Ysgol Cybi

Polisi Digwyddiadau Diogelwch Data Ysgolion / *Schools Data Breach Policy*

(Fersiwn 2, Hydref 2021 / *Version 2, October 2021*)

Ynglŷn â'r polisi hwn

Mae'r polisi hwn yn amlinellu'r weithdrefn i'w dilyn gan holl staff ysgolion a chontractwyr os oes digwyddiad diogelwch data yn digwydd. Mae'r polisi hwn yn berthnasol i unrhyw ddata personol a chategori arbennig a ddelir gan yr ysgol.

Cefnogir y polisi hwn gan adnoddau ar tudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

About this policy

This policy sets out the procedure to be followed by all school staff and contractors if a data breach takes place. This policy applies to all personal and special category data held by the school.

This policy is supported by resources on the Data Protection page on the Learning Service Microsite.

Fersiwn / *Version*	**Dyddiad / *Date***	**Crynodeb o newidiadau / *Summary of changes***	**Dyddiad a Dderbyniwyd gan Fwrdd o Lywodraethwyr / *Date Accepted by Board of Governors***
F1/*V1*	Ionawr 2021 / *January* 2021	Polisi newydd / *New policy.*	
F2/*V2*	Hydref 2021 / *October 2021*	Newid cyfeiriadau at GDPR i UK GDPR a mân newidiadau / *Change reference*	

		to GDPR to UK GDPR and minor changes	

Dyddiad yr adolygiad nesaf / *Date of next review*	
Bydd y polisi hwn yn cael ei adolygu yn: / *This policy will be reviewed in:*	Hydref 2023 / *October* 2023
Yr unigolyn a fydd yn ymgymryd â'r adolygiad fydd: / *The review will be undertaken by:*	Swyddog Diogelu Data Ysgolion / *Schools Data Protection Officer*

Manylion Cyswllt:

Swyddog Diogelu Data Ysgolion

E-bost:
dpoysgolionmon@ynysmon.gov.uk

Rhif ffôn: 01248 751833

Cyfeiriad:
Gwasanaeth Dysgu
Cyngor Sir Ynys Môn
Swyddfeydd y Cyngor
Llangefni
Ynys Môn
LL77 7TW

Contact Details:

Schools Data Protection Officer

E-mail:
dpoysgolionmon@ynysmon.gov.uk

Telephone: 01248 751833

Address:
Learning Service
Isle of Anglesey County Council
Council Offices
Llangefni
Anglesey
LL77 7TW

Rydym yn hapus i ddarparu'r polisi hwn ar ffurfiau eraill ar gais. Defnyddiwch y manylion cyswllt uchod. / *We are happy to provide this policy in alternative formats on request. Please use the above contact details.*

Dogfen:
Document: Templed polisi ar y weithdrefn i'w dilyn os oes digwyddiad diogelwch data mewn ysgol. / *Policy template on the procedure to be followed if a data breach takes place within the school.*

Cyfrifoldeb:
Responsibility: Cyfrifoldeb llywodraethwyr a Pennaeth yr ysgol yw sicrhau bod gweithdrefnau ar waith i sicrhau bod yr ysgol yn cydymffurfio â'r gofynion dan y *Rheoliadau Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR)* a *Deddf Diogelu Data 2018. / It is the responsibility of the school governors and Headteacher to ensure procedures are in place to ensure that the school complies with the requirements under the* UK General Data Protection Regulations (UK GDPR) *and the* Data Protection Act 2018.

Cynnwys **Tudalen**

1. Datganiad Polisi

Mae'r polisi hwn yn amlinellu'r weithdrefn i'w dilyn gan yr ysgol a sut y bydd yn cydymffurfio â rhwymedigaethau diogelu data yn achos digwyddiad diogelwch data. Mae'n sicrhau dull cyson ac effeithiol o reoli digwyddiadau diogelwch data ac yn sefydlu strwythur ar gyfer adrodd ar ddigwyddiadau o'r fath.

Mae'r ysgol wedi ei hymrwymo'n llawn i sicrhau ei bod yn cydymffurfio'n llawn â deddfwriaeth diogelu data ac yn sicrhau ei bod yn cwrdd â'i gofynion cyfreithiol, statudol a rheoliadol dan yr *UK GDPR*. Bydd yr ysgol yn sicrhau bod y camau gweithredu priodol yn cael eu cymryd yn syth i leihau'r effaith ar unigolion; er mwyn lliniaru risgiau cysylltiedig ac i atgyweirio unrhyw ddifrod.

Disgwylia'r ysgol i'w holl staff fewnosod ymarferion diogelwch ac atal yn eu gwaith dyddiol i sicrhau y diogelir gwybodaeth, ac mae'n rhaid iddynt gymryd y camau priodol i ddiogelu unrhyw wybodaeth.

Bydd yr ysgol yn ymgynghori ac yn ymofyn am gyngor gan y Swyddog Diogelu Data Ysgolion ynglŷn ag unrhyw ddigwyddiadau, problemau, pryderon neu gwestiynau ynglŷn â digwyddiadau diogelwch data.

2. Sgôp

Mae'r polisi hwn yn berthnasol ar gyfer gweithwyr yr ysgol a'r sawl sy'n gweithio ar ran yr ysgol, gan gynnwys llywodraethwyr ysgol a chontractwyr sydd gan fynediad i ac/neu sy'n prosesu gwybodaeth yr ysgol.

Mae'r polisi hwn yn berthnasol i unrhyw wybodaeth bersonol a chategori arbennig a ddelir gan yr ysgol.

Mae'n ymwneud â gwybodaeth a ddelir ym mhob fformat, gan gynnwys, ond ddim wedi'w gyfyngu i, bapur, electronig, clywedol a gweledol. Mae'r ysgol yn cadw gwybodaeth bersonol, gan gynnwys copïau caled a meddal, ac yn defnyddio systemau gwybodaeth amrywiol sy'n cadw data personol, sydd oll yn gymwys i'r polisi hwn.

Mae digwyddiadau diogelwch data yn cynnwys digwyddiadau sydd wedi eu cadarnhau neu amheuaeth o ddigwyddiadau.

3. Cyfrifoldebau

3.1. Corff Llywodraethu Ysgol
Mae'r corff llywodraethu ysgol yn gyfrifol am:

- monitro cydymffurfiad ac atebolrwydd cyffredinol yr ysgol ynglŷn â'r polisi yma;
- sicrhau bod yr ysgol yn gallu tystiolaethu cydymffurfiaeth gyda deddfwriaeth diogelu data.

3.2. Pennaeth (ac/neu'r Unigolyn sy'n Gyfrifol am Ddiogelu Data yn yr Ysgol)
Mae'r Pennaeth ac/neu'r unigolyn sy'n gyfrifol am ddiogelu data yn yr ysgol yn gyfrifol am sicrhau:

- bod proses ar waith i ddiogelu'r holl wybodaeth bersonol a chategori arbennig yn yr ysgol;
- bod proses gadarn ar waith i ganfod ac adnabod digwyddiadau diogelwch data; i ymchwilio ac asesu digwyddiadau gan gynnwys risgiau ac adrodd a hysbysu o unrhyw ddigwyddiadau diogelwch data;
- bod camau'n cael eu cymryd yn syth i leihau effaith digwyddiadau diogelwch data ac i benderfynu ar y camau gweithredu priodol a'r adnoddau sydd eu hangen i gyfyngu effaith digwyddiadau diogelwch data;
- bod *Ffurflenni Ymchwilio i Ddigwyddiadau Diogelwch Data Ysgolion* yn cael eu cwblhau cyn gynted â phosib; yn cynnwys gwybodaeth fanwl a chywir a'u bod yn cael eu rhannu'n syth â'r Swyddog Diogelu Data Ysgolion;
- bod cofnod canolog o'r holl ddigwyddiadau diogelwch data yn cael ei gadw gyda *Log Digwyddiadau Diogelwch Data;*
- bod y ffigyrau blynyddol ynglŷn â'r cyfanswm o ddigwyddiadau diogelwch data sydd wedi digwydd yn ystod y flwyddyn ysgol yn cael eu cyflwyno i gorff llywodraethu'r ysgol ac i'r Swyddog Diogelu Data Ysgolion;
- bod gwersi'n cael eu dysgu o ddigwyddiadau diogelwch data blaenorol a bod cynlluniau gweithredu'n cael eu gweithredu er mwyn newid a gwella gweithdrefnau ac ymarferion lle bod angen;
- bod y Swyddog Diogelu Data Ysgolion yn cael gwybod am yr holl fanylion ynghylch y digwyddiad ac yn prif bwynt cyswllt i'r Swyddog Diogelu Data Ysgolion wrth ddelio â digwyddiadau diogelwch data;
- bod yr holl staff yn cydymffurfio â'r polisi hwn; yn ymwybodol o'r broses pan fydd digwyddiad diogelwch data a bod staff yn cynorthwyo ag ymchwiliadau fel bod angen.

