Ysgol y Graig

Polisi Diogelu Data Ysgolion / *Schools Data Protection Policy*

(Fersiwn 1, Rhagfyr 2020 / *Version 1, December 2020*)

Ynglŷn â'r polisi hwn

Mae'r polisi hwn yn amlinellu'r hyn y mae'n rhaid i'r ysgol ei wneud i sicrhau bod gwybodaeth bersonol yn cael ei rheoli a'i hamddiffyn a'i bod yn sicrhau cydymffurfiad cyflawn â deddfwriaeth diogelu data.

Cefnogir y polisi hwn gan adnoddau ar Addysg Môn.

About this policy

This policy outlines what the school needs to do to ensure that personal information is properly managed and protected and that it ensures full compliance with data protection legislation.

This policy is supported by resources on Addysg Môn.

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*	Rhagfyr 2020 / *December* 2020	Polisi newydd / *New policy.*	Ionawr 2021

Dyddiad yr adolygiad nesaf / *Date of next review*	
Bydd y polisi hwn yn cael ei adolygu yn: / *This policy will be reviewed in:*	Hydref 2022 / *October* 2022
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 ddeddfwriaeth diogelu data, sef y *Rheoliad Diogelu Data Cyffredinol (GDPR)* a'r *Ddeddf Diogelu Data 2018. / Policy template on the data protection legislation namely the* General Data Protection Regulation (GDPR*) and the* Data Protection Act 2018.

Cyfrifoldeb:
Responsibility: Cyfrifoldeb y llywodraethwyr ysgol a'r Pennaeth yw sicrhau bod gweithdrefnau ar waith i sicrhau bod yr ysgol yn cydymffurfio â deddfwriaeth diogelu data. / *It is the responsibility of the school governors and the Headteacher to ensure procedures are in place to ensure that the school complies with data protection legislation.*

Cynnwys **Tudalen**

1. Datganiad Polisi

Er mwyn gweithredu'n effeithlon, mae'n rhaid i'r ysgol gasglu a defnyddio gwybodaeth am unigolion y mae'n gweithio gyda. Yn ogystal â hyn, gall fod yn gyfreithiol ofynnol i gasglu a defnyddio gwybodaeth er mwyn cydymffurfio â gofynion Llywodraeth Cymru.

Mae'r polisi hwn yn amlinellu sut mae'r ysgol yn cydymffurfio â rhwymedigaethau diogelu data ac yn ymofyn i ddiogelu gwybodaeth bersonol *(gweler eitem 4 ar gyfer y diffiniad perthnasol*). Mae'r ysgol yn llawn ymrwymedig i sicrhau bod gwybodaeth bersonol yn cael ei rheoli a'i hamddiffyn yn iawn a'i bod yn sicrhau cydymffurfiad llawn â deddfwriaeth diogelu data.

Ei bwrpas hefyd yw sicrhau bod yr holl aelodau staff yn deall ac yn cydymffurfio â'r rheolau yn ymwneud â chasglu, defnyddio a dileu data personol y gallent gael mynediad ato yng nghwrs eu gwaith. Mi fydd yr ysgol yn sicrhau ei fod yn trin gwybodaeth bersonol yn gyfreithlon ac yn gywir.

Bydd yr ysgol yn gwneud pob ymdrech i gwrdd â'i rhwymedigaethau dan y ddeddfwriaeth ac yn adolygu gweithdrefnau'n rheolaidd i sicrhau ei bod yn gwneud hynny. Bydd yr ysgol yn ymgynghori gyda'r Swyddog Diogelu Data Ysgolion ac yn ymofyn am ei chyngor ynglŷn ag unrhyw broblemau, pryderon neu gwestiynau a chyn dechrau ar unrhyw weithgareddau prosesu data newydd.

2. Sgôp

Mae'r polisi hwn yn berthnasol ar gyfer pob gweithiwr, llywodraethwr, contractwr, asiantaeth, cynrychiolydd, a staff dros dro sy'n gweithio i'r ysgol ac sy'n prosesu data personol ar ran yr ysgol.

Mae'r polisi hwn yn berthnasol ar gyfer gwybodaeth bersonol ymgeiswyr swyddi, staff presennol a blaenorol, gan gynnwys gweithwyr, gweithwyr dros dro ac asiantaeth, llywodraethwyr, cyflenwyr, gwirfoddolwyr, hyfforddai/myfyrwyr, ymwelwyr, disgyblion a rhieni/y sawl sydd â'r cyfrifoldeb rhieniol.

Mae'r polisi hwn yn berthnasol ar gyfer yr holl wybodaeth bersonol a grëir neu a ddalir gan yr ysgol ym mha bynnag fformat (gan gynnwys ond ddim wedi'w gyfyngu i bapur, electronig, e-bost, ffilm, fideo, CCTV, delweddau ffotograffig) a sut bynnag y caiff ei storio (er enghraifft system/bas data TGCh, strwythur ffeilio gyriant a rennir, e-bost, cwpwrdd ffeilio, silffoedd a droriau).

Mae'r egwyddorion hefyd yn ymestyn i'r holl wybodaeth mewn cofnodion addysg. Enghreifftiau o hyn fyddai enwau staff a disgyblion, dyddiadau geni, cyfeiriadau, rhifau yswiriant gwladol, marciau ysgol, gwybodaeth feddygol, canlyniadau arholiad, asesiadau AAA, adolygiadau datblygiad a chofnodion disgyblaethol staff.

Nid yw *GDPR* yn berthnasol ar gyfer unigolion sydd wedi marw gan nad yw gwybodaeth am berson sydd wedi marw yn cyfrif fel gwbodaeth personol ac felly ddim yn dod o dan *GDPR.*

3. Deddfwriaeth, Arweiniad a Pholisïau

Y brif ddeddfwriaeth diogelu data y mae'r polisi hwn yn cydymffurfio â hi yw'r *Rheoliad Diogelu Data Cyffredinol (GDPR)* a *Deddf Diogelu Data 2018.*

Mae'r polisi hwn hefyd yn seiliedig ar godau ymarfer ac arweiniad a gyhoeddwyd gan Swyddfa'r Comisiynydd Gwybodaeth (ICO).

Bydd yr ysgol hefyd yn cyfeirio at bolisïau ac arweiniadau mewnol perthnasol eraill sy'n cynnwys rhagor o wybodaeth am ddiogelu gwybodaeth bersonol mewn cyd-destunau eraill. Mae'r rhain i gyd ar gael ar Addysg Môn.

4. Diffiniadau

Data personol	Unrhyw wybodaeth sy'n ymwneud ag unigolyn naturiol sydd wedi ei adnabod neu a ellir ei adnabod yn uniongyrchol neu'n anuniongyrchol o'r wybodaeth honno. Gellir ei storio'n electronig, ar gyfrifiadur neu mewn systemau ffeilio papur.
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.
Digwyddiad diogelwch data	Toriad diogelwch sy'n arwain at ddinistrio, colli, addasu, datgelu neu fynediad anawdurdodedig at ddata personol a drosglwyddir, a storir neu a brosesir mewn unrhyw ddull arall, yn ddamweiniol neu'n anghyfreithlon.
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.
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.
Defnyddwyr data	Yn cynnwys gweithwyr sydd â'u gwaith yn ymwneud â data personol. Mae gan ddefnyddwyr data ddyletswydd i ddiogelu'r wybodaeth y maent yn ymdrin â hi drwy ddilyn polisïau

	diogelu data a diogelwch bob amser. Mae staff a gyflogir gan ysgolion yn ddefnyddwyr 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.
Swyddog Diogelu Data	Mae DPO yn helpu i fonitro cydymffurfiaeth fewnol, hysbysu a chynghori ar rwymedigaethau diogelu data, rhoi cyngor ynghylch Asesiadau Effaith Diogelu Data (DPIAau) a gweithredu fel pwynt cyswllt ar gyfer gwrthrychau data a'r awdurdod goruchwylio.
Gwybodaeth Trydydd Parti	Trydydd parti yw rhywun nad yw'n rheolwr data, yn brosesydd data nac yn wrthrych i'r data.
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 wneud unrhyw beth â hi.
Gwybodaeth am gofnodion troseddol	Gwybodaeth bersonol yn ymwneud ag euogfarnau, troseddau, honiadau, achosion troseddol, a mesurau diogelwch cysylltiedig.
Caniatâd	Gan y gwrthrych data yn golygu unrhyw arwydd rhydd, penodol, gwybodus a diamwys o ddymuniadau gwrthrych y data y mae ef neu hi, drwy ddatganiad neu drwy gam cadarnhaol clir, yn arwydd o gytundeb i brosesu data personol sy'n ymwneud ag ef neu hi. Mae'r baich o ddangos caniatâd ar y rheolydd data.
Ffugenwi	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 dienw	Cael gwared â gwybodaeth a ellir ei defnyddio i adnabod rhywun oddi ar rywbeth (megis data cyfrifiadur) fel na ellir gwybod beth oedd y ffynhonnell wreiddiol na'i hadnabod.
Data genetig	Data personol sy'n ymwneud â nodweddion genetig person a etifeddwyd neu a gaffaelwyd sy'n rhoi gwybodaeth unigryw am ffisioleg neu iechyd y person naturiol hwnnw ac sy'n deillio, yn benodol, o ddadansoddiad o sampl biolegol gan y person naturiol dan sylw.
Data biometrig	Data personol sy'n deillio o brosesu technegol penodol sy'n ymwneud â nodweddion corfforol, ffisiolegol neu ymddygiadol person naturiol, sy'n caniatáu neu'n cadarnhau adnabyddiaeth unigryw'r person naturiol hwnnw, megis delweddau wyneb neu ddata dactyloscopig. Mae cydnabyddiaeth ôl bys yn enghraifft o ddata dactyloscopig.
Data ynghylch iechyd	Data personol sy'n gysylltiedig ag iechyd corfforol neu feddyliol person naturiol, gan gynnwys darpariaeth

	gwasanaethau gofal iechyd, sy'n datgelu gwybodaeth am statws iechyd 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.
Anawdurdodedig	Heb hawl cyfreithlon.

5. Cyfrifoldebau

Mae diogelu data personol yn gyfrifoldeb ar bawb. Mae'n rhaid i'r holl aelodau staff sicrhau eu bod yn ymrwymedig i gydymffurfio â rhwymedigaethau diogelu data.

Dan ddeddfwriaeth diogelu data newydd, mae'n rhaid i ysgolion bellach 'arddangos' sut y maent yn cydymffurfio â diogelu data, nid 'cydymffurfio' yn unig. Bydd yn ofynnol i ysgolion dystiolaethu cydymffurfiad er mwyn cyrraedd yr egwyddor hollgyffredinol o atebolrwydd.

5.1. Corff Llywodraethu Ysgol

Mae'r corff llywodraethu ysgol yn gyfrifol am:

- gydymffurfiad cyffredinol yr ysgol gyda *GDPR* a *Deddf Diogelu Data 2018*;
- cynnal trosolwg strategol o gydymffurfiad yr ysgol drwy ofyn am gael gweld tystiolaeth o gydymffurfiad ac ymgymryd ag ymweliadau monitro i'r ysgol;
- penodi llywodraethwr fel Pencampwr Diogelu Data ar y corff llywodraethu;
- trafod problemau a materion diogelu data yn rheolaidd yn y cyfarfodydd corff llywodraethu;
- monitro'r risgiau diogelu data a adnabyddir yn yr ysgol a monitro gweithredoedd sydd ar waith i liniaru'r risgiau hyn;
- ymgymryd â hyfforddiant diogelu data a gynhigir.

5.2. 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 cydymffurfiad â *GDPR* a *Deddf Diogelu Data 2018* o fewn gweithgareddau dyddiol yr ysgol;
- bod yn gynrychiolydd i'r ysgol fel rheolydd data;
- sicrhau a hyrwyddo dealltwriaeth a chydymffurfiad gyda'r polisi hwn a pholisïau statudol a rheoliadol eraill mewn perthynas â diogelu data;

- cadw *Rhestr Asedau Gwybodaeth* a *Chofnodion o Weithgareddau Prosesu (ROPA)* yr ysgol yn gyfredol a'u diweddaru'n rheolaidd;
- sicrhau y rheolir asedau a risgiau gwybodaeth yn yr ysgol;
- sicrhau bod yr ysgol wedi cofrestru a thalu'r ffi diogelu data blynyddol i'r ICO;
- cynnal archwiliadau mewnol sy'n monitro cydymffurfiad;
- sicrhau bod gwybodaeth perthnasol a chefnogaeth yn cael ei ddarparu ynglyn â ceisiadau gan wrthrych y data fel bod ceisiadau yn cael eu prosesu o fewn un mis calendr;
- sefydlu diwylliant adrodd a dysgu i ganiatáu'r ysgol i sefydlu ble mae problemau'n bodoli a datblygu strategaethau gyda'r Swyddog Diogelu Data Ysgolion i atal problemau rhag digwydd yn y dyfodol;
- gweithio gyda, a gweithredu fel prif gyswllt, rhwng yr ysgol a'r Swyddog Diogelu Data Ysgolion i sicrhau bod yr ysgol yn cydymffurfio â'i rhwymedigaethau diogelu data.

Gall yr ysgol benodi aelod o staff i fod yr unigolyn sy'n *gyfrifol* am ddiogelu data yn yr ysgol a fydd yn delio â thasgau a chyfrifoldebau diogelu data dyddiol, ond *na fydd* yn ymgymryd â chyfrifoldebau statudol Swyddog Diogelu Data. Bydd y cyfrifoldeb hwn yn parhau gyda'r Swyddog Diogelu Data Ysgolion.

5.3. Holl Staff yr Ysgol

Mae'r holl staff a gyflogir gan yr ysgol neu sy'n gwirfoddoli yn yr ysgol, gan gynnwys athrawon, cymorthyddion dosbarth a staff cefnogi busnes yn gyfrifol am:

- gydymffurfio'n unigol ac ar y cyd gyda'r *GDPR* a *Deddf Diogelu Data 2018* o fewn gweithgareddau dyddiol yr ysgol;
- sicrhau y cadwir ac y prosesir gwybodaeth bersonol yn unol â *GDPR* a *Deddf Diogelu Data 2018;*
- hysbysu'r Pennaeth ac/neu'r person sy'n gyfrifol am ddiogelu data yn yr ysgol yn syth o unrhyw ddigwyddiadau, pryderon, ceisiadau neu dor-rheolau mewn perthynas â diogelu data;
- hysbysu'r Pennaeth o unrhyw newidiadau i fanylion personol er mwyn cynorthwyo'r ysgol i gadw gwybodaeth bersonol am staff yn gyfredol;
- sicrhau dealltwriaeth a chydymffurfiad â'r polisi hwn;
- sicrhau dealltwriaeth a chydymffurfiad â'r holl bolisïau sy'n gysylltiedig â diogelu a diogelwch data;
- mabwysiadu safonau arfer dda mewn perthynas â diogelu data;
- ymgymryd ag unrhyw hyfforddiant diogelu data a gynhigir.

5.4. Swyddog Diogelu Data Ysgolion

Mae'r Swyddog Diogelu Data Ysgolion yn gyfrifol am:

- hysbysu a chynghori ysgolion ar eu rhwymedigaethau diogelu data;
- monitro cydymffurfiad a pherfformiad yn erbyn rhwymedigaethau, gan gynnwys cynnal archwiliadau ac adolygiadau diogelu data;

- darparu cyngor, arweiniad ac argymhellion ar effaith ymdrechion a materion diogelu data'r ysgol;
- darparu adroddiad sicrwydd llywodraethu gwybodaeth i gorff llywodraethu'r ysgol yn flynyddol, a darparu adroddiad crynodeb blynyddol lefel uchel ar yr holl ysgolion i Uwch Dîm Rheoli'r Gwasanaeth Dysgu ac i Bwyllgor Archwilio a Llywodraethu Cyngor Sir Ynys Môn;
- creu ac adolygu gweithdrefnau, polisïau, arweiniad a thempledi diogelu data yn rheolaidd;
- hwyluso a chefnogi'r ysgol i ymateb i geisiadau gan wrthrych y data o fewn y cyfnod o amser;
- cefnogi a darparu cyngor yn achos digwyddiad diogelwch data;
- gwirio a chymeradwyo trydydd partïon sy'n ymdrin â data'r ysgol, unrhyw gontractau neu gytundebau ynglŷn â phrosesu data;
- trefnu a darparu hyfforddiant diogelu data i staff mewn ysgolion gan gynnwys llywodraethwyr ysgol;
- bod yn bwynt cyswllt cyntaf i unigolion y mae'r ysgol yn prosesu eu data, ac ar gyfer yr ICO.

