chyflogwyd trwy asiantaeth a chontractwyr neu ymgynghorwyr yn y Brifysgol.

2.3 Mae'r Weithdrefn hon yn berthnasol i achosion y bu ond y dim iddynt ddigwydd h.y. sefyllfaoedd lle mae toriad data personol wedi'i gynnwys heb amlygu unrhyw unigolion i risg o niwed.

\* <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>

**3.0 Diffiniad / Mathau o Dor Diogelwch Data**

3.1 At ddibenion y Weithdrefn hon, mae achosion o dorri rheolau diogelwch data yn cynnwys digwyddiadau a gadarnhawyd ac a amheuir.

3.2 Digwyddiad yng nghyd-destun y Weithdrefn hon yw digwyddiad neu weithred a allai beryglu cyfrinachedd, uniondeb neu argaeledd systemau neu ddata, naill ai'n ddamweiniol neu'n fwriadol, a allai arwain at niwed i unigolyn/unigolion neu ddiffyg cydymffurfio deddfwriaethol fel arall y mae'r Brifysgol yn gyfrifol amdano.

3.3 Bydd hyn yn berthnasol ai'r Brifysgol yw'r Rheolwr Data (sy'n gyfrifol am y diben y mae'r Data'n cael ei brosesu) neu Brosesydd Data (prosesu data ar ran Rheolwr Data).

3.4 Mae digwyddiad tor rheolau yn cynnwys ond heb ei gyfyngu i’r canlynol:

**• Colli neu ddwyn data neu offer cyfrinachol neu sensitif y cedwir data o'r fath arnynt (e.e. colli gliniadur, ffon USB, dyfais iPad/tabled, neu gofnod papur)   
• Dwyn offer neu offer yn methu  
• Defnydd anawdurdodedig o ddata neu systemau gwybodaeth neu fynediad iddynt neu eu haddasu  
• Ymdrechion (wedi methu neu'n llwyddiannus) i gael mynediad heb awdurdod at wybodaeth neu system(au) TG  
• Datgelu data sensitif / cyfrinachol heb awdurdod   
• Difenwi gwefannau   
• Ymosodiad hacio   
• Gwall dynol (anfon e-bost neu lythyr at y derbynnydd anghywir)   
• Troseddau 'blagio' lle ceir gwybodaeth drwy dwyllo'r sefydliad sy'n ei ddal**

3.5 Mae Swyddog Cydymffurfiaeth Data a Gwybodaeth y Brifysgol yn gweithredu fel y Swyddog Diogelu Data Statudol yn unol â gofynion GDPR. Hwy sy'n gyfrifol am y Weithdrefn hon a'r deiliad rôl hwnnw sy'n gyfrifol am y penderfyniad i hysbysu Swyddfa'r Comisiynydd Gwybodaeth.

3.6 Rhaid i'r Dirprwy Lywydd gael llinell adrodd uniongyrchol i'r Uwch Reolwyr. Yr Ysgrifennydd a Chlerc y Llywodraethwyr yw'r Uwch Reolwr cyfrifol ar gyfer materion Diogelu Data yn y Brifysgol.

**4.0 Adrodd am ddigwyddiad**

4.1 Mae'r holl staff yn gyfrifol am roi gwybod am Dor Diogelwch Data posibl ar unwaith yn unol â Pholisi Diogelu Data'r Brifysgol [(ar gael yma](http://www.cardiffmet.ac.uk/about/structureandgovernance/Pages/Data-Protection---Records-Management.aspx)). Rhaid hysbysu'r Swyddog Cydymffurfiaeth Data a Gwybodaeth cyn gynted â phosibl er mwyn asesu difrifoldeb ac effaith bosibl y toriad.

4.2 Os bydd y toriad yn digwydd neu'n cael ei ddarganfod y tu allan i oriau gwaith arferol, rhaid rhoi gwybod amdano cyn gynted ag y bo'n ymarferol. Dim ond 72 awr sydd gan y Brifysgol i roi gwybod i'r rheoleiddiwr am doriad data posibl, felly mae hysbysu ar unwaith yn allweddol.

4.3 Rhaid llenwi [Ffurflen Adroddiad Digwyddiad](https://outlookuwicac-my.sharepoint.com/personal/sm22791_cardiffmet_ac_uk/Documents/Data%20Protection%20and%20Data%20Processing/Data%20Breach%20Incident%20Report%20Form%20.docx) fel rhan o'r broses adrodd a'i hanfon at [dataprotection@cardiffmet.ac.uk](mailto:dataprotection@cardiffmet.ac.uk).

**5.0 Cyfyngu ac Adfer**

5.1 Bydd asesiad cychwynnol yn cael ei wneud gan y Dirprwy Lywydd, ar y cyd â swyddogion perthnasol, i archwilio pa mor ddifrifol ydy’r toriad. Yn seiliedig ar ddifrifoldeb, penderfynir a yw'r Dirprwy Lywydd yn cwblhau ymchwiliad llawn i'r toriad neu a all yr Ysgol/Swyddogion Cyfrifol reoli'r gwall a mân effaith/risg lefel isel.