3.3. Y Swyddog Diogelu Data Ysgolion
Mae'r Swyddog Diogelu Data Ysgolion yn gyfrifol am:

- fod yn brif bwynt cyswllt i'r ysgol ar gyfer adrodd ar unrhyw ddigwyddiadau diogelwch data/achosion agos;
- hysbysu a chynghori ysgolion ar eu rhwymedigaethau o ran digwyddiadau diogelwch data;
- creu ac adolygu gweithdrefnau, polisïau, canllawiau a thempledi digwyddiadau diogelwch data yn rheolaidd;
- darparu cyngor ac arweiniad i'r ysgol ynglŷn ag unrhyw fesurau angenrheidiol i ymatal, lliniaru a mynd i'r afael â digwyddiadau diogelwch data;
- cwblhau Rhan C o'r Ffurflen Ymchwilio i Ddigwyddiadau Diogelwch Data Ysgolion i ddarparu argymhellion ynglŷn ag adrodd ar ddigwyddiadau diogelwch data i'r ICO;
- darparu cyngor a chefnogaeth i'r ysgol ynglŷn â hysbysu trydydd bartïon am ddigwyddiadau diogelwch data;
- gwneud y penderfyniad a oes angen adrodd ar y digwyddiad diogelwch data i'r ICO;
- hysbysu'r ICO o unrhyw ddigwyddiadau diogelwch data adroddadwy;

- hysbysu unigolion a effeithir os yw digwyddiad diogelwch data yn debygol o arwain at risg uchel i'w hawliau a'u rhyddid;
- cefnogi'r ysgol mewn perthynas â gwersi a ddysgwyd a chreu cynllun gweithredu er mwyn newid a gwella gweithdrefnau ac ymarferion lle bo angen;
- casglu gwybodaeth gan y Pennaeth ynglŷn â'r cyfanswm o ddigwyddiadau diogelwch data sydd wedi digwydd yn ystod y flwyddyn ysgol a chadw *Log Digwyddiadau Diogelwch Data* ar gyfer pob ysgol.

3.4. Yr Holl Staff yn yr Ysgol
Mae'r holl staff a gyflogir gan neu sy'n gwirfoddoli yn yr ysgol, gan gynnwys athrawon, cymorthyddion dosbarth a staff cefnogi busnes yn gyfrifol am sicrhau eu bod yn:

- ymgyfarwyddo a chydymffurfio'n llawn â'r polisi hwn;
- adrodd yn syth ar unrhyw ddigwyddiadau gwirioneddol, amheuol, bygythiol neu botensial o ddigwyddiadau diogelwch data i'r Pennaeth ac/neu i'r unigolyn sy'n gyfrifol am ddiogelu data yn yr ysgol;
- cynorthwyo ag ymchwiliadau yn ôl yr angen, yn arbennig os oes angen cymryd camau gweithredu brys i atal difrod pellach.

Os oes gan staff unrhyw ymholiadau, dylent drafod y rhain â'r Pennaeth; y swyddog sy'n gyfrifol am ddiogelu data yn yr ysgol neu'r Swyddog Diogelu Data Ysgolion.

4. Deddfwriaeth, Canllawiau a Pholisïau

Mae gan yr ysgol ddyletswydd orfodol i sicrhau bod data personol yn cael ei ddiogelu a'i brosesu yn unol â'r *Rheoliadau Diogelu Data Cyffredinoly y Deyrnas Unedig (UK GDPR)* a'r *Ddeddf Diogelu Data 2018.*

Mae *Deddf Diogelu Data 2018* yn darparu ar gyfer rheoleiddio prosesu (defnyddio) gwybodaeth ynglŷn ag unigolion, gan gynnwys derbyn, cadw a defnyddio'r fath wybodaeth.

Mae'r *UK GDPR* yn nodi y dylid prosesu gwybodaeth bersonol *"mewn ffordd sy'n sicrhau bod data personol yn cael ei ddiogelu'n briodol, gan gynnwys amddiffyn rhag prosesu anawdurdodedig neu anghyfreithlon ac amddiffyn rhag colled, dinistr neu ddifrod damweiniol, drwy ddefnyddio mesurau technegol neu drefniadol priodol."*

Mae'r polisi hwn yn seiliedig ar godau ymarfer perthnasol a chanllawiau a gyhoeddwyd gan yr ICO.

Dylid darllen y polisi hwn ochr yn ochr â'r *Polisi Diogelu Data Ysgolion; Canllaw Digwyddiadau Diogelwch Data Ysgolion; Polisi Diogelwch Gwybodaeth Ysgolion* a *Polisi Prosesu Data Ysgolion.*

Mae'r holl bolisïau, dogfennau a thempledi perthnasol ar gael ar tudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

5. Diffiniadau

Data personol	Unrhyw wybodaeth ynglŷn ag unigolyn naturiol yr adnabyddir neu y gellir ei adnabod yn uniongyrchol neu'n anuniongyrchol drwy'r wybodaeth honno. Gellir ei storio'n ddigidol, ar gyfrifiadur, neu mewn systemau ffeilio ar bapur.
Data categori arbennig	Gwybodaeth ynglŷn â hil, tarddiad ethnig, barn wleidyddol, credoau crefyddol neu athronyddol, aelodaeth undeb llafur (neu ddiffyg aelodaeth), gwybodaeth enetig, gwybodaeth fiometreg (i adnabod unigolyn) unigolyn, a gwybodaeth ynglŷn ag iechyd, bywyd rhywiol neu ogwydd rhywiol unigolyn. Data categori arbennig yw data personol sydd angen amddiffyniad bellach oherwydd ei fod yn sensitif.
Prosesu gwybodaeth	Casglu, derbyn, cofnodi, trefnu, strwythuro, storio, cadw, diwygio, addasu, newid, adennill, ymgynghori, lledaenu, cyfyngu, datgelu, dinistrio, cael gwared â gwybodaeth, ei defnyddio neu gwneud unrhyw beth â hi.
Rheolydd data	Y bobl neu'r sefydliadau sy'n pennu'r pwrpasau dros brosesu data personol, ac ym mha fodd y caiff ei brosesu. Mae gan y rheolydd data gyfrifoldeb i sefydlu ymarferion a pholisïau yn unol â deddfwriaeth. Yr ysgol yw'r rheolydd data.
Proseswyr data	Yn cynnwys unrhyw berson sy'n prosesu data personol ar ran rheolydd data (heblaw am y sawl sy'n gyflogedig gan y rheolydd data). Gall proseswyr data gynnwys cyflenwyr sy'n ymdrin â data personol ar ran yr ysgol.
Gwrthrych y data	Yr unigolyn y mae'r wybodaeth bersonol yn ymwneud ag ef neu hi.
Systemau Gwybodaeth	Cyfrifiaduron prosesu gwybodaeth neu systemau cyfathrebu data.
Cywirdeb	Cadw'r wybodaeth yn gyflawn, yn gywir ac yn ddilys.
Risg	Effaith ansicrwydd ar amcanion. Risgiau i unigolion: y potensial am ddifrod neu drallod. Nodweddir risg yn aml gan gyfeirio at "ddigwyddiadau" a "chanlyniadau" posibl, neu gyfuniad o'r rhain.
Asesiad Risg	Adnabyddiad a dadansoddiad o risgiau i amcanion busnes y sefydliad.
Effaith	Beth fyddai canlyniadau'r risg pe bai'n digwydd. Effaith yn cael ei ystyried fel un sy'n cael effaith uniongyrchol neu effaith yn y dyfodol.
Tebygolrwydd	Pa mor debygol yw'r risg o ddigwydd – ansicrwydd, siawns a thebygolrwydd.
Rheolaeth	Mesur sy'n addasu risg.
Bygythiad	Achos potensial o ddigwyddiad dieisiau, y gall arwain at niwed i system neu sefydliad.
Anawdurdodedig	Heb hawl cyfreithlon.
Ffugenwau	Y broses lle prosesir gwybodaeth bersonol mewn ffordd na ellir ei defnyddio i adnabod unigolyn heb ddefnyddio gwybodaeth ychwanegol, a gadwir ar wahân ac yn amodol ar fesurau technegol a sefydliadol i sicrhau na ellir priodoli gwybodaeth bersonol i unigolyn a ellir ei adnabod.