6. Egwyddorion Diogelu Data

Mi fydd dull ymdrin â diogelu data yr ysgol yn 'diogelu data drwy dylunio a rhagosod' a 'preifatrwydd drwy ddylunio', fel mae'r *GDPR* yn ymofyn. Mae hyn yn golygu bod angen integreiddio diogelu data i fewn i weithgareddau prosesu ac ymarferion busnes yr ysgol, o'r cam dylunio ac ar hyd cylch bywyd y broses.

Bydd yr ysgol yn cydymffurfio â'r **chwe egwyddor diogelu data sylfaenol** canlynol wrth brosesu gwybodaeth bersonol:

1. Bydd gwybodaeth bersonol yn cael ei phrosesu mewn modd cyfreithiol, teg a thryloyw;
2. Bydd gwybodaeth bersonol yn cael ei chasglu at ddibenion penodedig, eglur a chyfreithlon yn unig, ac ni chaiff ei phrosesu mewn ffordd sy'n anghydnaws â'r dibenion cyfreithiol hynny;
3. Byddwn ond yn prosesu gwybodaeth bersonol os yw'n ddigonol, yn berthnasol ac yn gyfyngedig i'r hyn sy'n angenrheidiol at y dibenion perthnasol (lleihau data);
4. Mae'n rhaid cadw gwybodaeth bersonol yn gywir ac yn gyfredol, a bydd camau rhesymol yn cael eu cymryd i sicrhau bod gwybodaeth bersonol anghywir yn cael ei dileu neu ei chywiro heb oediad;
5. Bydd gwybodaeth bersonol yn cael ei chadw ar ffurf sy'n caniatáu adnabod gwrthrychau data am ddim hirach na'r hyn sy'n angenrheidiol at y dibenion y caiff yr wybodaeth ei phrosesu ar eu cyfer;
6. Bydd gwybodaeth bersonol yn cael ei phrosesu'n ddiogel. Bydd mesurau diogelwch technegol yn cael eu cymryd i sicrhau y cadwir data personol yn ddiogel a'i fod yn cael ei amddiffyn rhag cael ei brosesu'n anawdurdodedig neu'n anghyfreithlon, ac yn erbyn colled, dinistr neu niwed damweiniol.

Bydd yr ysgol yn adolygu pwrpasau'r gweithgaredd prosesu penodol ac yn dewis y sail (neu seiliau) gyfreithiol fwyaf priodol ar gyfer y prosesu hwnnw cyn i'r prosesu ddechrau am y tro cyntaf ac yna'n rheolaidd wrth iddo barhau. Gwelir rhan 10 ar gyfer diffiniadau o weithgareddau prosesu penodol.

Mae'n rhaid i'r ysgol allu **arddangos** cydymffurfiad â'r egwyddorion hyn. Os na all yr ysgol gydymffurfio â'r chwe egwyddor i gyd, **ni ddylid** prosesu data.

7. Hawliau'r Gwrthrych Data

Mae deddfwriaeth diogelu data yn rhoi'r hawliau canlynol i unigolion:

1. Yr hawl i gael gwybod
2. Yr hawl i fynediad
3. Yr hawl i gywiro
4. Yr hawl i ddileu
5. Yr hawl i gyfyngu ar brosesu
6. Yr hawl i gludadwyedd data
7. Yr hawl i wrthwynebu
8. Hawliau'n ymwneud â phroffilio a gwneud penderfyniadau awtomataidd.

Bydd y Swyddog Diogelu Data Ysgolion yn cefnogi'r ysgol i ymdrin ag unrhyw geisiadau gan unigolion i ymarfer eu hawliau.

7.1. Yr hawl i gael gwybod

Mae gan unigolion yr hawl i wybod bod gwybodaeth amdanynt yn cael ei phrosesu. Bydd yr ysgol yn hysbysu unigolion drwy Hysbysiad Preifatrwydd, ar y pwynt o gaslgu'r gwybodaeth, o sut, pam ac ar ba sail y prosesir yr wybodaeth honno.

7.2. Yr hawl i fynediad

Mae gan unigolion yr hawl i dderbyn cadarnhad bod eu gwybodaeth yn cael ei phrosesu a hefyd i wneud cais am fynediad at a chael copïau o wybodaeth bersonol y mae'r ysgol yn ei chadw amdanynt neu wybodaeth am blentyn y maent yn gyfrifol amdano (ceisiadau gan wrthrych y data - SAR).

Gellir gwneud cais gan wrthrych y data ar lafar neu'n ysgrifenedig ond mae'n rhaid iddo fod yn gwbl glir pa wybodaeth bersonol y gwneir cais amdani.

Cyn ymateb i gais gan wrthrych y data, bydd camau rhesymol yn cael eu cymryd i wirio hunaniaeth yr unigolyn sy'n gwneud y cais ac a oes ganddynt yr awdurdod i ofyn am wybodaeth ar ran unigolyn arall. Mae'n bosib gofyn am wybodaeth ychwanegol i gadarnhau hunaniaeth ac mae'n bosib gofyn am gael gweld dogfennau hunaniaeth megis trwydded yrru neu basbort a fydd yn gwirio hunaniaeth yr unigolyn.

Unwaith y derbynnir cais gan wrthrych y data, mae'n rhaid darparu'r wybodaeth a ofynnir amdani heb oediad ac ar yr hwyraf o fewn **un mis calendr** o dderbyn y cais. Os yw cais gan wrthrych y data yn gymhleth (h.y. os yw cais yn amlwg yn ddi-sail neu'n ormodol, neu os oes angen cael data o fwy nag un ffynhonnell neu os yw'r

gwrthrych data wedi gwneud ceisiadau niferus (yn gyfredol ai pheidio)), gellir rhoi estyniad o hyd at ddau fis pellach i'r cyfnod ymateb. Bydd yr ymgeisydd yn cael ei hysbysu os bydd yr amserlen yn cael estyniad a'r rhesymau dros hynny. Disgwylir i'r ysgol ymateb o fewn y cyfnod hyd yn oed os yw gwyliau ysgol yn digwydd yn ystod y cyfnod ymateb. Bydd yr ysgol yn hysbysu disgyblion a rhieni/y sawl â'r cyfrifoldeb rhieniol bod mynediad cyfyngedig i geisiadau yn ystod y tymor ysgol, ond y bydd yn dal i ddelio â cheisiadau o fewn y cyfnod ymateb.

Mae cyfnodau amser cyfyngedig i ymateb i gais, a gall unrhyw oediad arwain at beidio â gallu cwrdd â'r amseroedd hynny, a gall hyn arwain at gamau gorfodaeth gan yr ICO ac/neu gamau cyfreithiol gan yr unigolyn yr effeithir.

Dan rhai amgylchiadau, gall yr ysgol fod wedi ei heithrio rhag darparu peth neu'r holl ddata personol a ofynnwyd amdano. Dylid ond rhoi eithriadau ar sail achos fesul achos ar ôl ystyried yr holl ffeithiau'n ofalus. Bydd y Swyddog Diogelu Data Ysgolion yn darparu cyngor ac arweiniad ar ba wybodaeth y gellir ac na ellir ei rhannu.

Bydd yr ysgol yn casglu a choladu'r holl ddata personol a ofynnwyd amdano. Bydd angen i'r ysgol gasglu'r holl gofnodion electronig a phapur sy'n cynnwys data personol mewn ffeiliau, e-byst, CCTV, llythyrau, adroddiadau a delweddau.

Ni all yr ysgol godi ffi am ddelio a cheisiadau gan wrthrych y data. Fodd bynnag, os yw cais yn ddi-sail, yn ormodol ac wedi cael ei gyflwyno'n flaenorol, mae gan yr ysgol yr hawl i godi ffi weinyddol 'rhesymol'. Mi fydd y Swyddog Diogelu Data Ysgolion yn gallu rhoi arweiniad o ran be sydd yn cael ei ystyried yn 'ffi resymol'.

Bydd y Swyddog Diogelu Data Ysgolion yn darparu ffigyrau ynglŷn â'r nifer o geisiadau gan wrthrych y data a dderbyniwyd yn yr adroddiad sicrwydd llywodraethiant gwybodaeth blynyddol i gorff llywodraethu'r ysgol. Bydd ffigyrau hefyd yn cael eu cynnwys yn adroddiad crynodeb lefel uchel blynyddol y Swyddog Diogelu Data Ysgolion ar yr holl ysgolion, a gyflwynir i Uwch Dîm Rheoli'r Gwasanaeth Dysgu a Phwyllgor Archwilio a Llywodraethu Cyngor Sir Ynys Môn.

Bydd yr ysgol yn dilyn y *Polisi Delio gyda Chais gan Wrthrych Data Ysgolion* ar sut i ddelio gyda cheisiadau gan wrthrych y data, sydd ar gael ar Addysg Môn.

7.3. Yr hawl i gywiro

Mae gan unigolion yr hawl i gywiro eu data personol os yw'n anghywir neu'n anghyflawn. Bydd yr ysgol yn cywiro'r data personol cyn gynted â phosib ac yn gwneud hynny o fewn un mis calendr o dderbyn y cais i gywiro. Gellir rhoi estyniad o ddau fis i hyn lle mae cais i gywiro yn gymhleth. Dylid gwneud nodyn ar gofnodion perthnasol os oes unrhyw amheuaeth ynglŷn â chywirdeb wrth ddelio â'r cais.

Efallai na fydd yn bosib i'r ysgol newid neu ddileu'r wybodaeth bersonol ar bob achlysur, ond dylid cywiro unrhyw beth sy'n ffeithiol anghywir.

Lle na fydd yr ysgol yn gweithredu mewn ymateb i'r cais i gywiro, bydd yr ysgol yn egluro'r rhesymau pam i'r unigolyn ac yn eu hysbysu o'u hawl i gwyno i'r ICO. Mi fydd yr ysgol yn gwneud cofnod o hyn.

7.4. Yr hawl i ddileu

Mae gan unigolion yr hawl i ofyn am gael dileu neu gael gwared â gwybodaeth bersonol a gadwir amdanynt os nad yw'r data bellach yn angenrheidiol at y diben y cafodd ei chasglu/ei phrosesu yn wreiddiol, neu os nad oes seiliau cyfreithiol pwysig dros ei phrosesu. Enw arall am yr hawl hon yw'r hawl i anghof.

Gellir ond gwrthod cais i ddileu os yw eithriad yn berthnasol, ond mae'n debygol y bydd eithriad yn berthnasol yng nghyd-destun dileu cofnodion ysgol. Bydd yr ysgol yn ystyried pob cais ar sail unigol. Bydd yr ysgol yn ymateb i'r cais i ddileu o fewn un mis calendr.

Gall yr ysgol wrthod cais i ddileu data personol:

- lle mae'n rhaid i'r ysgol gydymffurfio â rhwymedigaeth gyfreithiol (dros gadw'r data);
- i amddiffyn buddiannau hanfodol unigolion neu ar gyfer tasgau a gynhelir er buddiannau'r cyhoedd;
- wrth archifo mewn perthynas â buddiannau'r cyhoedd, ymchwil gwyddonol/hanesyddol neu at ddibenion ystadegol;
- pan fydd y data personol yn ofynnol ar gyfer ymarfer hawliadau cyfreithiol;
- pan fydd y prosesu'n angenrheidiol i ymarfer yr hawl i ryddid mynegiant a gwybodaeth.

Bydd yr ysgol yn hysbysu trydydd partïon sydd hefyd yn prosesu'r data personol oni bai ei fod yn ymwneud ag ymdrech anghymesur i wneud hynny.

7.5. Yr hawl i gyfyngu ar brosesu

Mae gan unigolion yr hawl i blocio y prosesu o'u gwybodaeth bersonol mewn rhai amgylchiadau. Gall y data barhau i gael ei storio ond mae'n rhaid i'r prosesu ddarfod.

Mae gan unigolion yr hawl i gyfyngu ar brosesu eu data personol lle:

- mae cywirdeb yr wybodaeth yn cael ei herio;
- mae'r prosesu yn anghyfreithlon (ond nid ydynt eisiau i'r data gael ei ddileu, ond yn hytrach ei gyfyngu); neu
- nid yw'r ysgol bellach angen yr wybodaeth bersonol ond mae angen y data i sefydlu, ymarfer neu amddiffyn hawliad cyfreithiol.

Mae gan unigolion hefyd yr hawl i gyfyngu ar brosesu gwybodaeth bersonol dros dro lle:

- maent yn credu ei bod yn gywir (ac mae'r ysgol yn gwirio a yw'n gywir);
- maent wedi gwrthod prosesu (ac mae'r ysgol yn ystyried a yw'r seiliau cyfreithlon yn bwysicach na'u buddiannau).

Bydd angen i'r ysgol hysbysu unrhyw drydydd parti sydd wedi derbyn y data o'r angen i gyfyngu ar brosesu, a hysbysu'r unigolyn o hunaniaeth y trydydd partïon hyn. Bydd yr ysgol yn hysbysu unigolion pan fydd yn penderfynu codi cyfyngiad ar brosesu.

7.6. Yr hawl i gludadwyedd data

Mae gan unigolion yr hawl i ofyn am gopi o'u data personol mewn ffurf strwythuredig. Dylid prosesu ceisiadau o fewn un mis calendr, gan gymryd yn ganiataol nad oes baich gormodol ac nad yw'n cyfaddawdu preifatrwydd unigolion eraill. Gall unigolion hefyd ofyn i'w data personol gael ei drosglwyddo'n uniongyrchol i system arall. Ni ellir codi ffi am hyn. Dim ond y canlynol y mae'r hawl i gludadwyedd data yn berthnasol:

- data personol y mae unigolyn wedi ei ddarparu i'r ysgol fel y rheolydd data;
- lle mae'r prosesu yn seiliedig ar gysyniad yr unigolyn neu ar gyfer perfformiad contract; ac
- pan brosesir gwybodaeth yn awtomataidd.

7.7. Yr hawl i wrthwynebu

Mae gan unigolion yr hawl i wrthwynebu prosesu eu gwybodaeth bersonol os yw'r ysgol yn:

- prosesu yn seiliedig ar fuddiannau cyfreithiol neu berfformiad tasg er buddiant y cyhoedd/ymarfer awdurdod swyddogol (gan gynnwys proffilio);
- marchnata uniongyrchol (gan gynnwys proffilio); a
- prosesu at ddibenion ymchwil ac ystadegau gwyddonol/hanesyddol.

Bydd yr ysgol yn cydymffurfio â'r cais oni bai bod rhesymau cadarn, cyfreithiol dros brosesu neu os oes angen sefydlu, ymarfer neu amddiffyn hawliadau cyfreithiol.

7.8. Hawliau'n ymwneud â phroffilio a gwneud penderfyniadau awtomataidd

Mae deddfwriaeth diogelu data yn caniatáu:

- Gwneud penderfyniadau unigol awtomataidd- gwneud penderfyniad drwy ddulliau awtomataidd yn unig heb unrhyw gysylltiad gan fod dynol; a
- Proffilio- prosesu data personol yn awtomataidd i werthuso pethau penodol am unigolyn. Gall proffilio fod yn rhan o broses gwneud penderfyniadau.

Mae gan yr ysgol yr hawl i wneud penderfyniadau a phroffilio yn awtomataidd, ond ddim ond os:

- yw'r prosesu'n angenrheidiol ar gyfer mynd i mewn i gontract neu berfformio contract;
- yw'r prosesu wedi cael ei awdurdodi gan gyfraith aelod wladwriaeth sy'n cynnwys mesurau i ddiogelu hawliau gwrthrychau data; neu os
- yw'r prosesu'n seiliedig ar ganiatâd eglur.

Mae rheolau ychwanegol i amddiffyn unigolion os yw gwneud penderfyniadau a phroffilio awtomataidd yn cael effeithiau cyfreithiol neu'n effeithio arnynt yn yr un modd. Rhaid i'r ysgol sicrhau bod unigolion yn gallu:

- derbyn ymyrraeth ddynol;
- mynegi eu barn; a
- chael eglurhad o'r penderfyniad a'i herio.

Ni fydd yr ysgol yn gwneud penderfyniadau awtomataidd, gan gynnwys proffilio, yn seiliedig ar unrhyw wybodaeth bersonol sensitif unigolyn.

7.9. Hawliau eraill

Yn ogystal â'r hawliau uchod, mae gan unigolion hefyd yr hawl i:

- dynnu eu caniatâd dros brosesu yn ôl ar unrhyw amser;
- wneud cwyn i'r ICO.