5.2 Bydd yr ymchwiliad yn sefydlu a ellir gwneud unrhyw beth i adennill unrhyw golledion a chyfyngu ar y niwed y gallai'r toriad ei achosi.

5.3 Bydd yr ymchwiliad yn sefydlu pwy sydd angen ei hysbysu fel rhan o'r camau gweithredu cychwynnol ac yn penderfynu ar gamau addas i'w cymryd i sicrhau datrysiad i'r digwyddiad.

**6.0 Ymchwilio ac Asesu Risg**

6.1 Bydd ymchwiliad yn cael ei gynnal gan y Swyddog Gwybodaeth ar unwaith a lle bynnag y bo modd o fewn 24 awr i'r toriad gael ei ddarganfod / adrodd.

6.2 Bydd y Swyddog Gwybodaeth yn ymchwilio i'r toriad ac yn asesu'r risgiau sy'n gysylltiedig ag ef, er enghraifft, y canlyniadau andwyol posibl i unigolion, pa mor ddifrifol neu sylweddol yw'r rheini a pha mor debygol ydynt o ddigwydd.

6.3 Bydd angen i'r ymchwiliad ystyried y canlynol:

* sensitifrwydd a math y data dan sylw;
* pwy yw'r unigolion, nifer yr unigolion dan sylw a'r effeithiau posibl ar y testun neu destunau data hynny;
* mae'r amddiffyniadau ar waith (e.e. amgryptio);
* beth sydd wedi digwydd i'r data, a yw wedi'i golli neu ei ddwyn;
* a ellid rhoi'r data at unrhyw ddefnydd anghyfreithlon neu amhriodol;
* a oes canlyniadau ehangach i'r toriad.

**7.0 Hysbysiad**

7.1 Bydd y Swyddog Gwybodaeth, mewn ymgynghoriad â'r Dirprwy Lywydd a'r Swyddog Diogelwch Gwybodaeth/Pennaeth Gwasanaethau Gwybodaeth (os yw'r mater yn ymwneud â diogelwch ein systemau) yn penderfynu pwy sydd angen ei hysbysu am y toriad.

7.2 Bydd pob digwyddiad yn cael ei asesu fesul achos; fodd bynnag, bydd angen ystyried y canlynol:

• A oes unrhyw ofynion hysbysu cyfreithiol/cytundebol;  
• a fyddai hysbysiad yn cynorthwyo'r unigolyn yr effeithir arno – a allent weithredu ar y wybodaeth i liniaru risgiau?   
• a fyddai hysbysu'n helpu i atal y defnydd anawdurdodedig neu anghyfreithlon o ddata personol?   
• a fyddai hysbysu yn helpu'r Brifysgol i gyflawni ei rhwymedigaethau o dan y seithfed egwyddor diogelu data;  
• Os effeithir ar nifer fawr o bobl, neu os oes canlyniadau difrifol iawn, a ddylid hysbysu Swyddfa'r Comisiynydd Gwybodaeth (SCG). Dim ond os bydd data personol yn gysylltiedig y bydd Swyddfa'r Comisiynydd Gwybodaeth yn cael ei hysbysu. Mae canllawiau ar pryd a sut i hysbysu Swyddfa'r Comisiynydd Gwybodaeth ar gael ar eu gwefan [: https://ico.org.uk/media/1536/breach\_reporting.pdf](https://ico.org.uk/media/1536/breach_reporting.pdf)

• Peryglon gor-hysbysu. Nid yw pob digwyddiad yn gwarantu hysbysiad a gall gor-hysbysu achosi ymholiadau a gwaith anghymesur.

7.3 Y Dirprwy Lywydd sy'n gyfrifol yn y pen draw am y penderfyniad i hysbysu Swyddfa'r Comisiynydd Gwybodaeth ond rhaid i uwch reolwyr gael eu hysbysu drwy Glerc ac Ysgrifennydd y Llywodraethwyr.

7.4 Bydd hysbysu'r unigolion y mae'r digwyddiad wedi effeithio ar eu data personol yn cynnwys disgrifiad o sut a phryd y digwyddodd y toriad a'r data dan sylw. Rhoddir cyngor penodol a chlir ar yr hyn y gallant ei wneud i amddiffyn eu hunain, a chynnwys pa gamau sydd eisoes wedi'u cymryd i liniaru'r risgiau. Bydd unigolion hefyd yn cael ffordd o gysylltu â'r Brifysgol i gael rhagor o wybodaeth neu i ofyn cwestiynau am yr hyn sydd wedi digwydd.

7.5 Bydd y Swyddog Gwybodaeth a/neu'r Dirprwy Lywydd yn ystyried a ddylid hysbysu'r Tîm Cyfathrebu ynghylch datganiad i'r wasg a bod yn barod i ymdrin ag unrhyw ymholiadau i'r wasg sy'n ein cyrraedd.

7.6 Bydd yr holl gamau gweithredu yn cael eu cofnodi gan y Dirprwy Lywydd.

Atodiad 1 – Ffurflen Adroddiad Tor Diogelwch Data