Gwybodaeth Trydydd Parti	Trydydd parti yw rhywun nad yw'n rheolwr data, yn brosesydd data nac yn wrthrych i'r data.
Swyddfa'r Comisiynydd Gwybodaeth (ICO)	Yr ICO yw corff annibynnol y DU (awdurdod goruchwylio) a sefydlwyd i gynnal hawliau gwybodaeth. Rôl yr ICO yw cynnal hawliau gwybodaeth er budd y cyhoedd. Mae hyn yn cynnwys ymdrin â chwynion ynghylch problemau, cael gafael ar wybodaeth bersonol gan sefydliad, neu os oes pryderon ynghylch sut mae sefydliad wedi ymdrin â gwybodaeth - os yw'r wybodaeth yn anghywir, wedi'i cholli neu ei datgelu i rywun arall. Adroddir am achosion o dorri data sy'n risg uchel i unigolion i'r ICO.

6. Digwyddiad Diogelwch Data

Digwyddiad diogelwch data yw digwyddiad diogelwch sy'n arwain at ddinistrio, colli, addasu, datgelu anawdurdodedig neu fynediad at ddata personol a drosglwyddir, a storir neu a brosesir mewn unrhyw ddull arall gan yr ysgol, yn ddamweiniol neu'n anghyfreithlon.

Mae enghreifftiau o ddigwyddiadau diogelwch data yn cynnwys:

- colli neu ddwyn data neu offer y mae gwybodaeth bersonol yn cael ei storio arno e.e. gwybodaeth neu offer TG (gliniaduron, tabledi, ffonau symudol, dyfeisiau sy'n cynnwys data personol fel cofion bach);
- gwall dynol fel data'n cael ei rannu gyda derbynnydd anfwriadol drwy e-bostio gwybodaeth i gyfeiriad e-bost anghywir; gwybodaeth bersonol yn cael ei gadael mewn lleoliad ansefydlog; uwchlwytho gwybodaeth bersonol i wefan neu gyfrif cyfryngau cymdeithasol;
- mynediad heb awdurdod at wybodaeth bersonol neu gwybodaeth bersonol yn cael ei defnyddio naill ai gan aelod o staff neu drydydd parti gan gynnwys rheolaethau mynediad amhriodol, gan arwain at gyfrifon defnyddwyr yn cael eu cyfaddawdu, sydd yna'n arwain at fynediad heb awdurdod at ddata;
- methiant offer neu systemau TG (gan gynnwys caledwedd a meddalwedd) sy'n arwain at golli data neu anargaeledd data a gadwir arno;
- difrodi, dinistrio neu golli data personol; newid neu ddileu data personol yn ddamweiniol neu'n anghyfreithlon (e.e. oherwydd methiant cyfarpar neu wall dynol);
- colli data neu offer drwy ddigwyddiadau naturiol nas rhagwelwyd fel tân neu lifogydd;
- ymosodiadau bwriadol ar systemau TG a seiberfwlio fel hacio, firysau, sgamiau *"phishing"* neu haint drwgwedd;
- lle ceir gwybodaeth drwy dwyllo aelod o staff;
- torri mewn i fynediad/diogelwch adeiladau corfforol;
- newidiadau anarferol neu heb reolaeth i'r system;
- storio a/neu waredu offer TG yn amhriodol.

Mae tri chategori o ddigwyddiadau diogelwch data:

- **digwyddiad cyfrinachedd** - lle datgelir data personol neu le ceir mynediad ato yn anawdurdodedig neu'n ddamweiniol;

- **digwyddiad cywirdeb** – lle mae data personol yn cael ei newid yn anawdurdodedig neu'n ddamweiniol;
- **digwyddiad argaeledd** – lle mae colled mynediad at, neu ddinistr i ddata personol yn ddamweiniol neu'n anawdurdodedig.

Gall digwyddiad diogelwch data o bosib cael ystod o effeithiau anffafriol arwyddocaol ar unigolion, y gall arwain at drallod emosiynol ac/neu ddifrod corfforol, materol neu anfaterol. Gall y rhain gynnwys:

- coll rheolaeth dros eu data personol;
- cyfyngiadau ar eu hawliau;
- anffafriaeth;
- lladrad neu dwyll hunaniaeth;
- colled ariannol;
- gwrthdroad anawdurdodedig o ffugenw;
- difrod i enw da;
- coll cyfrinachedd data personol yr amddiffynnir gan gyfrinachedd proffesiynol;
- unrhyw anfantais economeg neu gymdeithasol i'r unigolion hynny.

Er mwyn lleihau'r risg o ddigwyddiadau diogelwch data gymryd lle, bydd yr ysgol yn sicrhau bod:

- ei holl staff wedi ymgymryd â hyfforddiant diogelu data;
- y polisïau a'r gweithdrefnau priodol wedi eu gweithredu a'u gorfodi'n llawn;
- rheolyddion technegol priodol ar waith;
- rheolyddion trefniadol priodol ar waith;
- risgiau yn cael eu rheoli'n ddigonol;
- gwersi'n cael eu dysgu o ddigwyddiadau diogelwch data.

Dylid cymryd gofal i ddiogelu'r math hwn o wybodaeth bersonol, i sicrhau na chaiff ei newid (un ai'n ddamweiniol neu'n fwriadol), ei golli, ei ddwyn nac yn cael ei rhoi yn y dwylo anghywir, a bod ei dilysrwydd a'i chywirdeb yn cael ei chynnal bob amser.

Mae'n bwysig bod yr ysgol yn gallu adnabod digwyddiadau diogelwch data; i asesu'r risg i unigolion ac yna hysbysu os oes angen. Mae'n rhaid i'r ysgol fod â gweithdrefnau cadarn ar waith i adnabod, ymchwilio ac adrodd yn fewnol ar ddigwyddiadau diogelwch data i allu gwneud hyn.

7. Cyfyngiant ac Adfer

Nid ymateb cychwynnol yn unig i ymchwilio ac ymatal y sefyllfa fydd ei angen pan fydd digwyddiad diogelwch data yn digwydd, bydd hefyd angen cynllun adfer sy'n cynnwys, lle bo'n briodol, cyfyngiant ar ddifrod.

7.1. Ymchwilio i Ddigwyddiad Diogelwch Data
Mae'n rhaid i'r unigolyn cyntaf sy'n darganfod/derbyn hysbysiad o ddigwyddiad diogelwch data neu 'ddigwyddiad agos' roi gwybod i'r Pennaeth/yr unigolyn sy'n gyfrifol am ddiogelu

data yn yr ysgol yn syth. Os yw'r digwyddiad diogelwch data yn digwydd neu'n cael ei ddarganfod y tu allan i oriau gwaith arferol, dylai hyn ddechrau cyn gynted ag sy'n ymarferol.

Mae'n bwysig adrodd ar 'ddigwyddiadau agos' yn ogystal â digwyddiadau gwirioneddol, fel y gall yr ysgol gymryd y cyfle i adnabod unrhyw wersi a ddysgwyd.

Bydd yr ysgol yn cysylltu â'r Swyddog Diogelu Data Ysgolion fel y prif bwynt cyswllt i adrodd ar yr holl ddigwyddiadau diogelwch data/'digwyddiadau agos' cyn gynted â phosib a dim hwyrach na 24 awr ar ôl dod yn ymwybodol o'r digwyddiad diogelwch data. Bydd yr ysgol yn sicrhau bod unrhyw ddigwyddiadau'n cael eu hadrodd i'r Swyddog Diogelu Data Ysgolion, hyd yn oed os oes ansicrwydd ynglŷn ag a yw'n ddigwyddiad diogelwch data ai peidio.

Pan ddarganfyddir digwyddiad diogelwch data gan sefydliad sy'n prosesu data ar ran yr ysgol (prosesydd data), mae'n rhaid iddynt hysbysu'r ysgol heb oediad diangen h.y. cyn gynted ag y daw'r prosesydd yn ymwybodol o'r digwyddiad. Mae'n rhaid adnabod pob digwyddiad diogelwch data a'u hadrodd i'r ysgol, waeth beth yw maint y digwyddiad a'r niwed neu'r potensial o niwed.

Dylai'r Pennaeth adnabod aelod priodol o staff i arwain ar ymchwilio i'r digwyddiad. Dylai gael cefnogaeth ddigonol ac adnoddau priodol.

7.2. Cyfyngu ar Effaith y Digwyddiad Diogelwch Data
Mae'n rhaid i'r ysgol ganfod a yw'r digwyddiad diogelwch data yn dal i ddigwydd. Os ydyw, mae'n rhaid cymryd camau yn syth i leihau effaith y digwyddiad.

Mi fydd angen sicrhau bod y wybodaeth yn cael ei chasglu/dychwelyd ac ei dinistro yn syth fel cam cyntaf pan mae'r ysgol yn dod yn ymwybodol o'r digwyddiad.