8. Hawliau Plant

Mae gan blant yr un hawliau ag oedolion dros eu gwybodaeth bersonol, a gallent arfer yr hawliau hyn cyn belled â'u bod yn gymwys i wneud hynny. Lle na ystyrir plentyn yn gymwys i wneud hyn, bydd oedolyn â chyfrifoldeb rhieniol gan amlaf yn arfer hawliau diogelu data'r plentyn.

Yng Nghymru, nid oes oed penodol y caiff plentyn ei ystyried yn gyffredinol gymwys i ddarparu ei ganiatâd ei hun dros brosesu. Asesir cymhwysedd yn dibynnu ar y lefel o ddealltwriaeth sydd gan y plentyn. Os yw plentyn yn gymwys yna, yn union fel oedolyn, gall awdurdodi rhywun arall i weithredu ar ei ran. Gall hyn fod yn rhiant/y sawl â chyfrifoldeb rhieniol, oedolyn arall, neu gynrychiolydd megis gwasanaeth eiriolaeth plant, elusen neu gyfreithiwr.

Yn y DU, dim ond plant 13 oed a throsodd sy'n gallu darparu eu caniatâd ar gyfer *information society services (ISS*). Mae ISS yn gyffredinol yn cynnwys gwefannau, apiau, porwyr, marchnadfa ar-lein a gwasanaethau cynnwys ar-lein megis gwasanaethau a lawrlwytho cerddoriaeth, gemau a fideo ar alw.

9. Hawliau Rhieni

Gall unigolyn â chyfrifoldeb rhiant arfer hawliau ar ran plentyn os:

- yw'r plentyn yn eu hawdurdodi i wneud hynny;
- nid oes gan y plentyn ddigon o ddealltwriaeth i arfer yr hawliau ei hun; neu
- pan mae'n amlwg bod hyn ym muddiant gorau'r plentyn.

Person sydd â chyfrifoldeb rhiant yw rhywun sydd, yn ôl y gyfraith yng ngwlad breswyl y plentyn, â'r hawliau a'r cyfrifoldebau cyfreithiol dros blentyn a roddir fel arfer i rieni. Ni fydd hyn bob amser yn 'rhieni naturiol' plentyn a gall mwy nag un person naturiol neu gyfreithiol fod â chyfrifoldeb rhiant.

Rhaid i'r ysgol gadarnhau bod gan y person sy'n rhoi caniatâd, mewn gwirionedd, gyfrifoldeb rhiant dros y plentyn. Mae gan yr ysgol hawl i ofyn am ddogfennau perthnasol i ddangos tystiolaeth o hyn yn ogystal â manylion y person sy'n gwneud unrhyw geisiadau ar ran y plentyn.

Yn ogystal, mae gan rieni eu hawl annibynnol eu hunain o dan *Reoliadau Addysg (Gwybodaeth am Ddisgyblion) (Cymru) 2004* i gael mynediad at gofnodion addysg swyddogol eu plant sy'n mynychu ysgol a gynhelir. Gall rhieni wneud ceisiadau ysgrifenedig i'r Pennaeth. Gall disgyblion hefyd wneud cais am eu cofnod addysg eu hunain. Rhaid i gais am gofnod addysgol gael ymateb gan yr ysgol o fewn 15 diwrnod ysgol. Gall yr ysgol atal gwybodaeth mewn rhai amgylchiadau, megis lle y gellir achosi niwed difrifol i iechyd corfforol neu feddyliol y disgybl neu unigolyn arall, neu os wneir cais am sgript arholiad neu am farciau arholiad cyn iddynt gael eu cyhoeddi'n swyddogol. Gall yr ysgol godi ffi am wybodaeth a ddarperir o gofnod addysg yn dibynnu ar nifer y tudalennau a ddarperir.

10. Amodau dros Brosesu (Sail Gyfreithiol)

10.1. Erthygl 6

Mae'n rhaid prosesu data personol yn deg ac yn gyfreithlon yn unol â hawliau'r unigolyn. Bydd yr ysgol ond yn prosesu gwybodaeth bersonol lle mae o leiaf un o amodau *Erthygl 6 y GDPR* wedi cael ei fodloni:

- 6(1)(a)- **cysyniad yr unigolyn-** mae'r unigolyn wedi rhoi cysyniad clir i'r ysgol dros brosesu ei ddata personol at ddiben penodol;
- 6(1)(b)- **mae prosesu yn angenrheidiol ar gyfer contract-** mae'r prosesu yn angenrheidiol ar gyfer contract gyda'r unigolyn, neu oherwydd eu bod wedi gofyn i gymryd camau penodol cyn mynd i mewn i gontract;
- 6(1)(c)- **mae prosesu yn angenrheidiol ar gyfer contract-** mae'r prosesu'n angenrheidiol er mwyn i'r ysgol gydymffurfio â'r gyfraith (ddim yn cynnwys rhwymedigaethau cytundebol);
- 6(1)(d)- **mae prosesu yn angenrheidiol er buddiannau hanfodol yr unigolyn neu berson naturiol arall-** mae'r prosesu yn angenrheidiol i amddiffyn bywyd rhywun;
- 6(1)(e)- **mae prosesu'n angenrheidiol ac yn ymgymryd â thasg ym muddiannau'r cyhoedd neu'n ymarfer awdurdod swyddogol-** mae prosesu yn angenrheidiol i'r ysgol berfformio tasg er budd y cyhoedd neu ar gyfer swyddogaethau swyddogol yr ysgol, ac mae gan y dasg neu'r swyddogaeth sail glir mewn cyfraith;
- 6(1)(f)- **mae prosesu yn angenrheidiol at ddibenion buddiannau cyfreithiol y rheolydd data neu drydydd parti-** mae'r prosesu'n angenrheidiol er buddiannau cyfreithiol neu fuddiannau cyfreithiol trydydd parti oni bai bod rheswm da i amddiffyn data personol unigolyn sy'n bwysicach na'r buddiannau hynny (*nid yw hyn yn berthnasol ar gyfer awdurdodau cyhoeddus yn prosesu data i berfformio tasgau swyddogol).*

Bydd yr ysgol yn dogfennu ei phenderfyniad am ba sail gyfreithiol sy'n berthnasol, i helpu arddangos cydymffurfiad â'r egwyddorion diogelu data. Bydd yr ysgol yn

cynnwys gwybodaeth am ddibenion y prosesu a'r sail gyfreithiol drosto yn Hysbysiad Preifatrwydd yr ysgol.

10.2. Erthygl 9

Mae'n ofynnol dan y sail gyfreithiol dros brosesu **data categori arbennig** bod rhaid bodloni amod yn *Erthygl 9* o *GDPR* yn ogystal ag o leiaf un amod o *Erthygl 6 (gwelir rhan 11 am ddifiniad o ddata categori arbennig)* . Bydd yr ysgol ond yn prosesu gwybodaeth bersonol sensitif os oes amod yn *Erthygl 9* wedi ei fodloni:

- 9(2)(a)- **prosesu gyda chydsyniad eglur a phenodol yr unigolyn -** oni bai bod cyfraith yr UE neu Aelod-wladwriaeth yn gwahardd dibynnu ar gydsyniad;
- 9(2)(b)- **mae prosesu'n angenrheidiol o dan gyfraith cyflogaeth -** neu gyfraith nawdd cymdeithasol neu warchodaeth gymdeithasol, neu gytundeb ar y cyd;
- 9(2)(c)- **mae prosesu'n angenrheidiol er mwyn diogelu buddiannau hanfodol yr unigolyn -** gwrthrych data sy'n analluog yn gorfforol neu'n gyfreithiol i roi caniatâd;
- 9(2)(d)- **prosesu ar gyfer defnyddio grŵp categori arbennig (sefydliad dielw gyda nod gwleidyddol neu grefyddol neu undeb llafur);**
- 9(2)(e)- **mae prosesu'n ymwneud â gwybodaeth a gyhoeddir gan yr unigolyn;**
- 9(2)(f)- **mae prosesu'n angenrheidiol fel y gall y sefydliad amddiffyn hawliadau cyfreithiol -** neu lle mae'r llysoedd yn gweithredu yn rhinwedd eu swydd farnwrol;
- 9(2)(g)- **mae prosesu'n angenrheidiol am resymau buddiannau cyhoeddus sylweddol yn seiliedig ar y gyfraith -** sy'n gymesur â'r nod a ddilynir ac sy'n cynnwys mesurau diogelu priodol - mae hyn yn golygu y gall Aelod-wladwriaethau ymestyn yr amgylchiadau lle gellir prosesu data sensitif er budd y cyhoedd;
- 9(2)(h)- **mae angen prosesu er mwyn ymateb i anghenion lechyd Galwedigaethol a Gofal Cymdeithasol -** sy'n angenrheidiol at ddibenion meddygaeth ataliol neu alwedigaethol, ar gyfer asesu capasiti gwaith cyflogai, diagnosis meddygol, darparu iechyd neu ofal cymdeithasol neu drin neu reoli systemau a gwasanaethau iechyd neu ofal cymdeithasol ar sail cyfraith Aelod-wladwriaeth yr Undeb neu gontract gyda gweithiwr iechyd proffesiynol;
- 9(2)(i)- **mae prosesu'n angenrheidiol am resymau lechyd y Cyhoedd -** megis diogelu rhag bygythiadau trawsffiniol difrifol i iechyd neu sicrhau safonau uchel o ofal iechyd a chynhyrchion meddyginiaethol neu ddyfeisiau meddygol;
- 9(2)(j)- **mae prosesu'n angenrheidiol at ddibenion archifo er budd y cyhoedd; neu at ddibenion ymchwil gwyddonol neu hanesyddol; neu at ddibenion ystadegol.**

Cynhwysir amodau categori arbennig pellach yn *Atodlen 1* o'r *Ddeddf Diogelu Data 2018.*

Ni fydd yr ysgol yn prosesu gwybodaeth bersonol sensitif nes bod yr unigolyn wedi cael ei hysbysu'n briodol (drwy Hysbysiad Preifatrwydd neu fel arall) o natur y prosesu, at ba ddibenion, a'r sail gyfreithiol ar ei gyfer.

Pan fydd gwybodaeth am droseddau'n cael ei phrosesu, bydd yr ysgol yn nodi amod cyfreithlon ar gyfer prosesu'r wybodaeth honno a bydd yn dogfennu hyn.

Bydd yr ysgol yn hysbysu'r Swyddog Diogelu Data Ysgolion cyn prosesu unrhyw wybodaeth bersonol sensitif, fel y gall y Swyddog Diogelu Data Ysgolion asesu a yw'r prosesu yn cydymffurfio â'r criteria a nodir uchod.

11. Categorïau Arbennig o Ddata Personol

Cyfeirir weithiau at gategorïau arbennig o ddata personol fel gwybodaeth bersonol sensitif neu ddata personol sensitif. Ystyrir bod y rhain yn fwy sensitif a dim ond dan amgylchiadau mwy cyfyngedig y gellir eu prosesu.

Mae *GDPR* yn diffinio data categori arbennig fel:

- data personol sy'n datgelu hil neu darddiad ethnig;
- data personol sy'n datgelu barn wleidyddol;
- data personol sy'n datgelu credoau crefyddol neu athronyddol;
- data personol sy'n datgelu aelodaeth undeb llafur;
- data genetig;
- data biometrig (lle caiff ei ddefnyddio at ddibenion adnabod);
- data am iechyd;
- data ynglŷn â bywyd rhyw unigolyn;
- data ynglŷn â gogwydd rhywiol unigolyn.

Ymhellach i adran 10.2, mae'n rhaid i'r ysgol bennu'r amod dros brosesu data categori arbennig cyn dechrau prosesu'r wybodaeth a bydd yn dogfennu'r amod.

Ni fydd yr ysgol yn rhannu unrhyw wybodaeth feddygol am ddisgybl oni bai bod sail gyfreithiol dros wneud hynny. Gall yr ysgol roi arferion ar waith i rannu gwybodaeth feddygol gyda chaniatâd y disgybl/rhiant/y sawl sydd â chyfrifoldeb rhiant os teimlir bod angen rhannu'r wybodaeth yn benodol er mwyn diogelu iechyd a lles y disgybl penodol (e.e. hysbysiad ar hysbysfwrdd mewn ystafell staff gyda mynediad cyfyngedig sy'n cynnwys gwybodaeth bersonol a sensitif am ddisgybl ag alergedd bwyd difrifol). Dan amgylchiadau o'r fath, bydd yr ysgol yn ceisio cyngor gan y Swyddog Diogelu Data Ysgolion a bydd yn rhaid cydbwyso'r risgiau iechyd a lles a achosir, a'r angen i gadw gwybodaeth bersonol sensitif yn ddiogel, yn erbyn ei gilydd.

12. Caniatâd

Gall yr ysgol ddefnyddio caniatâd fel sail gyfreithiol ar gyfer prosesu os mai dyma'r sail gyfreithiol fwyaf priodol i'w defnyddio neu os nad yw sail gyfreithlon arall yn briodol.

Rhaid i ganiatâd fod yn gam cadarnhaol, felly mae'n rhaid i unigolion optio i mewn bob amser a chymryd camau cadarnhaol wrth roi eu caniatâd. Bydd angen caniatâd ar yr ysgol ar gyfer pob gweithgaredd prosesu ar wahân.

Bydd yr ysgol yn cadw cofnod o ganiatâd drwy gofrestr sy'n rhestru pawb sydd wedi rhoi caniatâd neu sydd heb roi caniatâd ac y mae gweithgarwch prosesu penodol ar ei gyfer. Bydd yr ysgol yn sicrhau bod hyn yn cael ei gadw'n gywir ac yn gyfoes a bod proses wedi'i sefydlu ar gyfer sicrhau bod yr ysgol yn cydymffurfio â'r penderfyniadau caniatâd a gofnodir.

Rhaid rhoi caniatâd yn rhydd, a rhaid iddo fod mor hawdd i'w dynnu'n ôl ag y mae i'w roi. Mae gan unigolion yr hawl i dynnu caniatâd yn ôl ar unrhyw adeg a bydd yr ysgol yn diweddaru'r cofnod o ganiatâd i adlewyrchu unrhyw newidiadau.

Os nad yw'r ysgol wedi derbyn ffurflen ganiatâd neu os na ddarparwyd unrhyw gamau cadarnhaol eraill i roi caniatâd, bydd yr ysgol yn cymryd yn ganiataol na ddarperir caniatâd a bydd yn dogfennu ac yn gweithredu hyn.

Mae ffurflenni caniatâd ar gael ar Addysg Môn.

13. Cywirdeb a Pherthnasedd

Bydd yr ysgol yn sicrhau bod unrhyw wybodaeth bersonol a brosesir yn gywir, yn gyfredol, yn berthnasol, yn ddigonol ac nad yw'n ormodol (yn gymesur), a'i bod yn cael ei phrosesu at y diben y cafodd ei derbyn. Ni fydd data personol a geir at un diben yn cael ei brosesu at unrhyw ddiben sydd ddim yn gysylltiedig oni bai bod yr unigolyn dan sylw wedi cytuno i hyn neu y byddai fel arall yn rhesymol i ddisgwyl hyn.

Bydd yr ysgol yn ei gwneud yn glir bod yn rhaid i unigolion gymryd camau rhesymol i sicrhau bod data personol sydd gan yr ysgol amdanynt yn gywir a'i fod wedi'i ddiweddaru yn ôl y gofyn. Mae hyn wedi'i gynnwys yn Hysbysiad Preifatrwydd yr ysgol a bydd yr ysgol yn cadarnhau'n rheolaidd bod yr wybodaeth a gadwir yn gywir, yn enwedig cyfeiriadau a manylion cyswllt. Bydd yr ysgol yn diweddaru'r wybodaeth cyn gynted â phosibl mewn cofnodion papur ac electronig.

14. Cadw Gwybodaeth Bersonol

Bydd gwybodaeth bersonol (a gwybodaeth categori arbennig) yn cael ei chadw'n ddiogel yn unol â'r *Cyfnodau Cadw Cofnodion Ysgolion* sydd ar gael ar Addysg Môn.

Ni ddylid cadw gwybodaeth bersonol (a gwybodaeth categori arbennig) am fwy o amser na'r angen. Bydd yr amser y dylid cadw data yn dibynnu ar yr amgylchiadau, gan gynnwys y rhesymau pam y cafwyd yr wybodaeth bersonol. Dylai'r ysgol ddilyn y *Cyfnodau Cadw Cofnodion Ysgolion* sy'n nodi'r cyfnod cadw perthnasol ar gyfer

gwahanol fathau o wybodaeth a dogfennau personol. Os oes unrhyw ansicrwydd, dylai'r ysgol ymgynghori â'r Swyddog Diogelu Data Ysgolion am arweiniad.

Mae angen i'r ysgol sicrhau nad yw gwybodaeth bersonol yn cael ei chadw am fwy o amser na'r angen ond hefyd nad yw gwybodaeth bersonol yn cael ei gwaredu cyn diwedd y cyfnod cadw.

15. Cofnodi Data

Bydd yr ysgol yn cadw cofnodion yn y fath fodd fel y gall yr unigolyn dan sylw eu harolygu. Gall y llysoedd neu unrhyw swyddog cyfreithiol hefyd archwilio'r wybodaeth rywbryd yn y dyfodol. Felly, dylai fod yn gywir, yn ddiduedd, yn ddiamwys ac yn amlwg ddeongladwy/darllenadwy. Pan geir gwybodaeth o ffynhonnell allanol, dylid cofnodi manylion y ffynhonnell a'r dyddiad a gafwyd.

16. Cofnodion o Weithgareddau Prosesu (ROPA)

Bydd yr ysgol yn cadw cofnodion ysgrifenedig o weithgareddau prosesu, gan gynnwys:

- enw a manylion yr ysgol; manylion cyswllt y Swyddog Diogelu Data Ysgolion ac unrhyw reolwyr data eraill ar y cyd os yw'n berthnasol;
- dibenion y prosesu;
- disgrifiad o'r categorïau o unigolion a chategorïau o ddata personol a brosesir;
- categorïau o dderbynwyr data personol;
- lle y bo'n bosibl, y cyfnodau cadw ar gyfer y gwahanol gategorïau o ddata personol;
- lle y bo'n bosibl, disgrifiad cyffredinol o fesurau diogelwch technegol a sefydliadol.

Bydd yr ysgol hefyd, fel rhan o'r cofnod o weithgareddau prosesu, yn dogfennu neu'n darparu dolen gyswllt i ddogfennaeth ar:

- wybodaeth sy'n ofynnol ar gyfer Hysbysiadau Preifatrwydd;
- cofnodion o ganiatâd;
- contractau prosesydd-rheolwyr;
- lleoliad data personol;
- Asesiadau Effaith Diogelu Data (DPIAau);
- digwyddiadau tor-rheolau data personol;
- data categori arbennig neu gollfarn droseddol a data trosedd.

Os yw'r ysgol yn prosesu data categori arbennig neu ddata ar gollfarnau troseddol a throseddau, bydd cofnodion ysgrifenedig yn cael eu cadw o:

- at ba ddiben(ion) perthnasol y mae'r prosesu'n digwydd, gan gynnwys (lle bo angen) pam ei fod yn angenrheidiol at y diben hwnnw;

- y sail gyfreithlon dros brosesu; ac
- a yw'r ysgol yn cadw ac yn dileu'r wybodaeth bersonol yn unol â'r ddogfen bolisi ac, os nad yw, y rhesymau dros beidio â dilyn y polisi.

Bydd yr ysgol yn cynnal adolygiadau rheolaidd o'r wybodaeth bersonol sy'n cael ei phrosesu a'r dogfennau diweddaraf yn unol â hynny. Gall hyn gynnwys:

- cynnal archwiliadau gwybodaeth i ganfod pa wybodaeth bersonol sydd gan yr ysgol;
- creu mapiau llif data ar gyfer gwahanol brosesau gwybodaeth;
- dosbarthu holiaduron a siarad â holl staff yr ysgol i gael darlun cyflawn o weithgareddau prosesu'r ysgol; ac
- adolygu polisïau, gweithdrefnau, contractau a chytundebau i fynd i'r afael â meysydd fel cadw, diogelwch a rhannu data.

Bydd yr ysgol yn dogfennu gweithgareddau prosesu ar ffurf electronig fel y gellir ychwanegu, dileu a diwygio gwybodaeth yn hawdd fel bod y cofnod o weithgareddau prosesu yn cael ei gadw'n gywir ac yn gyfoes.

Mae templed ar gyfer *Cofnodion o Weithgareddau Prosesu* a chanllawiau cysylltiedig ar gael ar Addysg Môn.

Bydd yr ysgol yn cydymffurfio â'r *Polisi Rheoli Cofnodion Ysgolion.*

17. Datgelu a Rhannu Gwybodaeth

Nid yw cyfraith diogelu data yn atal rhannu gwybodaeth, ac nid yw'n rhwystr, ond yn hytrach mae'n darparu fframwaith i sicrhau bod gwybodaeth bersonol yn cael ei rhannu'n gyfreithlon ac mewn ffordd briodol a diogel. Fodd bynnag, mae'n drosedd cael neu ddatgelu gwybodaeth am unigolyn yn fwriadol neu'n ddi-hid heb achos cyfreithlon. Dylid ond rhoi data perthnasol, cyfrinachol i:

- aelodau eraill o staff yn ôl yr angen;
- rhieni perthnasol/y sawl sydd â chyfrifoldeb rhiant;
- sefydliadau eraill os oes angen er budd y cyhoedd e.e. atal troseddu;
- awdurdodau eraill fel yr Awdurdod Addysg Lleol ac ysgolion y gall disgybl symud iddynt, lle mae gofynion cyfreithiol;
- sefydliadau sy'n cydweithio â'r ysgol (fel Gwasanaethau Cymdeithasol *(gwelir adran 17.2))* neu sy'n rhan o Brotocol Rhannu Gwybodaeth (ISP).

Wrth rannu gwybodaeth bersonol, bydd yr ysgol yn sicrhau:

- ei bod â hawl i rannu'r wybodaeth bersonol;
- dim ond gyda'r bobl *angenrheidiol* y caiff yr wybodaeth ei rhannu;
- bod diogelwch digonol (gan ystyried natur yr wybodaeth) ar waith i ddiogelu'r wybodaeth ac i sicrhau ei bod yn cael ei rhannu'n ddiogel;

- bydd yn rhoi amlinelliad mewn Hysbysiad Preifatrwydd o bwy sy'n derbyn gwybodaeth bersonol gan yr ysgol;
- bod yr wybodaeth yn gywir ac yn gyfoes;
- bod yr wybodaeth yn cael ei rhannu'n amserol.

Bydd aelodau unigol o staff ond yn cael gafael ar wybodaeth y mae ganddynt yr awdurdod i'w defnyddio, a dim ond at ddibenion awdurdodedig, a byddant ond yn caniatáu i staff eraill yr ysgol gael gafael ar wybodaeth bersonol os oes ganddynt yr awdurdodiad priodol.

Rhaid i benderfyniadau ynghylch a ddylid rhannu gwybodaeth gael eu gwneud fesul achos. Bydd yr ysgol yn seilio ei phenderfyniadau ynghylch rhannu gwybodaeth ar ystyriaethau o ddiogelwch a lles yr unigolyn ac eraill a allai gael eu heffeithio. Ni fydd yr ysgol yn datgelu unrhyw beth ar gofnod disgybl a fyddai'n debygol o achosi niwed difrifol i iechyd corfforol neu feddyliol y disgybl neu unrhyw un arall.

Ni ddylid datgelu gwybodaeth bersonol heb sefydlu pwy yw'r derbynnydd. Ni ddylid darparu gwybodaeth i bartïon eraill, hyd yn oed os ydynt yn gysylltiedig (e.e. yn achos rhieni sydd wedi'u gwahanu, mae'n bwysig nad yw gwybodaeth am un parti yn cael ei rhoi i'r parti arall nad oes ganddo hawl iddi). Bydd yr ysgol yn cadw cofnod o'r penderfyniad i rannu gwybodaeth ai peidio a bydd yn egluro'r rhesymau y tu ôl i'r penderfyniad. Os yw'r ysgol wedi rhannu gwybodaeth, cedwir cofnod o ba wybodaeth bersonol sydd wedi'i rhannu, gyda phwy y cafodd ei rhannu ac at ba ddiben.

Bydd unrhyw ddata personol a gaiff ei drosglwyddo i drydydd parti i'w brosesu (sef cwmni allanol) yn dod o dan Gytundeb Prosesu Data (DPA). Mae angen Cytundeb Prosesu Data pan fydd yr ysgol fel y Rheolwr Data yn gofyn i Brosesydd Data brosesu data ar ran yr ysgol.

Bydd yr ysgol yn ymuno â Chytundeb Rhannu Gwybodaeth Bersonol Cymru (WASPI). Offeryn yw hwn i helpu i rannu gwybodaeth bersonol yn effeithiol ac yn gyfreithlon ar sail amlasiantaethol yng Nghymru.

Os yw'r ysgol yn rhannu gwybodaeth yn rheolaidd ag asiantaeth neu sefydliad, efallai y bydd angen Protocol Rhannu Gwybodaeth (ISP) neu Gytundeb Datgelu Data (DDA) yn dibynnu ar y math o rannu gwybodaeth.

Gall yr ysgol hefyd rannu data personol gyda'r gwasanaethau brys ac awdurdodau lleol i'w helpu i ymateb i sefyllfa frys sy'n effeithio ar unrhyw ddisgyblion neu aelodau o staff.

Dylai'r ysgol gysylltu â'r Swyddog Diogelu Data Ysgolion i gael cyngor os oes gan yr ysgol unrhyw amheuaeth a ddylid rhannu gwybodaeth bersonol ai peidio gydag asiantaethau a thrydydd partïon sy'n gofyn am wybodaeth.

17.1. Cais gan Drydydd Parti am Wybodaeth Bersonol Unigolyn
Gall yr ysgol dderbyn ceisiadau gan asiantaethau neu drydydd partïon eraill fel yr Heddlu, yr Adran Gwaith a Phensiynau, cyfreithwyr ac ati i gael mynediad corfforol at neu dderbyn copi o'r wybodaeth bersonol sy'n ymwneud ag unigolyn.

Bydd yr ysgol yn rhannu data personol â gorfodaeth y gyfraith a chyrff llywodraethu lle mae'n ofynnol yn gyfreithiol iddi wneud hynny, gan gynnwys ar gyfer:

- atal neu ganfod trosedd a/neu dwyll;
- dal neu erlyn troseddwyr;
- asesu neu gasglu treth sy'n ddyledus i HMRC;
- yn gysylltiedig ag achosion cyfreithiol;
- lle mae'n ofynnol i'r datgeliad fodloni rhwymedigaethau diogelu;
- dibenion ymchwil ac ystadegol, cyn belled â bod data personol yn ddigon dienw neu fod caniatâd wedi'i ddarparu.

Bydd yr ysgol yn dilyn y *Weithdrefn ar gyfer Rhannu Gwybodaeth gydag Awdurdodau'r Heddlu yn y Deyrnas Unedig* wrth ddelio â cheisiadau gan yr Heddlu.

17.2. Amddiffyn Plant ac Oedolion Bregus

Nid yw *GDPR* na *Deddf Diogelu Data 2018* yn atal, nac yn cyfyngu ar rannu gwybodaeth at ddibenion cadw plant a phobl ifanc yn ddiogel.

Gellir rhannu gwybodaeth bersonol berthnasol yn gyfreithlon os yw am gadw plentyn neu unigolyn sydd mewn perygl yn ddiogel rhag esgeulustod neu niwed corfforol, emosiynol neu feddyliol, neu os yw'n diogelu ei les corfforol, meddyliol neu emosiynol. Yr ystyriaeth bwysicaf yw a yw rhannu gwybodaeth yn debygol o gefnogi diogelu ac amddiffyn plentyn.

Ni ddylai ofnau ynghylch rhannu gwybodaeth fod yn rhwystr i ddiogelu a hyrwyddo lles plant sydd mewn perygl o gael eu cam-drin neu eu hesgeuluso.

Bydd angen i'r ysgol ddilyn polisïau a gweithdrefnau diogelu yn ddi-oed o ran pa wybodaeth bersonol y gellir ei rhannu â'r awdurdodau perthnasol megis Gwasanaethau Plant a Theuluoedd, Gwasanaethau Oedolion neu'r Heddlu os oes unrhyw bryderon y gallai plentyn neu oedolyn sy'n agored i niwed fod mewn perygl o niwed difrifol neu sylweddol.

Dan rhai amgylchiadau, rhaid diystyru'r ddyletswydd o ddiogelu cyfrinachedd gwybodaeth bersonol, pan fo dyletswydd i amddiffyn plant neu oedolion sy'n agored i niwed sydd mewn perygl o niwed difrifol. Dan amgylchiadau o'r fath, bydd yr ysgol yn gofyn am gyngor gan y Swyddog Diogelu Data Ysgolion. Bydd yn rhaid cydbwyso'r risg a achosir a hawl yr unigolyn i breifatrwydd yn erbyn ei gilydd.

Os nad ydych yn siŵr pa wybodaeth y gellir ei rhannu, trafodwch gyda'r Swyddog Diogelu Data Ysgolion.

I gael rhagor o wybodaeth am rannu gwybodaeth i ddiogelu plant, cyfeiriwch at ddogfen *Llywodraeth Cymru - Deddf Gwasanaethau Cymdeithasol a Llesiant (Cymru) 2014, Gweithio Gyda'n Gilydd i Ddiogelu Pobl, Rhannu gwybodaeth i ddiogelu plant, Canllaw anstatudol i ymarferwyr*, Gorffennaf 2019 sydd ar gael ar Addysg Môn.

18. Digwyddiadau Diogelwch Data

Digwyddiad diogelwch data yw toriad diogelwch sy'n arwain at ddinistrio, colli, addasu, datgelu neu fynediad anawdurdodedig at ddata personol a drosglwyddir, a storir neu a brosesir mewn unrhyw ddull arall gan yr ysgol, yn ddamweiniol neu'n anghyfreithlon. Golyga hyn fod yr wybodaeth bersonol wedi cael ei chyfaddawdu, ei difrodi, ei cholli neu ei dwyn.

Gall digwyddiad diogelwch data fod ar sawl ffurf wahanol, mae enghreifftiau'n 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.

Bydd yr ysgol yn cysylltu â'r Swyddog Diogelu Data Ysgolion i roi gwybod am yr **holl** ddigwyddiadau diogelwch data/'digwyddiadau agos' **cyn gynted â phosibl.** Bydd yr ysgol yn ymchwilio i unrhyw achosion o dorri rheolau o'r fath a bydd yn cwblhau'r adroddiad gofynnol ar ddigwyddiadau diogelwch data heb oedi diangen. Mae

templed adroddiad digwyddiad diogelwch data ar gyfer ysgolion a chanllawiau cysylltiedig ar gael ar Addysg Môn.

Bydd angen i'r ysgol gymryd unrhyw gamau angenrheidiol i fynd i'r afael â'r digwyddiad diogelwch data a'i liniaru a bydd yn cymryd unrhyw gamau adferol os bydd angen. 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 yr ysgol hefyd yn adolygu a oes angen iddi wneud unrhyw newidiadau gofynnol i brosesau ac/neu arferion cyfredol er mwyn lleihau'r risg o ddigwyddiad tebyg yn digwydd eto.

Rhaid i'r ysgol gadw cofnod canolog o'r holl ddigwyddiadau diogelwch data a fydd yn cofrestru'r holl fethiannau cydymffurfio. Bydd ffigurau ynghylch nifer y digwyddiadau diogelwch data yn cael eu cynnwys yn yr adroddiad sicrwydd llywodraethu gwybodaeth blynyddol i gorff llywodraethu'r ysgol. Bydd y ffigurau hefyd yn cael eu cynnwys yn adroddiad cryno blynyddol lefel uchel y Swyddog Diogelu Data Ysgolion ar bob ysgol a gyflwynir i Uwch Dîm Rheoli'r Gwasanaeth Dysgu a Phwyllgor Archwilio a Llywodraethu Cyngor Sir Ynys Môn.

Os yw'r digwyddiad diogelwch data yn debygol o arwain at risg i hawliau a rhyddid unigolion, mae'n ofynnol i'r ysgol roi gwybod i Swyddfa'r Comisiynydd Gwybodaeth am y digwyddiad diogelwch data, **o fewn 72 awr** o ddod yn ymwybodol ohono. **Y Swyddog Diogelu Data Ysgolion sy'n penderfynu a oes angen rhoi gwybod i Swyddfa'r Comisiynydd Gwybodaeth am y toriad ai peidio.**

Bydd angen i'r ysgol hefyd hysbysu'r unigolion yr effeithir arnynt heb oedi diangen os yw digwyddiad diogelwch data yn debygol o arwain at risg *uchel* i'w hawliau a'u rhyddid.