Bydd y camau gweithredu priodol a'r adnoddau sydd eu hangen i gyfyngu effaith y digwyddiad yn cael eu penderfynu. Bydd angen cymryd unrhyw fesurau angenrheidiol i ymdrin, cyfyngu a lliniaru'r digwyddiad diogelwch data yn ogystal ag unrhyw gamau adfer neu adennill os oes angen. Mae hyn yn cynnwys cyfyngu ar gwmpas ac effaith y digwyddiad diogelwch data. Gall camau gynnwys:

- cau system i lawr;
- ynysu neu gau proses;
- hysbysu staff perthnasol yn yr ysgol;
- ceisio adennill offer sydd ar goll;
- cysylltu â'r Gwasanaeth Dysgu neu Wasanaethau Cyngor perthnasol eraill fel eu bod wedi eu paratoi ar gyfer unrhyw ymholiadau posib;
- cysylltu â thîm cyfathrebu'r Cyngor fel y gallent baratoi i ymdrin ag unrhyw ymholiadau gwasg;
- defnyddio ffeiliau wrth gefn i adfer data coll/wedi ei ddifrodi/wedi ei ddwyn;
- newid unrhyw godau mynediad neu gyfrineiriau yn syth os yw'r digwyddiad yn cynnwys unrhyw godau mynediad neu gyfrineiriau.

Mae sefydlu pwy sydd angen eu hysbysu o'r digwyddiad diogelwch data ar y pwynt hwn yn angenrheidiol, ac adnabod sut y gallent gynorthwyo â'r broses gyfyngiant.

8. Asesu'r Risgiau

Yn ogystal â sefydlu graddfa ac achos y digwyddiad diogelwch data, dylai'r ymchwiliad ystyried y risgiau i'r:

- unigolion (y sawl a gollwyd eu gwybodaeth);
- yr ysgol;
- y Cyngor.

Mae'n bwysig asesu'r risgiau y gall fod ynghlwm â'r digwyddiad diogelwch data gan ystyried y canlyniadau anffafriol posib i unigolion; pa mor ddifrifol neu sylweddol yw'r rhain a pa mor debygol ydynt o ddigwydd.

Bydd yr ymchwiliad yn ystyried y pwyntiau canlynol:

- y math o wybodaeth sydd ynghlwm;
- sensitifrwydd yr wybodaeth;
- pa amddiffyniadau sydd ar waith (e.e. amgryptio);
- beth sydd wedi digwydd i'r wybodaeth;
- p'run ai a ellir defnyddio'r wybodaeth yn anghyfreithlon neu'n amhriodol;
- faint o bobl a effeithir arnynt;
- pa fath o unigolion sydd wedi eu heffeithio;
- pa niwed y gall ddigwydd i'r unigolion hyn;
- p'run ai a oes canlyniadau ehangach i'r digwyddiad diogelwch data.

9. Ffurflen Ymchwilio i Ddigwyddiad Diogelwch Data Ysgolion

Bydd angen cwblhau *Ffurflen Ymchwilio i Ddigwyddiad Diogelwch Data Ysgolion* heb oediad diangen er mwyn adrodd ar y digwyddiad diogelwch data. Cynhwysir arweiniad ar gwblhau'r ffurflen ymchwilio yn y *Canllaw Digwyddiad Diogelwch Data Ysgolion.* Mae'r ffurflen a'r canllaw ar gael ar tudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu. Gellir cael rhagor o wybodaeth gan y Swyddog Diogelu Data Ysgolion.

Mae'r *Ffurflen Ymchwilio i Ddigwyddiad Diogelwch Data Ysgolion* yn darparu cofnod ysgrifenedig o'r broses ymchwilio i ddigwyddiad diogelwch data. Mae'n rhaid cwblhau'r ffurflen pryd bynnag y mae **data personol wedi ei gyfaddawdu** fel bod gan ysgolion dystiolaeth o'r camau a gymerodd i liniaru.

Bydd y ffurflen yn annog yr ysgol i ganfod data pwy oedd ynghlwm â'r digwyddiad diogelwch data; yr effaith bosib ar y gwrthrych data a pha gamau pellach sydd angen eu cymryd i liniaru'r sefyllfa.

Mae'n bwysig bod y ffurflen hon yn cael ei chwblhau'n gywir fel y gellir ystyried ffeithiau ac amgylchiadau'r digwyddiad yn llawn ac fel y gellir cymryd camau cadarnhaol i leihau ac i liniaru'r effeithiau i unigolion a'r ysgol.

Mae tair rhan i'r ffurflen hon:

- Dylai'r swyddog ymchwilio gwblhau a llofnodi **Rhan A**;
- Mae **Rhan B** wedi ei chyflwyno i gael ymateb y Pennaeth/aelod o'r Uwch Dîm Rheoli a fydd yn gallu adnabod gwelliannau er mwyn lleihau'r posibilrwydd o ddigwyddiad tebyg yn y dyfodol;
- Y Swyddog Diogelu Data Ysgolion sydd i gwblhau **Rhan C** er mwyn darparu argymhellion parthed adrodd i'r ICO.

10. Hysbysiad o Ddigwyddiadau Diogelwch Data

Gall hysbysu pobl a sefydliadau bod digwyddiad diogelwch data wedi digwydd fod yn elfen bwysig yn y strategaeth rheoli digwyddiad diogelwch data. Dylai hysbysiad fod â phwrpas clir.

10.1. Asesu'r Angen i Adrodd yr Wybodaeth i Swyddog y Comisiynydd Gwybodaeth (ICO)
Bydd rhaid i'r ysgol a'r Swyddog Diogelu Data Ysgolion ystyried tebygolrwydd a difrifoldeb y risg i hawliau a rhyddid pobl yn dilyn y digwyddiad diogelwch data. Os yw digwyddiad diogelwch data'n debygol o arwain at risg i hawliau a rhyddid unigolion, mae'n ddigwyddiad adroddadwy y bydd rhaid i'r Swyddog Diogelu Data Ysgolion adrodd i'r ICO, heb oediad diangen, ond ddim hwyrach na **72 awr** ers dod yn ymwybodol o'r digwyddiad diogelwch data. Os oes angen cymryd mwy na 72 awr i adrodd, mae'n rhaid darparu rhesymau dros yr oediad.

Yn dilyn cwblhau asesiad, os yw'n annhebygol bod risg i hawliau a rhyddid unigolion, ni fydd rhaid i'r ysgol adrodd ar y digwyddiad diogelwch data i'r ICO. Nid oes rhaid adrodd ar bob ddigwyddiad diogelwch data i'r ICO, ond mae'n rhaid i'r ysgol ddogfennu **bob** digwyddiad diogelwch data. Bydd rhaid i'r ysgol hefyd allu cyfiawnhau'r penderfyniad i beidio ag adrodd i'r ICO, felly mae'n rhaid dogfennu hyn hefyd.

Y Swyddog Diogelu Data Ysgolion sydd i wneud y penderfyniad a oes angen adrodd ar ddigwyddiad diogelwch data i'r ICO. Bydd pob digwyddiad yn cael ei ystyried fesul achos.

Y Swyddog Diogelu Data Ysgolion fydd yn hysbysu'r ICO o unrhyw ddigwyddiadau diogelwch data yn yr ysgol gan ddarparu unrhyw wybodaeth berthnasol sydd ei hangen er mwyn adrodd. Efallai y bydd yn fwy priodol mewn rhai achlysuron i'r ysgol ei hun adrodd ar y digwyddiad diogelwch data, yn dibynnu ar yr amgylchiadau.

10.2. Darparu Gwybodaeth i Swyddfa'r Comisiynydd Gwybodaeth (ICO)
Efallai y bydd gwybodaeth yn cael ei darparu i'r ICO mewn rhannau os nad yw ar gael yn gychwynnol gan yr ysgol. Bydd yr ysgol yn darparu cymaint o wybodaeth â phosib yn y man cyntaf i'r Swyddog Diogelu Data Ysgolion ac yn sicrhau bod yr wybodaeth a rennir yn gywir.

Os oes unrhyw beth yn newid o'r amser y rhoddir yr hysbysiad cychwynnol i'r ICO, bydd rhaid i'r ysgol ddiweddaru'r Swyddog Diogelu Data Ysgolion cyn gynted â phosib, a bydd y Swyddog Diogelu Data Ysgolion yn ystyried a fydd angen diweddaru'r ICO ar y newidiadau i'r digwyddiad diogelwch data.

Bydd yr ICO angen yr wybodaeth ganlynol:

- manylion ynglŷn â beth ddigwyddodd;
- pa bryd y digwyddodd a pa bryd y daeth yr ysgol yn ymwybodol ohono;
- sut y digwyddodd;
- mesurau sydd ar waith y gall fod wedi rhwystro'r digwyddiad;
- faint o bobl y gellir eu heffeithio;
- y niwed gwirioneddol neu botensial i bobl;
- mesurau a gymerwyd i gynorthwyo'r sawl a effeithir;
- sut gall yr ysgol atal digwyddiadau tebyg yn y dyfodol.