Bydd yr ysgol yn cydymffurfio â'r *Polisi Tor-rheolau Data Ysgolion.*

Mae angen i'r holl staff fod yn agored am unrhyw ddigwyddiadau fel bod yr ysgol yn sicrhau ei bod yn gweithredu'n gyfrifol, yn cefnogi aelodau o staff ac yn delio â'r digwyddiad cyn gynted â phosib ac mor effeithlon â phosib. Gall peidio â rhoi gwybod am ddigwyddiad y dylid bod wedi'i adrodd i Swyddfa'r Comisiynydd Gwybodaeth arwain at ganlyniadau i'r ysgol ac i'r aelod unigol o staff.

19. Rhannu Pryderon Diogelu Data

Dylai staff yn yr ysgol hysbysu'r Pennaeth/person sy'n gyfrifol am ddiogelu data o fewn yr ysgol, ac os yw'n briodol, y Swyddog Diogelu Data Ysgolion, os oes ganddynt unrhyw bryderon neu os ydynt yn amau bod un o'r canlynol wedi digwydd (neu'n digwydd neu'n debygol o ddigwydd):

- prosesu data personol heb sail gyfreithlon ar gyfer ei brosesu neu, yn achos gwybodaeth bersonol sensitif, heb fodloni un o'r amodau cyfreithiol yn *Erthygl 9*;

- mynediad at wybodaeth bersonol heb yr awdurdodiad priodol;
- gwybodaeth bersonol nad yw'n cael ei chadw na'i dileu/ei dinistrio'n ddiogel;
- cael gwared ar wybodaeth bersonol, neu ddyfeisiau sy'n cynnwys gwybodaeth bersonol (neu y gellir eu defnyddio i gael mynediad ati), o safle'r ysgol heb i fesurau diogelwch priodol fod ar waith;
- unrhyw achos arall o dorri'r polisi hwn neu unrhyw un o'r egwyddorion diogelu data a nodir yn adran 6.

20. Rhestr o Asedau Gwybodaeth

Bydd angen i'r Pennaeth sicrhau bod *Rhestr o Asedau Gwybodaeth* ar waith a'i bod yn cael ei hadolygu'n rheolaidd. Mae'r *Rhestr o Asedau Gwybodaeth* yn cynnwys gwybodaeth am ba ddata a gedwir, lle caiff ei storio, sut y caiff ei ddefnyddio, pwy sy'n gyfrifol ac unrhyw reoliadau neu amserlenni cadw pellach a allai fod yn berthnasol.

Mae templed *Rhestr o Asedau Gwybodaeth* ar gael ar Addysg Môn.

21. Hysbysiad Preifatrwydd

Mae gan yr ysgol Hysbysiad Preifatrwydd ar waith sy'n rhoi gwybod i unigolion am yr wybodaeth bersonol sy'n cael ei chasglu ac sy'n cael ei chadw amdanynt a sut y gallent ddisgwyl i'w gwybodaeth bersonol gael ei defnyddio ac at ba ddibenion. Rhaid i'r Hysbysiad Preifatrwydd fod yn benodol i'r gweithgaredd sy'n gofyn am wybodaeth bersonol. Rhaid i hyn ddigwydd ar yr adeg y mae'r wybodaeth yn dechrau cael ei chasglu ar unigolyn am y tro cyntaf.

Pryd bynnag y cesglir gwybodaeth am unigolion, bydd yr ysgol yn darparu'r wybodaeth ganlynol fel bod yr ysgol yn dryloyw ac yn darparu gwybodaeth hygyrch am sut y defnyddir data personol:

- manylion adnabod a chyswllt yr ysgol fel y rheolwr data;
- y diben y mae'r wybodaeth yn cael ei chasglu ar ei gyfer;
- y sail gyfreithlon ar gyfer casglu'r wybodaeth;
- unrhyw ddibenion eraill y gellir ei ddefnyddio ar eu cyfer;
- sut y cesglir yr wybodaeth;
- gyda phwy y bydd neu y gellir rhannu'r wybodaeth (unrhyw drydydd partïon);
- pa mor hir y cedwir yr wybodaeth;
- manylion am hawliau unigolion (e.e. yr hawliau mynediad at ddata personol sy'n cael ei gadw gan yr ysgol);
- manylion am y Swyddog Diogelu Data Ysgolion.

Cymerir camau priodol i ddarparu gwybodaeth yn yr Hysbysiad Preifatrwydd ar ffurf gryno, dryloyw, ddealladwy a hygyrch, gan ddefnyddio iaith glir a phlaen. Os cesglir gwybodaeth yn uniongyrchol gan blentyn, rhaid i'r Hysbysiad Preifatrwydd fod yn briodol i'w oedran.

Bydd yr Hysbysiad Preifatrwydd yn cael ei rannu drwy wefan yr ysgol; cyfrifon cyfryngau cymdeithasol, a byddant ar gael ar ffurf copi caled ar gais.

Bydd crynodeb o'r Hysbysiad Preifatrwydd yn cael ei gynnwys ym mhob dogfen sy'n casglu gwybodaeth bersonol ac o fewn ffurflenni caniatâd.

Mae templed Hysbysiad Preifatrwydd ar gyfer rhieni a disgyblion a hefyd ar gyfer gweithlu'r ysgol, ar gael ar Addysg Môn.

22. Asesiadau Effaith Diogelu Data (DPIAau)

Lle mae prosesu'n debygol o arwain at risg uchel i hawliau a rhyddid unigolyn (e.e. lle mae'r ysgol yn bwriadu defnyddio math newydd o dechnoleg), cyn dechrau'r prosesu, bydd DPIA yn cael ei wneud i asesu'r canlynol:

- a yw'r prosesu'n angenrheidiol ac yn gymesur mewn perthynas â'i ddiben;
- y risgiau i unigolion;
- pa fesurau y gellir eu rhoi ar waith i fynd i'r afael â'r risgiau hynny a diogelu gwybodaeth bersonol.

Cyn cyflwyno unrhyw fath newydd o dechnoleg, dylai'r ysgol felly gysylltu â'r Swyddog Diogelu Data Ysgolion er mwyn gallu ymgymryd â DPIA.

Yn ystod unrhyw DPIA, bydd yr ysgol yn ceisio barn unrhyw grŵp cynrychioliadol ac unrhyw randdeiliaid perthnasol eraill (lle bo hynny'n berthnasol).

Mae DPIAau yn ofyniad cyfreithiol ar gyfer gweithgareddau prosesu sy'n debygol o fod yn risg uchel. Dylid ystyried DPIA fel proses barhaus gydag adolygiadau rheolaidd yn seiliedig ar lefel y risg a natur y gweithgaredd prosesu.

Mae polisi a templed *Asesiad Effaith Diogelu Data Ysgolion (DPIA)* yn ogystal â *Matrics Risg Diogelu Data Ysgolion* a templed *Rhestr Risg Diogelu Data Ysgolion* ar gael ar Addysg Môn.

23. Diogelwch Gwybodaeth

23.1. Ysgol

Bydd yr ysgol yn defnyddio mesurau technegol a threfniadol priodol i gadw gwybodaeth bersonol yn ddiogel, ac yn arbennig i ddiogelu rhag prosesu anawdurdodedig neu anghyfreithlon ac yn erbyn colled, dinistr neu ddifrod damweiniol.

Bydd yr ysgol yn sicrhau:

- lle y bo'n bosibl, bod gwybodaeth bersonol yn cael ei ffugenwi neu ei hamgryptio;

- cyfrinachedd, uniondeb, argaeledd a gwydnwch parhaus mewn systemau a gwasanaethau prosesu;
- os bydd digwyddiad corfforol neu dechnegol, y gellir adfer argaeledd a mynediad at wybodaeth bersonol mewn modd amserol;
- bod proses ar waith i brofi, asesu a gwerthuso effeithiolrwydd mesurau technegol a sefydliadol yn rheolaidd er mwyn sicrhau diogelwch y prosesu;
- bod mannau diogel priodol ar gael yn yr ysgol i gynnal sgyrsiau preifat rhwng staff, disgyblion, rhieni/y rhai sydd â chyfrifoldeb rhiant ac ymwelwyr e.e. derbynfeydd sy'n addas i rannu gwybodaeth bersonol gyda dim ond y rhai y mae angen iddynt fod yn rhan o'r sgwrs heb y risg y bydd eraill yn clywed;
- bod yn rhaid nodi'r holl ddata categorïau personol ac arbennig sy'n cael ei storio ar systemau TG yr ysgol gan ddefnyddio termau dosbarthu data (SWYDDOGOL neu SWYDDOGOL-SENSITIF).

Bydd yr ysgol yn cydymffurfio gyda'r *Polisi Diogelwch Data Ysgolion.*

23.2. Sefydliadau Allanol

Lle mae'r ysgol yn defnyddio sefydliadau allanol i brosesu gwybodaeth bersonol ar ei rhan, mae angen gweithredu trefniadau diogelwch ychwanegol mewn contractau a chytundebau gyda'r sefydliadau hynny i ddiogelu gwybodaeth bersonol. Rhaid i gontractau a chytundebau â sefydliadau allanol sicrhau:

- dim ond ar gyfarwyddiadau ysgrifenedig yr ysgol y gall y sefydliad weithredu;
- mae'r rhai sy'n prosesu'r data yn destun dyletswydd hyder;
- cymerir camau priodol i sicrhau diogelwch prosesu;
- dim ond gyda chydsyniad yr ysgol ymlaen llaw ac o dan gontract ysgrifenedig y mae isgontractwyr yn ymwneud â hwy;
- bydd y sefydliad yn cynorthwyo'r ysgol i ddarparu mynediad i wrthrychau a chaniatáu i unigolion arfer eu hawliau mewn perthynas â diogelu data;
- bydd y sefydliad yn cynorthwyo'r ysgol i gyflawni ei rhwymedigaethau mewn perthynas â diogelwch prosesu, hysbysu am ddigwyddiadau diogelwch data ac Asesiadau Effaith Diogelu Data (DPIAau);
- bydd y sefydliad yn dileu neu'n dychwelyd yr holl wybodaeth bersonol i'r ysgol yn ôl y gofyn ar ddiwedd y contract; a
- bydd y sefydliad yn cyflwyno archwiliadau ac arolygiadau; darparu pa wybodaeth bynnag sydd ei hangen ar yr ysgol i sicrhau ei bod yn cyflawni ei rhwymedigaethau diogelu data, a dweud wrth yr ysgol ar unwaith os gofynnir iddi wneud rhywbeth sy'n dor-cyfraith diogelu data.

Cyn i unrhyw gytundeb newydd sy'n ymwneud â phrosesu gwybodaeth bersonol gan sefydliad allanol gael ei ymrwymo, neu cyn i gytundeb presennol gael ei newid, rhaid i'r ysgol ofyn i'r Swyddog Diogelu Data Ysgolion gymeradwyo ei thelerau. Bydd y Swyddog Diogelu Data Ysgolion yn sicrhau bod cytundebau sydd wedi'u diffinio'n glir ar waith rhwng yr ysgol a'r sefydliad i sicrhau bod data wedi'i ddiogelu'n briodol ac yn rhoi eglurder ynghylch rolau a chyfrifoldebau.

24. Storio Gwybodaeth Bersonol yn Ddiogel

Rhaid storio gwybodaeth bersonol mewn lleoliad diogel gyda mynediad ar gael i unigolion awdurdodedig sydd angen mynediad i'r wybodaeth bersonol benodol honno yn unig. Rhaid diogelu a chadw'r holl wybodaeth bersonol yn ddiogel er mwyn atal colled, camddefnydd neu ddifrod.

24.1. Cofnodion Papur

Dylid cadw gwybodaeth bersonol dan glo bob amser. Dylai unrhyw ddroriau, cypyrddau, cabinetau, ystafelloedd storio neu gynwysyddion storio fod yn gadarn ac wedi'u cloi pan nad ydynt yn cael eu defnyddio. Ni ddylid gadael dogfennau sy'n cynnwys gwybodaeth bersonol ar ddesgiau swyddfa ac ystafell ddosbarth, ar fyrddau ystafelloedd staff na'u pinio i hysbysfyrddau lle ceir mynediad cyffredinol.

Dylid cymryd gofal arbennig os oes rhaid mynd â dogfennau allan o adeilad yr ysgol. Ni ddylid mynd â dogfennau sy'n cynnwys gwybodaeth bersonol oddi ar safle'r ysgol oni bai bod mesurau diogelwch priodol ar waith i ddiogelu'r wybodaeth.

Dylid cadw dogfennau mewn lleoliad diogel a hygyrch sy'n cael ei ddiogelu rhag llifogydd, lleithder ac elfennau eraill. Efallai y bydd angen cadw rhai dogfennau mewn cynwysyddion aerdyn i'w diogelu rhag difrod amgylcheddol.

Dylid cau bleindiau ar ffenestri llawr gwaelod ar ddiwedd y dydd.

24.2. Cofnodion Electronig

Os cedwir gwybodaeth bersonol yn electronig, mae angen i fesurau diogelwch technegol priodol fod ar waith ar bob dyfais fel ffugenwi, amgryptio neu ddiogelu cyfrinair.

Mae angen i bob dyfais electronig sy'n cynnwys gwybodaeth bersonol gael ei diogelu â chyfrinair gyda mynediad yn cael ei ddarparu i unigolion awdurdodedig yn unig.

Mae angen i gyfrineiriau cryf fod ar waith sy'n cynnwys o leiaf naw nod; cynnwys symbolau; cymysgedd o gymeriadau bras a bach a chymysgedd o rifau a llythrennau. Dylid defnyddio cyfrineiriau gwahanol ar gyfer systemau a dyfeisiau ar wahân. Ni ddylid ysgrifennu cyfrineiriau a manylion mewngofnodi ac ni ddylid eu rhannu ag unrhyw un arall.

Bydd yr holl sgriniau cyfrifiaduron a gliniaduron yn cloi'n awtomatig ar ôl cyfnod penodol a bydd staff hefyd yn cloi eu sgriniau'n gorfforol os byddant yn gadael eu desgiau am gyfnod o amser.

Bydd data'n cael ei gadw wrth gefn yn unol â gweithdrefnau gwneud copi wrth gefn.

Dylid cadw pob dyfais electronig gludadwy mor ddiogel â phosibl. Os ydynt yn cynnwys gwybodaeth bersonol, dylid eu cadw dan glo ag allwedd pan nad ydynt yn cael eu defnyddio.

Dylid defnyddio meddalwedd amgryptio i ddiogelu pob dyfais gludadwy a chyfryngau symudadwy, megis dyfeisiau USB (cofion bach neu fath arall o storio cof nad yw'n rhan o'r cyfrifiadur ei hun) sy'n dal gwybodaeth bersonol. Ni ddylai aelodau'r staff symud dyfeisiau sy'n cynnwys gwybodaeth bersonol (neu y gellir eu defnyddio i gael mynediad ati), o safle'r ysgol oni bai bod mesurau diogelwch priodol ar waith i ddiogelu gwybodaeth a'r ddyfais.

Ni anogir defnyddio dyfeisiau cyfryngau symudadwy pan fydd technolegau amgen ar gael lle nad oes angen trosglwyddo data'n gorfforol rhwng lleoliadau. Bydd yr ysgol yn symud i ffwrdd o ddefnyddio'r mathau hyn o ddyfeisiau ar gyfer storio gwybodaeth bersonol lle bynnag y bo modd.

Ni fydd aelodau'r staff yn defnyddio dyfeisiau personol na gyriannau (fel ffonau symudol) i storio neu rannu gwybodaeth bersonol sy'n ymwneud â'r ysgol a busnes gwaith.

25. Cael Gwared â Gwybodaeth Bersonol yn Ddiogel

Bydd gwybodaeth bersonol (a gwybodaeth categori arbennig) nad oes ei hangen mwyach yn unol â'r *Cyfnodau Cadw Cofnodion Ysgolion* yn cael ei dileu'n barhaol o systemau gwybodaeth yr ysgol a bydd unrhyw gopïau caled o wybodaeth bersonol yn cael eu dinistrio mewn modd diogel.

Gellir dinistrio gwybodaeth bersonol yn ddiogel drwy ddefnyddio peiriannau rhwygo traws neu drwy drefniadau gwaredu gwastraff diogel. Gall yr ysgol ddefnyddio trydydd parti priodol i waredu cofnodion yn ddiogel ar ran yr ysgol. Os felly, bydd yr ysgol yn ei gwneud yn ofynnol i'r trydydd parti ddarparu digon o sicrwydd ei fod yn cydymffurfio â chyfraith diogelu data (e.e. Tystysgrif Dinistr).

Ni fydd data personol yn cael ei adael mewn lleoliad anniogel tra yn y broses o gael ei ddinistrio'n ddiogel. Ni chaiff gwybodaeth bersonol ei diystyru drwy wastraff cyffredinol, ailgylchu na thrwy sgip. **Rhaid** defnyddio dull diogel ym mhob achos lle ceir data personol.

26. Ffi Diogelu Data Flynyddol

Mae'n ofynnol i ysgolion, fel pob sefydliad neu unig fasnachwr sy'n prosesu gwybodaeth bersonol, o dan *Reoliadau Diogelu Data (Ffioedd a Gwybodaeth) 2018*, dalu ffi diogelu data flynyddol i Swyddfa'r Comisiynydd Gwybodaeth, oni bai eu bod wedi'u heithrio. **Mae'n ofynnol i bob ysgol dalu'r ffi diogelu data flynyddol**. Bydd methu â gwneud hynny yn arwain at gosb benodedig. Bydd yr ysgol yn cofrestru fel corff cyhoeddus.

Ychwanegir manylion cofrestru at y gofrestr gyhoeddus diogelu data y gellir ei gweld ar wefan Swyddfa'r Comisiynydd Gwybodaeth. Mae gan yr ysgol rif cofrestru unigryw. Mae manylion cyswllt y Swyddog Diogelu Data Ysgolion wedi'u cynnwys yn erbyn manylion cofrestru'r ysgol.

27. Ffotograffau a Delweddau

Fel rhan o weithgareddau'r ysgol, bydd ffotograffau a delweddau yn cael eu tynnu o unigolion o fewn yr ysgol. Bydd ffotograffau a delweddau a dynnwyd at ddefnydd swyddogol yr ysgol y gellir eu defnyddio ar gyfer deunyddiau cyfathrebu, marchnata a hyrwyddo yn cael eu cynnwys o dan *GDPR* a *Deddf Diogelu Data 2018* a bydd angen i'r ysgol roi gwybod i ddisgyblion pam eu bod yn cael eu cymryd a beth y byddant yn cael eu defnyddio ar eu gyfer.

Mae ffurflen ganiatâd ar gael ar Addysg Môn sydd i'w defnyddio er mwyn cael caniatâd disgyblion/rhieni/y rhai sydd â chyfrifoldeb rhiant ynglŷn â ble y cyhoeddir y ffotograffau a'r delweddau. Darperir caniatâd ar wahanol elfennau o ran ble y gellir rhannu a defnyddio ffotograffau a delweddau megis ar wefan yr ysgol, cyfrifon cyfryngau cymdeithasol, papurau newydd, llyfrynnau, cylchlythyrau ac apiau.

Gellir gwrthod neu dynnu caniatâd yn ôl ar unrhyw adeg. Os tynnir caniatâd yn ôl, bydd yr ysgol yn dileu'r ffotograff neu'r fideo ac yn peidio â'i ddosbarthu ymhellach.

28. Gwefan a Chyfryngau Cymdeithasol

Bydd yr ysgol yn cael caniatâd ysgrifenedig i rannu gwybodaeth bersonol am ddisgyblion ar ei gwefan a chyfrifon cyfryngau cymdeithasol, gan gynnwys ffotograffau a delweddau. Bydd disgyblion, rhieni/y rhai sydd â chyfrifoldeb rhiant yn cael gwybod am ganlyniadau lledaenu data personol ledled y byd.

Mae ffurflen ganiatâd ar gael ar Addysg Môn sydd i'w defnyddio er mwyn cael caniatâd disgyblion/rhieni/y rhai sydd â chyfrifoldeb rhiant ynghylch pa wybodaeth, ffotograffau a delweddau fydd yn cael eu cyhoeddi ar unrhyw wefannau a chyfrifon cyfryngau cymdeithasol.

Gellir gwrthod neu dynnu caniatâd yn ôl ar unrhyw adeg. Os tynnir caniatâd yn ôl, bydd yr ysgol yn cymryd pob cam rhesymol i ddileu/tynnu'r wybodaeth/ffotograff/ delwedd oddi ar y wefan a/neu gyfrifon cyfryngau cymdeithasol i atal dosbarthiad pellach. Fodd bynnag, rhaid cydnabod gan fod y data personol ar wefan a/neu gyfrifon cyfryngau cymdeithasol, mae'n bosibl fod yr wybodaeth eisoes wedi'i gweld a'i rhannu y tu hwnt i reolaeth yr ysgol.

29. E-bost

Bydd staff yr ysgol ond yn defnyddio cyfrif e-bost awdurdodedig i gyfathrebu mewn perthynas â busnes yr ysgol. Ni fydd staff yr ysgol yn defnyddio eu cyfrif e-bost personol i gyfathrebu â disgyblion ac i rannu data personol.

Os oes rhaid rhannu dogfennau sy'n cynnwys gwybodaeth bersonol drwy e-bost, caiff y ddogfen ei diogelu â chyfrinair, gyda'r cyfrinair ar wahân a'i rhannu'n ddiogel gyda'r derbynnydd arfaethedig.

Bydd cyfrifon e-bost ysgolion hefyd yn amodol ar y rheoliadau diogelu data a rhaid dilyn y *Cyfnodau Cadw Cofnodion Ysgolion* ynghylch gwybodaeth bersonol a gynhwysir mewn negeseuon e-bost. Bydd yr ysgol yn cydymffurfio â *Pholisi E-bost Staff Ysgolion.*

30. CCTV (os yn berthnasol)

Mae cipio a/neu recordio delweddau o unigolion adnabyddadwy yn enghraifft o brosesu gwybodaeth bersonol ac felly mae angen iddynt gydymffurfio â *GDPR* a *Deddf Diogelu Data 2018*. Rhaid i'r ysgol hefyd fod â *Pholisi CCTV* ar waith. Mae *Polisi CCTV Ysgolion* ar gael ar Addysg Môn.

Mae angen cwblhau Asesiad Effaith Diogelu Data (DPIA) wrth ddefnyddio CCTV neu ystyried prynu system wyliadwriaeth. Bydd y Swyddog Diogelu Data Ysgolion yn rhoi arweiniad a chymorth i gwblhau'r rhain.

Rhaid i'r ysgol hysbysu staff, disgyblion ac ymwelwyr pam ei bod yn casglu gwybodaeth bersonol ar ffurf delweddau CCTV. Rhaid cael arwydd sy'n hysbysu hyn ar waith ym mhob parth sy'n cael ei ffilmio. Bydd defnyddio arwyddion mewn mannau amlwg wrth fynedfa'r ysgol ac yna defnyddio arwyddion pellach y tu mewn i'r parthau yn rhoi gwybod i bobl pan fyddant mewn ardal lle mae system wyliadwriaeth ar waith.

Bydd yr ysgol yn sicrhau bod ganddi gyfnod cadw penodol yn seiliedig ar yr angen posibl i adolygu'r ffilm a bydd yn ystyried pwy sy'n cael mynediad i'r ffilm hon a pham.

Bydd gan unigolion ac asiantaethau gorfodaeth y gyfraith yr hawl i ofyn am gael mynediad i'r delweddau. Bydd pob cais o'r fath yn cael ei gofnodi.

Bydd yr ysgol yn dilyn *'In the picture: A data protection code of practice for surveillance cameras and personal information'.*

31. Gwybodaeth Fiometrig (os yn berthnasol)

Ystyrir y math hwn o wybodaeth fel data categori arbennig. Rhaid ymdrin â'r holl ddata o'r fath yn briodol ac yn unol ag egwyddorion *GDPR* a *Deddf Diogelu Data 2018.*

Mae enghreifftiau o systemau adnabod biometrig yn cynnwys olion bysedd a systemau adnabod wynebau (e.e. myfyrwyr sy'n defnyddio olion bysedd i dderbyn cinio ysgol yn hytrach na thalu gydag arian parod).

Bydd yr ysgol yn cael caniatâd ysgrifenedig disgyblion/rhieni/y rhai sydd â chyfrifoldeb rhiant cyn cofnodi a phrosesu manylion biometrig y disgybl. Mae'r ffurflen ganiatâd ar gael ar Addysg Môn.

Gall disgyblion/rhieni/y rhai sydd â chyfrifoldeb rhiant wrthwynebu cymryd rhan yn systemau adnabod biometrig yr ysgol, neu dynnu caniatâd yn ôl ar unrhyw adeg, a bydd yr ysgol yn sicrhau bod unrhyw ddata perthnasol a gasglwyd eisoes yn cael ei ddileu. Rhaid nodi dulliau amgen o ddarparu gwasanaethau os nad yw rhiant/rhieni sydd â chyfrifoldeb rhiant neu ddisgybl yn rhoi caniatâd.

32. Trosglwyddiadau Data Rhyngwladol

Ni ellir trosglwyddo unrhyw ddata categori personol nac arbennig y tu allan i'r Ardal Economaidd Ewropeaidd (EEA), sy'n cynnwys y gwledydd yn yr Undeb Ewropeaidd a Gwlad yr Iâ, Liechtenstein a Norwy. Gellir trafod hyn ymhellach gyda'r Swyddog Diogelu Data Ysgolion os oes angen.

33. Hyfforddiant

Bydd y Pennaeth a'r Swyddog Diogelu Data Ysgolion yn sicrhau bod staff wedi'u hyfforddi'n ddigonol ynglŷn â'u cyfrifoldebau diogelu data. Bydd penaethiaid, llywodraethwyr ysgol ac unigolion y mae angen i'w rolau gael mynediad rheolaidd at wybodaeth bersonol, neu sy'n gyfrifol am weithredu'r polisi hwn, yn cael hyfforddiant ychwanegol i'w helpu i ddeall eu dyletswyddau a sut i gydymffurfio â hwy.

Bydd angen i holl staff yr ysgol sicrhau eu bod wedi cwblhau'r hyfforddiant modiwl e-ddysgu GDPR gorfodol.

Bydd y Pennaeth yn cadw cofnod o bresenoldeb a chofrestr o bwy sydd wedi cwblhau unrhyw hyfforddiant diogelu data a pha bryd y cafodd ei gwblhau.

34. Torri'r Polisi

Gallai peidio â chydymffurfio â'r polisi hwn gan aelodau o staff yr ysgol arwain at ganlyniadau difrifol.

Gall hyn arwain at roi'r unigolion y mae eu gwybodaeth bersonol yn cael ei phrosesu a'r ysgol mewn perygl.

Mae perygl o gosbau sifil a throseddol sylweddol i'r unigolyn a'r awdurdodau ysgol a gymerir gan drydydd partïon. Gall unigolyn gyflawni trosedd o dan y *GDPR*, er enghraifft, drwy gael a/neu ddatgelu data personol at ei ddibenion ei hun heb ganiatâd yr ysgol.

Felly, ystyrir bod diffyg cydymffurfio gan aelod o staff yn fater disgyblu a allai, yn dibynnu ar yr amgylchiadau, arwain at ddiswyddo am gamymddwyn difrifol.

Os bydd rhywun nad yw'n gyflogai yn torri'r polisi hwn, efallai y bydd ei gontract yn dod i ben ar unwaith.

35. Adolygu'r Polisi a Threfniadau Arolygiaeth

Bydd y polisi hwn yn cael ei adolygu gan y Swyddog Diogelu Data Ysgolion yn flynyddol. Caiff y polisi ei gymeradwyo gan Uwch Dîm Rheoli'r Gwasanaeth Dysgu a chaiff ei fabwysiadu gan gorff llywodraethu'r ysgol. Caiff cydymffurfiaeth â'r polisi hwn a gweithdrefnau cysylltiedig eu monitro gan Dîm Arweinyddiaeth yr ysgol a'r corff llywodraethu.

Os oes unrhyw ymholiadau neu bryderon am unrhyw beth a gynhwysir yn y polisi hwn, dylid cysylltu â'r Swyddog Diogelu Data Ysgolion heb betruso:

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

Gellir cael rhagor o wybodaeth am ddiogelu data ar wefan yr ICO: https://ico.org.uk/

Content **Page**

1. Policy Statement

In order to operate efficiently, the school has to collect and use information about individuals with whom it works with. In addition, it may be required by law to collect and use information in order to comply with the requirements of the Welsh Government.

This policy sets out how the school complies with data protection obligations and seeks to protect personal information *(please see section 4 for the relevant definition).* The school is fully committed to ensuring that personal information is properly managed and protected and that it ensures full compliance with data protection legislation.

Its purpose is also to ensure that all staff members understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access to in the course of their work. The school will ensure that it treats personal information lawfully and correctly.

The school will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so. The school will consult and seek the advice of the Schools Data Protection Officer relating to any issues, concerns or questions and before initiating any new data processing activities.

2. Scope

This policy applies to all employees, governors, contractors, agencies, representatives and temporary staff working for and who process personal data on behalf of the school.

This policy applies to the personal information of job applicants, current and former staff, including employees, temporary and agency workers, governors, suppliers, volunteers, trainees/students, visitors, pupils and parents/those with parental responsibility.

This policy applies to all personal information created or held by the school in whatever format (including, but not limited to, paper, electronic, e-mail, film, video, CCTV, photographic images) and however it is stored (for example ICT system/database, shared drive filing structure, e-mail, filing cabinet, shelves and drawers).

The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments, staff development reviews and disciplinary records.

GDPR does not apply to deceased individuals as information about a deceased person does not constitute personal data and therefore is not subject to the *GDPR.*

3. Legislation, Guidance and Policies

The main data protection legislation that this policy complies with is that of the *General Data Protection Regulation (GDPR)* and the *Data Protection Act 2018.*

This policy is also based on relevant codes of practice and on guidance published by the Information Commissioner's Office (ICO).

The school will also refer to other relevant internal policies and guidance which contain further information regarding the protection of personal information in other contexts. These are all available on Addysg Môn.

4. 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.
Data breach	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 information.
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.
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 users	Includes employees whose work involves using personal data. Data users have a duty to protect the information they handle by following data protection and security policies at all times. Staff employed within schools are data users.

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.
Data Protection Officer	A DPO assists to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
Third-party information	A third party is somebody who is not the data controller, the data processor or the data subject.
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.
Criminal records information	Personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.
Consent	Of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The burden of demonstrating consent is on the data controller.
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.
Anonymised	To remove identifying information from something (such as computer data) so that the original source cannot be known or identified.
Genetic data	Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. Fingerprint recognition is an example of dactyloscopic data.
Data concerning health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
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.
Unauthorised	Without a legitimate right.

5. Responsibilities

The protection of personal data is everybody's responsibility. All staff members must ensure that they are committed to complying with data protection obligations.

The new data protection legislation moves schools from being required to 'comply' with data protection, to being required to 'demonstrate' compliance with legislation. Schools will need to evidence compliance in order to meet the overarching principle of accountability.

5.1. School Governing Body

The school governing body has the responsibility for:

- the school's overall compliance with *GDPR* and the *Data Protection Act 2018;*
- maintaining the strategic oversight of the school's compliance by requesting to see evidence of compliance and to undertake monitoring visits to the school;
- appointing a governor as a Data Protection Champion on the governing board;
- regularly discussing data protection issues and matters at governing board meetings;
- monitoring the identified data protection risks of the school and to monitor actions that are in place to mitigate these risks;
- undertaking data protection training offered.

5.2. 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 compliance with *GDPR* and the *Data Protection Act 2018* within the day-to-day activities of the school;
- being the representative of the school as the data controller;
- ensuring and promoting understanding and compliance with this policy and other statutory and regulatory policies relating to data protection;
- regularly reviewing and keeping the school's *Information Asset Register* and *Records of Processing Activities (ROPA)* up-to-date;
- ensuring information assets and risks within the school are managed;

- ensuring that the school has registered and paid the annual data protection fee to the ICO;
- conducting internal audits that monitor compliance;
- to ensure that relevant information and support is provided regarding data subject access requests so that requests are processed within one calendar month;
- establishing a reporting and learning culture to allow the school to establish where problems exist and to develop strategies with the Schools Data Protection Officer to prevent future problems occurring;
- working with, and is the key link, between the school and the Schools Data Protection Officer in ensuring that the school is complying with its data protection obligations.

The school may appoint a member of staff to be the person who is *responsible* for data protection within the school who will deal with the day-to-day tasks and responsibilities for data protection, but will *not* take on the statutory responsibilities of a Data Protection Officer. This responsibility will remain with the Schools Data Protection Officer.