Adroddir ar ddigwyddiad diogelwch data i'r ICO dros eu llinell ffôn neu drwy eu ffurflen ar-lein. Bydd angen i ysgolion arddangos bod ei hymateb i'r digwyddiad diogelwch data yn:

- gyflym ac yn effeithiol;
- bod hawliau a rhyddid y gwrthrychau data wedi eu hamddiffyn; a
- bod yr ysgol yn cymryd camau i sicrhau nad yw'r digwyddiad aflonyddgar yn digwydd eto.

10.3. Hysbysu Unigolion
Efallai y bydd angen hysbysu'r unigolion yr effeithir arnynt heb oediad diangen os yw digwyddiad diogelwch data yn debygol o arwain at risg **uchel** i'w hawliau a'u rhyddid. Mae 'risg uchel' yn golygu bod y trothwy i hysbysu unigolion yn uwch na hynny ar gyfer hysbysu'r ICO.

Bydd yr ysgol yn ymofyn am gyngor a chefnogaeth y Swyddog Diogelu Data Ysgolion ynglŷn â hysbysu unigolion am y digwyddiad diogelwch data. Bydd difrifoldeb yr effaith wirioneddol neu'r potensial o effaith ar unigolion o ganlyniad i ddigwyddiad diogelwch data a'r tebygolrwydd o hyn yn digwydd yn cael ei asesu.

Bydd y Swyddog Diogelu Data Ysgolion yn hysbysu'r sawl yr effeithir arnynt heb oediad diangen, yn arbennig os oes angen lliniaru risg uniongyrchol o ddifrod iddynt. Efallai y bydd yn fwy priodol ar rai achlysuron i'r ysgol ei hun hysbysu unigolion, yn dibynnu ar yr amgylchiadau.

Mae hysbysiad yn gyfreithiol ofynnol, ac mae'n rhaid i'r cyfathrebiad fod mewn iaith glir a phlaen. Dylid darparu'r canlynol i unigolion yr effeithir gan ddigwyddiad diogelwch data:

- disgrifiad o sut a pha bryd y digwyddodd y digwyddiad diogelwch data a pha ddata oedd yn gysylltiedig;
- disgrifiad o ganlyniadau tebygol y digwyddiad diogelwch data;

- manylion o'r hyn sydd wedi ei wneud i ymateb i'r risgiau a ddaw yn sgil y digwyddiad diogelwch data;
- cyngor penodol a chlir ar y camau y gallent gymryd i amddiffyn eu hunain a hefyd be gall yr ysgol ei wneud i'w cynorthwyo;
- enw a manylion cyswllt y Swyddog Diogelu Data Ysgolion; a
- ffordd y gallent gysylltu â'r ysgol am wybodaeth bellach.

Bydd unigolion hefyd yn cael y cyfle i wneud cwyn ffurfiol dan *Weithdrefn Gwynion* yr ysgol.

Mae gan yr ICO y pŵer i orfodi'r ysgol i hysbysu unigolion yr effeithir os ydynt yn ystyried bod risg uchel. Bydd yr ysgol yn dogfennu ei holl benderfyniadau ynglŷn â hysbysu unigolion.

10.4. Hysbysu Trydydd Parti
Efallai y bydd rhaid hysbysu trydydd bartïon neu asiantaethau fel rhan o'r cyfyngiant cychwynnol. Fodd bynnag, bydd y penderfyniad gan amlaf yn cael ei wneud unwaith y bydd ymchwiliad wedi ei gynnal.

Rhaid hefyd ystyried a fydd angen hysbysu'r Heddlu. Byddai hyn yn briodol lle mae gweithgaredd anghyfreithlon yn wybyddus neu os tybir ei fod wedi digwydd, neu lle mae risg y bydd gweithgaredd anghyfreithlon yn digwydd yn y dyfodol.

Efallai y bydd hefyd yn briodol i hysbysu trydydd bartïon perthnasol eraill megis yswirwyr, noddwyr a chontractwyr os yn briodol.

Bydd yr ysgol yn ymofyn am gyngor a chefnogaeth y Swyddog Diogelu Data Ysgolion ynglŷn â hysbysu trydydd bartïon am y digwyddiad diogelwch data.

11. Arfarniad ac Ymateb

Mae'n bwysig nid yn unig i ymchwilio i achosion y digwyddiad diogelwch data, ond hefyd i werthuso effeithiolrwydd yr ymateb iddo. Yn ogystal â hyn, gellir cwblhau adolygiad pellach o achosion y digwyddiad diogelwch data ac argymhellion ar gyfer gwelliannau dyfodol unwaith y bydd y mater wedi ei ddatrys.

Os achoswyd y digwyddiad diogelwch data gan broblemau systemig ac/neu gyfredol, yna nid yw cyfyngu'r digwyddiad diogelwch data a pharhau gyda 'busnes fel arfer' yn dderbyniol. Os adnabyddir problemau systematig neu gyfredol, mae'n rhaid llunio cynllun gweithredu i liniaru'r rhain.

Gall prosesau, gweithdrefnau, ymarferion a mesurau presennol arwain at ddigwyddiad diogelwch data arall felly bydd yr ysgol yn gwerthuso'n feirniadol ac yn adnabod lle gellir gwneud gwelliannau a newidiadau er mwyn lleihau'r risg o rywbeth tebyg yn digwydd eto. Bydd newidiadau yr argymhellir i systemau, polisïau a gweithdrefnau'n cael eu dogfennu a'u rhoi ar waith cyn gynted â phosib.

Os rhoddir ystyriaeth ddigonol i'r materion hyn fel rhan o'r ymchwiliad, gall ymateb i ddigwyddiad diogelwch data arwain at ddeilliannau dysgu cadarnhaol i'r ysgol.

Gall fod yn briodol i rannu adroddiad ynglŷn â rhai digwyddiadau diogelwch data penodol gyda'r corff llywodraethu ysgol. Gellir defnyddio'r adroddiad hwn i ddechrau trafodaeth â'r corff llywodraethu ysgol ynglŷn ag unrhyw newidiadau sydd angen eu gwneud i broses, system neu bolisi o ganlyniad i ddigwyddiad diogelwch data. Mae templed *Adroddiad ar Ddigwyddiad Diogelwch Data i Gorff Llywodraethu Ysgol* ar gael ar tudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

12. Log Digwyddiadau Diogelwch Data ac Adrodd

Mae'n rhaid i'r ysgol gadw cofnod canolog o **unrhyw** ddigwyddiadau diogelwch data a fydd yn cofrestru bob methiant i gydymffurfio drwy *Log Digwyddiadau Diogelwch Data*. Bydd yr ysgol yn cofnodi pob digwyddiad diogelwch data, waeth a ydynt angen eu hadrodd i'r ICO ai pheidio. Bydd y *Log Digwyddiadau Diogelwch Data* yn cofnodi'r ffeithiau sydd ynghlwm â'r digwyddiad; ei effeithiau a'r camau adfer sydd wedi eu cymryd. Bydd dogfennu'r holl fanylion yn cynorthwyo'r ysgol i gydymffurfio ag egwyddor atebolrwydd yr *UK GDPR.*

Bydd y Pennaeth yn adrodd ar y nifer o ddigwyddiadau diogelwch data sydd wedi digwydd yn ystod y flwyddyn ysgol i'r corff llywodraethu a hefyd i'r Swyddog Diogelu Data Ysgolion yn flynyddol. Bydd y Swyddog Diogelu Data Ysgolion yn cadw *Log Digwyddiadau Diogelwch Data* cyffredinol ar gyfer pob ysgol.

Bydd ffigyrau hefyd yn ffurfio rhan o ffigyrau cyfunol ar gyfer ysgolion yn adroddiad sicrwydd llywodraethu gwybodaeth blynyddol y Swyddog Diogelu Data Ysgolion a gyflwynir i'r Uwch Dîm Rheoli ac i Bwyllgor Archwilio a Llywodraethu Cyngor Sir Ynys Môn.

Mae templed o'r *Log Digwyddiadau Diogelwch Data Ysgolion* ar gael ar tudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

13. Methiant i Hysbysu

Mae'n rhaid i'r holl staff fod yn agored ynglŷn ag unrhyw ddigwyddiad diogelwch data fel y gall yr ysgol sicrhau ei bod yn ymddwyn yn gyfrifol; yn cefnogi aelodau o staff ac yn delio â'r digwyddiad cyn gynted â phosib a mor effeithiol â phosib.

Drwy beidio ag adrodd ar ddigwyddiad diogelwch data y dylai fod wedi cael ei adrodd i'r ICO, gall fod canlyniadau i'r ysgol ac i'r aelod unigol o staff.

Wrth i ysgol fethu â hysbysu yr ICO ac/neu wrthrych data bod digwyddiad diogelwch data wedi bod, bydd yr ICO yn ystyried yr holl fesurau cywirol y gallent eu gosod sydd yn ddirwyon gweinyddol yn ogystal â, neu'n hytrach na'r pwerau cywirol.

Mae'r dirwyon gweinyddol yn disgyn i strwythur dwy haen, sy'n golygu y gellir rhoi dirwy lefel is i sefydliad, neu ddirwy lefel uwch, yn dibynnu ar natur y digwyddiad:

- gellir rhoi dirwy haen is o €10 miliwn (neu gyfwerth mewn punnoedd) neu 2% o'r trosiant blynyddol byd-eang ar gyfer y flwyddyn ariannol flaenorol (pa bynnag un yw'r mwyaf) am fethu â hysbysu'r ICO neu unigolion o ddigwyddiadau;

- bydd dirwy haen uwch o €20 miliwn (neu gyfwerth mewn punnoedd) neu 4% o'r trosiad blynyddol byd-eang ar gyfer y flwyddyn ariannol flaenorol (pa bynnag un yw'r mwyaf) am dorri unrhyw rai o'r egwyddorion prosesu data.

Mae pwerau cywirol yn cynnwys y gallu i roi rhybuddion neu geryddon; rhoi gorchmynion i reolwyr a phrosesyddion i gydymffurfio â cheisiadau gwrthrych data a rhoi gorchymyn i reolwr i gyfathrebu digwyddiad diogelwch data personol yn uniongyrchol i'r gwrthrych data.

Wrth benderfynu ar ba lefel o ddirwy i roi, bydd yr ICO yn ystyried ffactorau megis:

- **natur, difrifoldeb** a **hyd** y digwyddiad;
- y nifer o wrthrychau data a effeithir arnynt, a'r lefel o ddifrod a ddioddefir ganddynt;
- p'run ai oedd yr ysgol yn torri'r *UK GDPR* yn **fwriadol**, ynteu a oedd yn **esgeulus** o'i rhwymedigaethau dan yr *UK GDPR*;
- **graddfa'r cydymffurfiad** â'r ICO; a'r
- **categorïau o ddata** a gynhwysir.

14. Torri'r Polisi

Gall diffyg cydymffurfio â'r polisi hwn gan aelodau o staff ysgol arwain ar ganlyniadau difrifol i'r ysgol, yr aelod unigol o staff a'r Cyngor.

Mae'n bwysig i'r holl aelodau o staff chwarae eu rhan mewn adrodd ar ddigwyddiad. Gall methu â glynu at y polisi hwn neu anwybyddu digwyddiad diogelwch data posib arwain at gamau disgyblaethol. Eir i'r afael â hyn drwy'r broses ddisgyblu berthnasol a chymalau cytundebol trydydd parti (fel sy'n berthnasol).

Os yw'r digwyddiad diogelwch data yn gofyn am ymchwiliad disgyblaethol, bydd y Pennaeth yn llythyru ag Adnoddau Dynol am gyngor ac arweiniad.

15. Adolygu'r Polisi a Threfniadau Arolygiaeth

Bydd y polisi hwn yn cael ei adolygu gan y Swyddog Diogelu Data Ysgolion bob dwy flynedd, oni bai bod newidiadau i ddeddfwriaeth, codau ymarfer, canllawiau neu gyngor gan y comisiynydd neu wendidau newydd sy'n gofyn am adolygu'r polisi ynghynt.

Bydd y polisi'n cael ei gymeradwyo gan yr Uwch Dîm Rheoli Dysgu ac yn cael ei fabwysiadu gan gorff llywodraethu'r ysgol. Bydd cydymffurfiad â'r polisi hwn a'r gweithdrefnau sydd ynghlwm yn cael eu monitro gan Dîm Arweinyddol a chorff llywodraethu'r ysgol.

Os oes unrhyw ymholiadau neu bryderon ynglŷn ag unrhyw beth yn y polisi hwn, dylid cysylltu â'r Swyddog Diogelu Data Ysgolion heb oediad.

E-bost: dpoysgolionmon@ynysmon.gov.uk

Ffôn: 01248 751833

Cyfeiriad:
Gwasanaeth Dysgu
Swyddfeydd y Cyngor
Cyngor Sir Ynys Môn
Llangefni
Ynys Môn
LL77 7TW

Gellir cael rhagor o wybodaeth ynglŷn â digwyddiadau diogelwch data ar wefan yr ICO: https://ico.org.uk/

Content **Page**

1. Policy Statement

This policy sets out the procedure to be followed by the school and how it will comply with data protection obligations in the event of a data breach. It ensures a consistent and effective approach to the management of data breaches and establishes a structure for the reporting of such incidents.

The school is fully committed that it ensures full compliance with data protection legislation and ensures that it is meeting its legal, statutory and regulatory requirements under the *UK GDPR.* The school will ensure that appropriate action is taken immediately to minimise the impact on individuals; to mitigate associated risks and to repair any damage.

The school expects all staff to embed security and prevention practices in their day-to-day work to ensure information is protected and must take appropriate steps to safeguard all information.

The school will consult and seek the advice of the Schools Data Protection Officer relating to any incidents, issues, concerns or questions regarding data breaches.

2. Scope

This policy applies to all employees of the school and those working on behalf of the school, including school governors and contractors, who have access to and/or process the school's information.

This policy applies to all personal and special category information held by the school.

It relates to information held in all formats including, but not limited to, paper, electronic, audio and visual. The school holds personal information, both in hard and soft copy, and utilises various information systems that hold personal data, which are all covered by this policy.

Data breaches include both confirmed and suspected incidents.

3. Responsibilities

3.1. School Governing Body
The school governing body has the responsibility for:

- monitoring the school's overall compliance and accountability relating to this policy;
- ensuring that the school can evidence compliance with data protection legislation.

3.2. Headteacher (and/or Person Responsible for Data Protection within the School)
The Headteacher and/or the person who is responsible for data protection within the school is responsible for ensuring that:

- there is a process in place to protect all personal and special category information within the school;
- there is a robust process in place to detect and identify data breaches; to investigate and assess breaches including risks and to report and notify of any data breaches;
- steps are taken immediately to minimise the effects of data breach incidents and to determine the appropriate course of action and the required resources needed to limit the impact of data breaches;
- *Schools Data Breach Investigation Forms* are completed as soon as possible; contain detailed and accurate information and are immediately shared with the Schools Data Protection Officer;
- a central record of all data breaches is kept via a *Data Breach Log;*
- annual figures regarding the total number of data breach incidents that have occurred during the school year is presented to the school governing body and also to the Schools Data Protection Officer;
- lessons are learnt from previous data breaches and that action plans are implemented in order to change and improve procedures and practices where required;
- the Schools Data Protection Officer is fully informed of all details regarding the breach and is a main contact point for the Schools Data Protection Officer whilst dealing with data breaches;
- all staff comply with this policy; are aware of the data breach process and staff assist with investigations as required.

3.3. Schools Data Protection Officer
The Schools Data Protection Officer is responsible for:

- being the primary point of contact for the school to report all data breach incidents/'near misses' to;
- informing and advising schools on their obligations regarding data breaches;
- creating and regularly reviewing procedures, policies, guidance and templates regarding data breaches;
- providing advice and support to the school regarding any necessary measures to address, contain and mitigate data breaches;
- completing Part C of the *Schools Data Breach Investigation Form* in order to provide recommendations concerning reporting data breaches to the ICO;
- providing advice and support to the school regarding notifying third parties about data breaches;
- making the decision whether or not a data breach needs to be reported to the ICO;
- notifying the ICO of any reportable data breaches;
- notifying affected individuals if a data breach is likely to result in a high risk to their rights and freedoms;
- supporting the school in relation to lessons learnt and creating action plans in order to change and improve procedures and practices where required;

- gathering information from the Headteacher regarding the total number of data breach incidents that have occurred during the school year and keeping an overall *Data Breach Log* for all schools.

3.4. All Staff within the School

All staff employed or volunteering within the school, including teachers, classroom assistants and business support staff are responsible for ensuring that they:

- familiarise themselves and fully comply with this policy;
- immediately report all actual, suspected, threatened or potential data breaches to the Headteacher and/or the person who is responsible for data protection within the school;
- assist with investigations as required, particularly if urgent action must be taken to prevent further damage.

If staff have any queries, they should discuss these with the Headteacher; the officer responsible for data protection within the school or with the Schools Data Protection Officer.