5.3. All Staff within the School

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

- complying both on an individual and collective basis with the *GDPR* and the *Data Protection Act 2018* within the day-to-day activities of the school;
- ensuring personal information is kept and processed in line with the *GDPR* and the *Data Protection Act 2018*;
- informing the Headteacher and/or the person responsible for data protection within the school immediately of any incidents, concerns, requests and breaches relating to data protection;
- informing the Headteacher of any changes to personal details in order to help the school to keep personal information regarding staff up-to-date;
- ensuring understanding and compliance with this policy;
- ensuring understanding and compliance with all policies relating to data protection and security;
- adopting good practice standards relating to data protection;
- undertaking all data protection training offered.

5.4. Schools Data Protection Officer

The Schools Data Protection Officer is responsible for:

- informing and advising schools on their data protection obligations;
- monitoring compliance and performance against obligations, including conducting data protection compliance audits and reviews;

- providing advice, guidance and recommendations on the impact of the school's data protection efforts and issues;
- providing an annual information governance assurance report to the school's governing body, and to provide a high level annual summary report on all schools to the Learning Service Senior Management Team and the Isle of Anglesey County Council Audit and Governance Committee;
- creating and regularly reviewing data protection procedures, policies, guidance and templates;
- facilitating and supporting the school to respond to data subject access requests within the time period;
- supporting and providing advice in the event of a data breach;
- checking and approving with third parties that handle the school's data, any contracts or agreements regarding data processing;
- arranging and delivering data protection training for staff within schools including school governors;
- being the first point of contact for individuals whose data the school processes, and for the ICO.

6. Data Protection Principles

The school's approach to data protection will be, as required by GDPR, 'data protection by design and default' and 'privacy by design'. In essence, this means that the school needs to integrate data protection in to processing activities and business practices, from the design stage right through the lifecycle.

The school will comply with the following **six fundamental data protection principles** when processing personal information:

1. Personal information will be processed in a legal, fair and transparent manner;
2. Personal information will be collected for specified, explicit and legitimate purposes only, and will not be processed in a way that is incompatible with those legitimate purposes;
3. Will only process personal information if it is adequate, relevant and is limited to what is necessary for the relevant purposes (data minimisation);
4. Personal information must be kept accurate and up-to-date, and reasonable steps will be taken to ensure that inaccurate personal information is deleted or corrected without delay;
5. Personal information will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed;
6. Personal information will be processed safely. Appropriate technical security measures will be taken to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

The school will review the purposes of the particular processing activity and select the most appropriate lawful basis (or bases) for that processing before the processing starts for the first time and then regularly while it continues. Please see section 10 for definitions of specific processing activities.

The school must have the ability to **demonstrate** compliance with these principles. If the school is unable to comply with all six principles, then data should **not** be processed.

7. Data Subject's Rights

Data protection legislation provides the following rights for individuals:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erase;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling.

The Schools Data Protection Officer will support the school with dealing with any requests from individuals to exercise any of their rights.

7.1. The right to be informed

Individuals have the right to know that information about them is being processed. The school will inform individuals at the point of collection, by a Privacy Notice, about how, why and on what basis that information is processed.

7.2. The right of access

Individuals have the right to obtain confirmation that their information is being processed and to also request access and to have copies of personal information that the school holds about them or information about a child they are responsible for (subject access request-SAR).

A subject access request can be made verbally or in writing but it needs to be sufficiently clear what personal information is being requested.

Before responding to a subject access request, reasonable steps will be taken to verify the identity of the person making the request and whether they have the authority to request information on behalf of another individual. It is possible to ask for additional information to confirm identity and it is possible to ask to see identity documents such as a driving licence or passport that will verify the identity of the individual.

Once a data subject access request is received, the information requested must be provided without delay and at the latest within **one calendar month** of receiving the

request. If a data subject access request is complex (i.e. if a request is manifestly unfounded or excessive, or data is required from more than one source or the data subject has made numerous requests (whether current or not)), the response period can be extended by up to a further two months. The applicant will be informed if the response timeframe will be extended and the reasons why. It is expected that the school responds within the time period irrespective if school term breaks occur during the response period. The school will notify pupils and parents/those with parental responsibility that there is limited access to requests during the school term breaks, but will still deal with the requests within the response period.

There are limited timescales within which to respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the ICO and/or legal action by the affected individual.

In certain circumstances the school may be exempt from providing some or all of the personal data requested. Exemptions should only be applied on a case-by-case basis after careful consideration of all of the facts. The Schools Data Protection Officer will provide advice and guidance on what information can and cannot be shared.

The school will gather and collate all the personal data that has been requested. The school will need to gather all electronic and paper records that includes personal data within files, e-mails, CCTV, letters, reports and images.

No fee can be charged by the school for dealing with subject access requests. However, if a request is unfounded, excessive and has been submitted previously, the school has a right to charge a 'reasonable' administrative fee. The Schools Data Protection Officer can provide guidance on what is considered to be a 'reasonable fee'.

The Schools Data Protection Officer will provide figures regarding the number of subject access requests in the annual information governance assurance report to the school's governing body. Figures will also be included in the Schools Data Protection Officer's high level annual summary report on all schools that is presented to the Learning Service Senior Management Team and the Isle of Anglesey County Council Audit and Governance Committee.

The school will follow the *Schools Subject Access Request Policy* on how to deal with subject access requests that is available on Addysg Môn.

7.3. <u>The right to rectification</u>
Individuals have the right to have their personal data corrected if it is inaccurate or incomplete. The school will rectify the personal data as soon as possible and will do so within one calendar month of receiving the request to rectification. This can be extended by a further two months where the request to rectification is complex. A note should be made on relevant records if there is doubt regarding accuracy whilst dealing with the request.

It may be possible that the school may not be able to change or delete the personal information on every occasion, but anything that is factually incorrect should be corrected.

Where the school will not be taking any action in response to the request to rectification, the school will explain the reasons why to the individual and will inform them of their right to complain to the ICO. The school will also make a record of this.

7.4. The right to erase

Individuals have the right to request that any personal information held on them is deleted or removed if the data is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing. This right is also known as the right to be forgotten.

An erasure request can only be refused if an exemption applies, but it is likely an exemption will apply in the context of erasing school records. The school will consider every request on an individual basis. The school will respond to the request to erasure within one calendar month.

The school may refuse a request to erase personal data:

- where the school needs to comply with a legal obligation (to keep the data);
- for protecting an individual's vital interests or for tasks carried out in the public interest;
- when archiving in relation to public interest, scientific/historical research or statistical purposes;
- when the personal data is required for the exercise of legal claims;
- when the processing is necessary for exercising the right of freedom of expression and information.

The school will inform third parties that also process the personal data unless it involves a disproportionate effort to do so.

7.5. The right to restrict processing

Individuals are entitled to block the processing of their personal data in certain circumstances. The data may continue to be stored but processing of it must cease.

Individuals have the right to restrict the processing of their personal data where:

- the accuracy of the information is contested;
- the processing is unlawful (but they do not want the data to be erased, but restricted instead); or
- the school no longer needs the personal information but they require the data to establish, exercise or defend a legal claim.

Individuals also have the right to restrict the processing of personal information temporarily where:

- they do think it is accurate (and the school is verifying whether it is accurate);
- they have objected to the processing (and the school is considering whether the school's legitimate grounds override their interests).

The school will need to inform any third party that has received the data of the need to limit processing, and to inform the individual of the identity of these third parties. The school will inform individuals when the school decides to lift a restriction on processing.

7.6. The right to data portability

Individuals have the right to request that they receive a copy of their personal data in a structured format. Requests should be processed within one calendar month, provided there is no undue burden and it does not compromise the privacy of other individuals. Individuals can also request that their personal data is transferred directly to another system. No fee can be charged for this. The right to data portability only applies:

- to personal data an individual has provided to the school as the data controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

7.7. The right to object

Individuals have the right to object to their personal information being processed if the school is:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

The school will comply with the request unless there are strong, lawful reasons for processing or there is a need to establish, exercise or defend legal claims.

7.8. Rights in relation to automated decision making and profiling

Data Protection legislation allows:

- Automated individual decision-making- making a decision solely by automated means without any human involvement; and
- Profiling- automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process.

The school has a right to carry out automated decision making and profiling only if:

- the processing is necessary for entering into, or performance of, a contract;
- the processing has been authorised by member state law that includes measures to safeguard data subjects' rights; or
- the processing is based on explicit consent.

There are additional rules to protect individuals if automated decision making and profiling have legal effects or similarly significantly affects them. The school must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and to challenge it.

The school will not carry out automated decision making, including profiling, based on any individual's sensitive personal information.

7.9. Other rights
Additional to the rights above, individuals also have the right to:

- withdraw their consent to processing at any time;
- make a complaint to the ICO.

8. Children's Rights

Children have the same rights as adults over their personal information which they can exercise as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may usually exercise the child's data protection rights on their behalf.

In Wales there is no set age at which a child is generally considered to be competent to provide their own consent to processing. Competence is assessed depending upon the level of understanding of the child. If a child is competent then, just like an adult, they may authorise someone else to act on their behalf. This could be a parent/those with parental responsibility, another adult, or a representative such as a child advocacy service, charity or solicitor.

In the UK only children aged 13 or over are able provide their own consent for information society services (ISS). ISS generally includes websites, apps, search engines, online marketplaces and online content services such as on-demand music, gaming and video services and downloads.

9. Parent's Rights

A person with parental responsibility can exercise rights on behalf of a child if:

- the child authorises them to do so;
- when the child does not have sufficient understanding to exercise the rights him or herself; or
- when it is evident that this is in the best interests of the child.

A person with parental responsibility is someone who, according to the law in the child's country of residence, has the legal rights and responsibilities for a child that are normally afforded to parents. This will not always be a child's 'natural parents' and parental responsibility can be held by more than one natural or legal person.

The school must verify that the person giving consent does, in fact, hold parental responsibility for the child. The school is entitled to request relevant documentation to evidence this as well as the identity of the person making any requests on behalf of the child.

In addition, parents have their own independent right under *The Education (Pupil Information) (Wales) Regulations 2004* to access the official education records of their children who attend a maintained school. Parents can make requests in writing to the Headteacher. Pupils can also make a request for their own education record. A request for an educational record must receive a response from the school within 15 school days. The school may withhold information in certain circumstances, such as where serious harm may be caused to the pupil's physical or mental health or another individual, or where the request is for an exam script or for exam marks before they are officially announced. The school can charge an amount for information provided from an education record dependent upon the number of pages provided.

10. Conditions for Processing (Legal Basis)

10.1. Article 6

Personal data must be processed fairly and lawfully in accordance with the individual's rights. The school will only process personal information where at least one of the conditions of *Article 6 of GDPR* has been satisfied:

- 6(1)(a)- **individual's consent-** the individual has given clear consent for the school to process their personal data for a specific purpose;
- 6(1)(b)- **processing is necessary for a contract-** the processing is necessary for a contract with the individual, or because they have asked to take specific steps before entering into a contract;
- 6(1)(c)- **processing is necessary to comply with a legal duty-** the processing is necessary for the school to comply with the law (not including contractual obligations);
- 6(1)(d)- **processing is necessary for the individual's vital interests or another natural person-** the processing is necessary to protect someone's life;
- 6(1)(e)- **processing is necessary as it undertakes a task in the public interest or exercise of official authority-** the processing is necessary for the

school to perform a task in the public interest or for the school's official functions, and the task or function has a clear basis in law;

- 6(1)(f)- **processing is necessary for the purposes of legitimate interests of the data controller or third party-** the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests *(this does not apply to public authorities processing data to perform official tasks*).

The school will document its decision as to which lawful basis applies, to help demonstrate compliance with the data protection principles. The school will include information about both the purposes of the processing and the lawful basis for it in the school's Privacy Notice.

10.2. Article 9

The lawful basis for processing **special category data** requires that in addition to satisfying at least one of the conditions of *Article 6 of GDPR*, a condition in *Article 9 of GDPR* must also be satisfied *(please see section 11 for definitions of special category data).* The school will only process sensitive personal information if a condition in *Article 9* has been met:

- 9(2)(a)- **processing with the specific and explicit consent of the individual-** unless reliance on consent is prohibited by EU or Member State law;
- 9(2)(b)- **processing is necessary under employment law-** or social security or social protection law, or a collective agreement;
- 9(2)(c)- **processing is necessary to protect the individual's vital interests-** of a data subject who is physically or legally incapable of giving consent;
- 9(2)(d)- **processing for the use of a special category group (not-for-profit organisation with a political or religious aim or trade union);**
- 9(2)(e)- **processing relates to information made public by the individual;**
- 9(2)(f)- **processing is necessary so that the establishment can defend legal claims-** or where the courts are acting in their judicial capacity;
- 9(2)(g)- **processing is necessary for reasons of substantial public interests based on law-** which is proportionate to the aim pursued and which contains appropriate safeguarding measures- this means that Member States can extend the circumstances where sensitive data can be processed in the public interest;
- 9(2)(h)- **processing is necessary to respond to the needs of Occupational Health and Social Care-** necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union Member State law or a contract with a health professional;

- 9(2)(i)- **processing is necessary for Public Health reasons-** such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices;
- 9(2)(j)- **processing is necessary for archiving purposes in the public interest; or for scientific or historical research purposes; or for statistical purposes.**

Further special category conditions are included in *Schedule 1* of the *Data Protection Act 2018.*

The school will not process sensitive personal information until the individual has been properly informed (by way of a Privacy Notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Where criminal offence information is processed, the school will identify a lawful condition for processing that information and will document this.

The school will notify the Schools Data Protection Officer before processing any sensitive personal information, in order that the Schools Data Protection Officer may assess whether the processing complies with the criteria noted above.

11. Special Categories of Personal Data

Special categories of personal data is sometimes referred to as sensitive personal information or sensitive personal data. These are considered to be more sensitive and may only be processed in more limited circumstances.

The *GDPR* defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

Further to section 10.2, the school must determine the condition for processing special category data before beginning to process the information and will document the condition.

The school will not share any medical information regarding a pupil unless there is a legal basis in doing so. The school may put practices in place to share medical information with the consent of the pupil/parent/those with parental responsibility if it

is felt that there is a need to specifically share the information in order to protect the health and well-being of the particular pupil (e.g. a notice on a noticeboard in a restricted access staff room that contains personal and sensitive information of a pupil with a severe food allergy). In such circumstances, the school will seek advice from the Schools Data Protection Officer and the health and well-being risks posed, and the need to keep sensitive personal information safe, will have to be balanced against each other.

12. Consent

Consent may be used by the school as a legal basis for processing if it is the most appropriate legal basis to be used or if another lawful basis is not appropriate.

Consent must be a positive action, so individuals must always opt-in and take an affirmative action in providing their consent. The school will require consent to be provided for every separate processing activity.

The school will keep a record of consent via a register that lists everyone who has or has not provided consent and for which specific processing activity. The school will ensure that this is kept accurate and up-to-date and that there is a process in place for ensuring that the school complies with the consent decisions recorded.

Consent must be freely given, and it must be as easy to withdraw as it is to give. Individuals have the right to withdraw consent at any time and the school will up-date the record of consent to reflect any changes.

If the school has not received a consent form or no other positive action to provide consent has been provided, the school will take this as no consent being provided and will document and action this.

Consent forms are available on Addysg Môn.

13. Accuracy and Relevance

The school will ensure that any personal information that is processed is accurate, up-to-date, relevant, adequate and not excessive (proportionate) and is processed for the purpose for which it was obtained. Personal data obtained for one purpose will not be processed for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

The school will make it clear that individuals must take reasonable steps to ensure that personal data that the school holds about them is accurate and is up-dated as required. This is included in the school's Privacy Notice and the school will confirm at regular intervals that the information held is correct, in particular addresses and contact details. The school will up-date the information as soon as possible both in paper and in electronic records.

14. Retention of Personal Information

Personal information (and special category information) will be kept securely in accordance with the *Schools Retention Schedule* which is available on Addysg Môn.

Personal information (and special category information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend on the circumstances, including the reasons why the personal information was obtained. The school should follow the *Schools Retention Schedule* which sets out the relevant retention period for different types of personal information and documentation. Where there is any uncertainty, the school should consult with the Schools Data Protection Officer for guidance.

The school needs to ensure that personal information is not kept for longer than necessary but also that personal information is not disposed of before the end of the retention period.