4. Legislation, Guidance and Policies

The school has a mandatory duty to ensure that personal data is protected and processed in accordance with the *UK General Data Protection Regulations (UK GDPR*) and the *Data Protection Act 2018.*

The *Data Protection Act 2018* makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding or use of such information.

UK GDPR states that personal information should be *"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"*.

This policy is based on relevant codes of practice and on guidance published by the ICO.

This policy should be read in conjunction with the *Schools Data Protection Policy;* the *Schools Data Breach Guidance*; the *Schools Information Security Policy* and the *Schools Data Processing Policy.*

All relevant policies, documents and templates are available on the Data Protection page on the Learning Service Microsite.

5. Definitions

Personal data	Any information relating to an identified or identifiable natural person that can be identified either directly or indirectly from

	that information. This can be stored electronically, on a computer, or in paper-based filing systems.
Special category data	Information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation. Special category data is personal data that needs more protection because it is sensitive.
Processing information	Collecting, obtaining, recording, organising, structuring, storing, retaining, amending, adapting, altering, retrieving, consulting, disseminating, restricting, disclosing, destroying, erasing information or using or doing anything with it.
Data controller	The people, or organisations, which determine the purposes for which, and the manner in which, any personal data is processed. The data controller has a responsibility to establish practices and policies in line with legislation. The school is the data controller.
Data processors	Includes any person who processes personal data on behalf of a data controller (other than the employee of the data controller). Data processors could include suppliers which handle personal data on behalf of the school.
Data subject	The individual to whom the personal information relates.
Information Systems	Information processing computers or data communication systems.
Integrity	The preservation of the complete, accurate and validated state of information.
Risk	Effect of uncertainty on objectives. Risks to individuals: the potential for damage or distress. Risk is often characterised by reference to potential "events" and "consequences", or a combination of these.
Risk Assessment	The identification and analysis of risks to the organisation's business objectives.
Impact	What are the consequences of the risk were it to occur. Impact is considered as having either an immediate effect or a future effect.
Likelihood	How likely is it that the risk will occur- uncertainty, chance and probability.
Control	Measure that is modifying risk.
Threat	Potential cause of an unwanted incident, which can result in harm to a system or organisation.
Unauthorised	Without a legitimate right.
Pseudonymised	The process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual.
Third-party information	A third party is somebody who is not the data controller, the data processor or the data subject.

Information Commissioner's Office (ICO)	The ICO is the UK's independent body (supervisory authority) set up to uphold information rights. The ICO's role is to uphold information rights in the public interest. This includes dealing with complaints regarding problems accessing personal information from an organisation, or if there are concerns about how an organisation has handled information- if the information is wrong, has been lost or disclosed to someone else. Data breaches that are a high risk to individuals are reported to the ICO.

6. Data Breach

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the school.

Examples of data breach incidents are:

- accidental loss or theft of data or equipment on which personal information is stored e.g. information or IT equipment (laptops, tablets, mobile phones, devices containing personal data such as memory sticks);
- human error such as data shared with an unintended recipient via e-mailing information to an incorrect e-mail address; personal information being left in an insecure location; uploading personal information to a website or social media account;
- unauthorised access to or use of personal information either by a member of staff or third party including inappropriate access controls, resulting in compromised user accounts leading to unauthorised access to data;
- failure of equipment or IT systems (including hardware and software) resulting in loss of data or non-availability of data held on it;
- damage, destruction or loss of personal data; accidental or unlawful alteration or deletion of personal data (e.g. due to equipment failure or human error);
- loss of data or equipment through unforeseen natural events such as fire or flood;
- deliberate attacks on IT systems and cyber incidents such as hacking, viruses, phishing scams or malware infection;
- where information is obtained by deceiving a member of staff;
- breach of physical building access/security;
- unusual or uncontrolled system changes;
- inappropriate storage and/or disposal of IT equipment.

There are three categories of data breaches:

- **confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, personal data;
- **integrity breach** - where there is an unauthorised or accidental alteration of personal data;

- **availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

A data breach can potentially have a range of significant adverse effects on individuals, which can result in emotional distress and/or physical, material, or non-material damage. These can include:

- loss of control over their personal data;
- limitation of their rights;
- discrimination;
- identity theft or fraud;
- financial loss;
- unauthorised reversal of pseudonymisation;
- damage to reputation;
- loss of confidentiality of personal data protected by professional secrecy;
- any other significant economic or social disadvantage to those individuals.

In order to reduce the risk of data breaches occurring, the school will ensure that:

- all staff have undertaken data protection training;
- appropriate policies and procedures have been fully implemented and enforced;
- appropriate technical controls are in place;
- appropriate organisational controls are in place;
- risks are adequately managed;
- lessons are learnt from previous data breaches.

Care should be taken to protect this type of personal information, to ensure that it is not changed (either accidentally or deliberately), lost, stolen or falls in to the wrong hands, and that its authenticity and integrity is maintained at all times.

It is important that the school is able to identify a data breach; to assess the risk to individuals, and then notify if required. The school needs to have robust data breach detection, investigation and internal reporting procedures in place to be able to do this.

7. Containment and Recovery

The data breach incident will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation.

7.1. Investigating the Data Breach
The person who first discovers/receives a report of a data breach or a ‘near miss’ must immediately inform the Headteacher/person responsible for data protection within the school. If the data breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

It is important to report ‘near misses’ as well as actual incidents, so that the school can take the opportunity to identify any lessons learnt.

The school will contact the Schools Data Protection Officer as the primary point of contact to report all data breach incidents/'near misses' as soon as possible and no later than 24 hours of becoming aware of the data breach. The school will ensure that all breaches are reported to the Schools Data Protection Officer, even if there is uncertainty of whether or not it is a breach.

When a personal data breach is detected by an organisation that processes data on behalf of the school (data processor), they must notify the school without undue delay i.e. as soon as the processor has become aware of the breach. All data breaches have to be identified and reported to the school, regardless of size and regardless of the harm or potential harm.

An appropriate member of staff should be identified by the Headteacher to take the lead on investigating the incident. They should have sufficient support and have appropriate resources.

7.2. Limiting the Impact of the Data Breach
The school must ascertain whether the data breach is still occurring. If so, steps must be taken immediately to minimise the effect of the incident.

The school will need to ensure that the information is gathered/returned and is destroyed straight away as a first step when the school becomes aware of the incident.

The appropriate course of action and the required resources needed to limit the impact of the incident will be determined. Any necessary measures to address, contain and mitigate the data breach will need to be taken and also any remedial or recovery steps if necessary. This involves limiting the scope and impact of the data breach. Steps might include to:

- shut down a system;
- isolate or close a process;
- alert relevant staff within the school;
- attempt to recover lost equipment;
- contact the Learning Service or any other relevant Council Services, so that they are prepared for any potential enquiries;
- contact the Council's communication team so they can be prepared to handle any press enquiries;
- use backups to restore lost/damaged/stolen data;
- immediately change any access codes or passwords if the incident includes any access codes or passwords.

Establishing who needs to be made aware of the data breach at this point is necessary, and identifying how they could assist the containment process.

8. Assessing the Risks

The investigation should, in addition to establishing the extent and cause of the data breach, consider the risks posed to:

- the individuals (the subjects of the lost information);
- the school;
- the Council.

It is important to assess the risks which may be associated with the data breach considering the potential adverse consequences for individuals; how serious or substantial these are and how likely they are to happen.

The investigation will consider the following points:

- the type of information involved;
- the sensitivity of the information;
- what protections are in place (e.g. encryption);
- what has happened to the information;
- whether the information could be put to any illegal or inappropriate use;
- how many people are affected;
- what type of individuals have been affected;
- what harm can come to these individuals;
- whether there are wider consequences to the data breach.

9. Schools Data Breach Investigation Form

The *Schools Data Breach Investigation Form* will need to be completed without undue delay in order to report the data breach. Guidance on completing the investigation form is contained in the *Schools Data Breach Incident Guidance*. Both the form and guidance are available on the Data Protection page on the Learning Service Microsite. Additional advice can be obtained from the Schools Data Protection Officer.

The *Schools Data Breach Investigation Form* provides a written record of the investigation process into the data breach. The form must be completed whenever **personal data has been compromised** so that the school has evidence of the steps it has taken to put things right.

The form will prompt the school to ascertain whose data was involved in the data breach incident; the potential effect on the data subject and what further steps need to be taken to remedy the situation.

It is important that this form is completed accurately so that the full facts and circumstances of the data breach can be considered and positive steps taken to minimise and mitigate the risks to individuals and the school.

The form is made up of three parts:

- **Part A** should be completed and signed by the investigating officer;

- **Part B** has been introduced in order to gain the response of the Headteacher/ member of the Senior Management Team who will be able to identify improvements which will reduce the possibility of a similar incident in the future;
- **Part C** is for the Schools Data Protection Officer to complete to provide recommendations concerning reporting to the ICO.

10. Notification of Data Breaches

Informing people and organisations that a data breach incident has taken place can be an important element in the data breach management strategy. Notification should have a clear purpose.

10.1. Assessing the Need to Report to the Information Commissioner's Office (ICO)
The school and the Schools Data Protection Officer will need to consider the likelihood and severity of the risk to people's rights and freedoms, following the data breach. If the data breach is likely to result in a risk to the rights and freedoms of individuals, this is a notifiable breach which the Schools Data Protection Officer is required to report to the ICO, without undue delay, but not later than **72 hours** of becoming aware of the data breach. If there is a need to take longer than 72 hours to report, reasons for the delay must be provided.

Following completing an assessment, if it is unlikely there is a risk to the rights and freedoms of individuals, then the school will not have to report the data breach to the ICO. Not every data breach needs to be reported to the ICO, but the school needs to document **all** data breaches. The school will also need to be able to justify the decision not to report to the ICO, so this also needs to be documented.

It is the School's Data Protection Officer who makes the decision whether or not the data breach needs to be reported to the ICO. Every incident will be considered on a case by case basis.

It is the Schools Data Protection Officer who will notify the ICO of any reportable data breaches with the school providing all relevant information that is needed to be able to report. It may be more appropriate on some occasions for the school itself to report the data breach depending on the circumstances.

10.2. Providing Information to the Information Commissioner's Office (ICO)
Information may be provided to the ICO in phases if all the facts are not initially available to the school. The school will provide as much information as possible in the first instance to the Schools Data Protection Officer and will ensure that the information shared is accurate.

If anything changes from the time the initial notification has been sent to the ICO, the school will need to update the Schools Data Protection Officer as soon as possible and the Schools Data Protection Officer will consider whether the ICO will need to be updated about changes with the data breach.

The ICO will need the following information to be provided:

- details about what happened;
- when it happened and when the school discovered it;
- how it happened;
- measures in place that could have stopped it;
- how many people could be affected;
- the actual or potential detriment to people;
- measures taken to help people affected;
- how can the school stop similar breaches in the future.

A data breach is reported to the ICO via their telephone line or via their online form.

The school will need to be able to demonstrate that the response to the data breach was:

- both rapid and effective;
- that the rights and freedoms of the data subjects were protected; and
- that the school is taking steps to ensure the disruptive incident does not occur again.

10.3. Notifying Individuals

There may be a need to notify the affected individuals without undue delay if a data breach is likely to result in a **high** risk to their rights and freedoms. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.

The school will seek the advice and support of the Schools Data Protection Officer about notifying individuals about the data breach. Both the severity of the potential or actual impact on individuals as a result of a data breach and the likelihood of this occurring will be assessed.

The Schools Data Protection Officer will promptly inform those affected, without undue delay, particularly if there is a need to mitigate an immediate risk of damage to them. It may be more appropriate on some occasions for the school itself to notify individuals, depending on the circumstances.

Notification is required by law and communication must be in clear, plain language. Individuals affected by the data breach should be provided with:

- a description of how and when the data breach occurred and what data was involved;
- a description of the likely consequences of the data breach;
- details of what has been done to respond to the risks posed by the data breach;
- specific and clear advice on the steps they can take to protect themselves and also what the school can do to help them;
- the name and contact details of the Schools Data Protection Officer; and
- a way in which they can contact the school for further information.

Individuals will also be given the opportunity to make a formal complaint under the school's *Complaint Procedure*.

The ICO has the power to compel the school to inform affected individuals if they consider there is a high risk. The school will document all of its decisions regarding informing individuals.

10.4. Third Party Notification
Third parties or agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place.

It must also be considered whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

It may also be appropriate to notify other relevant third parties such as insurers, sponsors and contractors if appropriate.

The school will seek the advice and support of the Schools Data Protection Officer about notifying third parties about the data breach.

11. Evaluation and Response

It is important not only to investigate the causes of the data breach but also to evaluate the effectiveness of the response to it. Also, a further review of the causes of the data breach and recommendations for future improvements can be done once the matter has been resolved.

If the data breach was caused by systemic and/or ongoing problems, then simply containing the data breach and continuing 'business as usual' is not acceptable. If systematic or ongoing problems are identified, then an action plan must be drawn up to put these right.

Existing processes, procedures, practices and measures could result in another data breach therefore the school will critically evaluate and identify where improvements and changes can be made to reduce the risk of the likelihood of a similar incident taking place again. Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible.

If sufficient consideration is given to the issues as part of the investigation, the response to a data breach can result in positive learning outcomes for the school.

It may be appropriate to share a report regarding some specific data breaches with the school governing body. The report can be used to prompt discussion with the school's governing body regarding any changes that need to be made within a process, system or policy as a result of a data breach. The *Schools Data Breach Report to the School*

Governing Body template is available on the Data Protection page on the Learning Service Microsite.

12. Data Breach Log and Reporting

The school must keep a central record of **all** data breaches that will register all compliance failures via a *Data Breach Log.* The school will record all data breaches, regardless of whether or not they need to be reported to the ICO. The *Data Breach Log* records the facts relating to the breach; its effects and the remedial action taken. Documenting all details will assist the school in complying with the *UK GDPR's* accountability principle.

The Headteacher will report the total number of data breach incidents that have occurred during the school year to the governing body and also to the Schools Data Protection Officer on an annual basis. The Schools Data Protection Officer will keep an overall *Data Breach Log* for all schools.

Figures will also form part of collective figures for schools in the Schools Data Protection Officer annual information governance assurance report that is presented to the Learning Senior Management Team and to the Isle of Anglesey County Council's Audit and Governance Committee.

A *Schools Data Breach Log* template is available on the Data Protection page on the Learning Service Microsite.

13. Failure to Notify

All staff need to be open about any data breach incident so that the school ensures that it acts responsibly; supports members of staff and deals with the breach as quickly and efficiently as possible.

Not reporting a data breach that should have been reported to the ICO, may have consequences for the school and for the individual member of staff.

If the school fails to notify either the ICO or data subjects of a data breach or both, then the ICO will consider all of the corrective measures that they can impose which are administrative fines in addition to, or instead of, the corrective powers.

The administrative fines fall into a two-tier structure, which means that organisations can be fined up to either the lower-level fine, or up to the higher-level fine, depending on the nature of the infringement:

- the lower-level fine of €10 million (or equivalent in sterling) or 2% of global annual turnover for the preceding financial year (whichever is greater) can be imposed for failing to notify breaches to the ICO or to individuals;

- the higher-tier fine of €20 million (or equivalent in sterling) or 4% of total global annual turnover in the preceding financial year (whichever is greater) will be imposed for breaching any one of the data processing principles.

Corrective powers include the ability to issue warnings or reprimands; order controllers and processors to comply with data subject requests and order a controller to communicate a personal data breach directly to the data subject.

When determining what level of fine to impose, the ICO will consider factors such as:

- the **nature**, **gravity** and **duration** of the breach;
- the number of data subjects affected, and the level of damage suffered by them;
- whether the school was **intentionally** or **deliberately** infringing the *UK GDPR*, or if it was **negligent** of its obligations under the *UK GDPR;*
- the **degree of cooperation** with the ICO; and
- the **categories of data** involved.

14. Breach of the Policy

Non-compliance with this policy by members of school staff could lead to serious consequences for the school; the individual member of staff and the Council.

It is important that all members of staff play their part in reporting a breach. Failure to adhere to this policy or ignoring a possible data breach may result in disciplinary action. This will be addressed through the relevant disciplinary process and third party contractual clauses (as applicable).

If the data breach warrants a disciplinary investigation, the Headteacher will liaise with Human Resources for advice and guidance.

15. Review of Policy and Oversight Arrangements

This policy will be reviewed by the Schools Data Protection Officer every two years, unless changes to legislation, codes of practice, guidance or commissioner advice, or new vulnerabilities requires the policy to be updated sooner.

The policy will be approved by the Learning Senior Management Team and will be adopted by the school governing body. Compliance with this policy and related procedures will be monitored by the School Leadership Team and the governing body.

If there are any queries or concerns about anything contained in this policy, the Schools Data Protection Officer should be contacted without hesitation:

E-mail: dpoysgolionmon@ynysmon.gov.uk

Telephone: 01248 751833

Address:
Learning Service
Isle of Anglesey County Council
Council Offices
Llangefni
Anglesey
LL77 7TW

Further information regarding data breaches can be obtained from the ICO website:
https://ico.org.uk/