15. Data Recording

The school will keep records in such a way that the individual concerned can inspect them. The information may also be inspected by the courts or any legal official at some point in the future. It should therefore be correct, unbiased, unambiguous and clearly decipherable/readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

16. Records of Processing Activities (ROPA)

The school will keep written records of processing activities, including:

- the name and details of the school; contact details of the Schools Data Protection Officer and any other joint data controllers if applicable;
- the purposes of the processing;
- a description of the categories of individuals and categories of personal data processed;
- categories of recipients of personal data;
- where possible, the retention schedules for the different categories of personal data;
- where possible, a general description of technical and organisational security measures.

The school will also, as part of the record of processing activities, document or provide a link to documentation on:

- information required for Privacy Notices;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessments (DPIAs);
- personal data breaches;

- special category data or criminal conviction and offence data.

If the school processes special category data or criminal conviction and offence data, written records will be kept of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- the lawful basis for processing; and
- whether the school retains and erases the personal information in accordance with the policy document and, if not, the reasons for not following the policy.

The school will conduct regular reviews of the personal information that is processed and up-date documentation accordingly. This may include:

- carrying out information audits to find out what personal information the school holds;
- creating data map flows for different information processes;
- distributing questionnaires and talking to all staff within the school to get a complete picture of the school's processing activities; and
- reviewing policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

The school will document processing activities in electronic format so that information can be added, removed and amended easily so that the record of processing activities is kept accurate and up-to-date.

A template for *Records of Processing Activities* and accompanying guidance is available on Addysg Môn.

The school will comply with the *Schools Records Management Policy.*

17. Disclosure and Sharing of Information

Data protection law does not prevent, and is not a barrier, to sharing information but rather provides a framework to ensure that personal information is shared lawfully and in an appropriate and safe way. However, it is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- other staff members on a *need* to know basis;
- relevant parents/those with parental responsibility;
- other organisations if it is necessary in the public interest e.g. prevention of crime;
- other authorities such as the Local Education Authority and schools to which a pupil may move, where there are legal requirements;

- organisations that collaborate with the school (such as Social Services *(please see section 17.2)*) or that are part of an Information Sharing Protocol (ISP).

When sharing personal information, the school will ensure that:

- it is allowed to share the personal information;
- the information is shared only with the people who *need* to have it;
- adequate security (taking in to account the nature of the information) is in place to protect the information and to ensure that it is shared safely;
- it will provide an outline in a Privacy Notice of who receives personal information from the school;
- the information is accurate and up-to-date;
- the information is shared in a timely fashion.

Individual staff members will only access information that they have the authority to access, and only for authorised purposes and will only allow other school staff to access personal information if they have the appropriate authorisation.

Decisions on whether to share information must be taken on a case-by-case basis. The school will base its decisions around sharing information on considerations of the safety and well-being of the individual and others who may be affected. The school will not disclose anything on a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else.

Personal information should not be disclosed without establishing the identity of the recipient. Information should not be provided to other parties, even if they are related (e.g. in the case of divorced parents, it is important that information regarding one party is not given to the other party who which he/she is not entitled). The school will keep a record of the decision to share information or not and will explain the reasons behind the decision. If the school has shared information, a record will be kept on what personal information has been shared, with whom it has been shared and for what purpose.

Any personal data passed to a third party for processing (namely an external company) will be covered by a Data Processing Agreement (DPA). A Data Processing Agreement is needed when the school as the Data Controller asks a Data Processor to process data on behalf of the school.

The school will sign up to the Wales Accord on the Sharing of Personal Information (WASPI). This is a tool to help share personal information effectively and lawfully on a multi-agency basis within Wales.

If the school regularly shares information with an agency or organisation, there may be a need for an Information Sharing Protocol (ISP) or a Data Disclosure Agreement (DDA) depending on the type of information sharing.

The school may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any pupils or staff members.

The school should contact the Schools Data Protection Officer for advice if the school is in any doubt if personal information should be shared or not with agencies and third parties requesting information.

17.1. Request from Third Parties for an Individual's Personal Information
The school may receive requests from other agencies or third parties such as the Police, DWP, solicitors etc. to physically access or receive a copy of the personal information relating to an individual.

The school will share personal data with law enforcement and government bodies where it is legally required to do so, including for:

- the prevention or detection of crime and/or fraud;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax owed to HMRC;
- in connection with legal proceedings;
- where the disclosure is required to satisfy safeguarding obligations;
- research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

The school will follow the *Procedure for Sharing Information with Police Authorities in the United Kingdom* when dealing with requests from the Police.

17.2. Protection of Children and Vulnerable Adults
The *GDPR* and *Data Protection Act 2018* do not prevent, or limit, the sharing of information for the purposes of keeping children and young people safe.

Relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being. The most important consideration is whether sharing information is likely to support the safeguarding and protection of a child.

Fears about sharing information should not be a barrier to safeguarding and promoting the well-being of children at risk of abuse or neglect.

The school will need to follow safeguarding policies and procedures without delay regarding what personal information can be shared with the relevant authorities such as Children & Families Services, Adult Services or the Police if there are any concerns that a child or vulnerable adult may be at risk of serious or significant harm.

In some circumstances, the duty of protecting the confidentiality of personal information must be overridden, when there is a duty to protect children or vulnerable adults who are at risk of serious harm. In such circumstances, the school will seek

advice from the Schools Data Protection Officer. The risk posed and the individual's right to privacy will have to be balanced against each other.

If unsure of what information can be shared, please discuss with the Schools Data Protection Officer.

For more information regarding sharing information to safeguard children, please refer to the *Welsh Government's document- Social Services and Well-being (Wales) Act 2014, Working Together to Safeguard People, Information sharing to safeguard children, Non-statutory guide for practitioners,* July 2019 which is available on Addysg Môn.

18. Data Breaches

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. This means that personal information has been compromised, damaged, lost or stolen.

A data breach can take many different forms, examples include:

- 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.

The school will contact the Schools Data Protection Officer to report **all** data breach incidents/'near misses' **as soon as possible**. The school will investigate any such breaches and will complete the required report of a data breach without undue delay.

A data breach report template for schools and accompanying guidance is available on Addysg Môn.

The school will need to take any necessary measures to address and mitigate the data breach and will take any remedial steps if necessary. 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 school will also review if it needs to undertake any required changes to current processes and/or practices to reduce the risk of the likelihood of a similar incident taking place again.

The school must keep a central record of all data breaches that will register all compliance failures. Figures regarding the number of data breaches will be included in the annual information governance assurance report to the school's governing body. Figures will also be included in the Schools Data Protection Officer's high level annual summary report on all schools that is presented to the Learning Service Senior Management Team and the Isle of Anglesey County Council Audit and Governance Committee.

If the data breach is likely to result in a risk to the rights and freedoms of individuals, the school is required to report the data breach to the ICO, **within 72 hours** of becoming aware of the data breach. **It is the Schools Data Protection Officer who makes the decision whether or not the breach needs to be reported to the ICO**. The school will also 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.

The school will comply with the *Schools Data Breach Policy*.

All staff need to be open about any incidents 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 an incident that should have been reported to the ICO, may have consequences for the school and for the individual member of staff.

19. Sharing Data Protection Concerns

Staff within the school should inform the Headteacher/person who is responsible for data protection within the school, and if appropriate, the Schools Data Protection Officer, if they have any concerns or suspects that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the legal conditions in *Article 9* being met;
- access to personal information without the proper authorisation;
- personal information not kept or deleted/destroyed securely;
- removal of personal information, or devices containing personal information (or which can be used to access it), from the school's premises without appropriate security measures being in place;

- any other breach of this policy or of any of the data protection principles set out in section 6.

20. Information Asset Register

The Headteacher will need to ensure that an *Information Asset Register* is in place and that it is reviewed on a regular basis. The information asset register contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

An *Information Asset Register* template is available on Addysg Môn.

21. Privacy Notice

The school has a Privacy Notice in place that informs individuals about the personal information that is collected and is held about them and how they can expect their personal information to be used and for what purposes. The Privacy Notice must be specific to the activity which requires personal information. This must happen at the time that the information first starts to be gathered on an individual.

Whenever information is collected about individuals, the school will provide the following information so that the school is transparent and provides accessible information about how personal data is used:

- the identity and contact details of the school as the data controller;
- the purpose that the information is being collected for;
- the lawful basis for collecting the information;
- any other purposes that it may be used for;
- how the information is collected;
- with who the information will or may be shared with (any third parties);
- how long the information is kept;
- details about the rights of individuals (e.g. the rights of access to personal data that is being held by the school);
- details about the Schools Data Protection Officer.

Appropriate measures are taken to provide information in the Privacy Notice in a concise, transparent, intelligible and easily accessible form, using clear and plain language. If information is directly collected from a child, the Privacy Notice must be age appropriate.

The Privacy Notice will be shared via the school website; social media accounts, and will be made available in hard copy upon request.

A summary of the Privacy Notice will be included within all documents that collect personal information and within consent forms.

A Privacy Notice template for parents and pupils and also for the school workforce, are available on Addysg Môn.

22. Data Protection Impact Assessments (DPIAs)

Where processing is likely to result in a high risk to an individual's rights and freedoms (e.g. where the school is planning to use a new form of technology), before commencing the processing, a DPIA will be performed to assess the following:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals;
- what measures can be put in place to address those risks and protect personal information.

Before any new form of technology is introduced, the school should therefore contact the Schools Data Protection Officer in order that a DPIA can be undertaken.

During the course of any DPIA, the school will seek the views of any representative group and any other relevant stakeholders (where applicable).

DPIAs are a legal requirement for processing activities that are likely to be high risk. A DPIA should be considered as an on-going process with regular reviews based on the level of risk and the nature of the processing activity.

A *Schools Data Protection Impact Assessment (DPIA) Policy* and template as well as a *Schools Data Protection Risk Matrix* and a *Schools Data Protection Risk Register* template are available on Addysg Môn.

23. Information Security

23.1. School
The school will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The school will ensure:

- that where possible, personal information is pseudonymised or encrypted;
- the on-going confidentiality, integrity, availability and resilience of processing systems and services;
- that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner;
- that a process is in place for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

- that there are appropriate secure spaces available within the school to hold private conversations between staff, pupils, parents/those with parental responsibility and visitors e.g. reception areas that are suitable to share personal information with only those who need to be involved in the conversation without the risk of others overhearing;
- that all personal and special categories data stored on the school's IT systems must be identified using data classification terms (OFFICIAL or OFFICAL-SENSITIVE).

The school will comply with the *Schools Information Security Policy.*

23.2. External Organisations

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts and agreements with those organisations to safeguard the security of personal information. Contracts and agreements with external organisations must provide that:

- the organisation may act only on the written instructions of the school;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the school and under a written contract;
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will assist the school in meeting its obligations in relation to the security of processing, the notification of data breaches and Data Protection Impact Assessments (DPIAs);
- the organisation will delete or return all personal information to the school as requested at the end of the contract; and
- the organisation will submit to audits and inspections; provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or existing agreement is altered, the school must seek approval of its terms by the Schools Data Protection Officer. The Schools Data Protection Officer will ensure that there are clearly defined agreements in place between the school and the organisation to ensure that data is suitably protected and provides clarity on roles and responsibilities.

24. Secure Storage of Personal Information

Personal information must be stored in a secure location with access only available to authorised persons who need access to that particular personal information. All

personal information must be protected and kept secure in order to prevent loss, misuse or damage.

24.1. Paper Records

Personal information should always be kept locked away. Any drawers, cupboards, cabinets, storage rooms or storage containers should be robust and locked when not in use. Documents containing personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access.

Particular care should be taken if documents have to be taken out of the school building. Documents including personal information should not be removed from the school's premises unless appropriate security measures are in place to secure the information.

Documents should be kept in a safe and accessible location that is protected from flooding, dampness and other elements. Some documents may need to be kept in airtight containers to protect them from environmental damage.

Blinds on ground floor windows should be closed at the end of the day.

24.2. Electronic Records

If personal information is kept electronically, appropriate technical security measures need to be in place on all devices such as pseudonymisation, encryption or password protection.

All electronic devices that contain personal information need to be password protected with access only provided to authorised persons.

Strong passwords need to be in place which contain at least nine characters; contain symbols; a mix of upper and lower case characters and a mix of numbers and letters. Different passwords should be used for separate systems and devices. Passwords and login details should not be written down and should not be shared with anyone else.

All computer and laptop screens will automatically lock after a certain period and staff will also physically lock their screens if leaving their desks for a period of time. Data will be regularly backed up in line with backup procedures.

All portable electronic devices should be kept as securely as possible. If they contain personal information, they should be kept under lock and key when not in use.

Encryption software should be used to protect all portable devices and removable media, such as USB devices (memory sticks or another form of memory storage not part of the computer itself) which hold personal information. Staff members should not remove devices containing personal information (or which can be used to access

it), from the school's premises unless appropriate security measures are in place to secure information and the device.

The use of removable media devices is not encouraged when there are alternative technologies available that do not require physically transferring data between locations. The school will move away from using these kinds of devices for storing personal information wherever possible.

Staff members will not use personal devices or drives (such as mobile phones) to store or share personal information relating to school and work business.

25. Secure Disposal of Personal Information

Personal information (and special category information) that is no longer required according to the *Schools Retention Schedule* will be deleted permanently from the school's information systems and any hard copies of personal information will be destroyed in a secure manner.

Personal information can be destroyed securely by using a cross-cutting shredder or via secure waste disposal arrangements. The school may use an appropriate third party to safely dispose of records on the school's behalf. If this is the case, the school will require the third party to provide sufficient guarantees that it complies with data protection law (e.g. Certificate of Destruction).

Personal data will not be left in an insecure location whilst in the process of being destroyed safely. Personal information shall not be disregarded via general waste, recycling or via a skip. A secure method **must** be used in all instances where there is personal data.

26. Annual Data Protection Fee

Schools, like every organisation or sole trader who processes personal information, are required under the *Data Protection (Charges and Information) Regulations 2018*, to pay an annual data protection fee to the ICO, unless they are exempt. **All schools are required to pay the annual data protection fee.** Failure to do so will result in a fixed penalty**.** The school will register as a public body.

Registration details are added to the data protection public register that can be viewed on the ICO website. The school has a unique registration number. Contact details for the Schools Data Protection Officer is included against the school's registration details.

27. Photographs and Images

As part of school activities, photographs and images will be taken of individuals within the school. Photographs and images taken for official school use that may be used for communication, marketing and promotional materials will be covered under

GDPR and *Data Protection Act 2018* and the school will need to inform pupils why they are being taken and what they will be used for.

A consent form is available on Addysg Môn that is to be used in order to obtain consent by pupils/parents/those with parental responsibility regarding where the photographs and images will be published. Consent will be provided on different elements of where photographs and images can be shared and used such as on the school website, social media accounts, newspapers, brochures, newsletters and apps.

Consent can be refused or withdrawn at any time. If consent is withdrawn, the school will delete the photograph or video and not distribute it further.

28. Website and Social Media

The school will obtain written consent for sharing personal information regarding pupils on its website and social media accounts, including photographs and images. Pupils, parents/those with parental responsibility will be informed about the consequences of personal data being disseminated worldwide.

A consent form is available on Addysg Môn that is to be used in order to obtain consent by pupils/parents/those with parental responsibility regarding what information, photographs and images will be published on any websites and social media accounts.

Consent can be refused or withdrawn at any time. If consent is withdrawn, the school will take every reasonable steps to delete/remove the information/photograph/image from the website and/or social media accounts to stop further distribution. However, it must be recognised as the personal data is on a website and/or social media accounts, the information may already have been viewed and shared beyond the school's control.

29. E-mail

School staff will only use an authorised e-mail account to communicate in respect of school business. School staff will not use their personal e-mail account to communicate with pupils and to share personal data.

If documents that contain personal information have to be shared via e-mail, the document will be password protected with the password separately and securely shared with the intended recipient.

School e-mail accounts will also be subject to the data protection regulations and the *Schools Retention Schedule* must be followed regarding personal information contained within e-mails. The school will comply with the *Schools Staff E-mail Policy.*

30. CCTV (if relevant)

Capturing and/or recording images of identifiable individuals is an example of processing personal information and therefore needs to comply with *GDPR* and the *Data Protection Act 2018*. The school must also have a *CCTV Policy* in place. A *Schools CCTV System Policy* is available on Addysg Môn.

Data Protection Impact Assessment (DPIA) needs to be completed when using CCTV or considering purchasing a surveillance system. The Schools Data Protection Officer will provide guidance and support with completing these.

The school must notify staff, pupils and visitors why it is collecting personal information in the form of CCTV images. A sign notifying this must be in place within all zones that are being filmed. Using prominently placed signs at the entrance to the school and then using further signs inside the zones will let people know when they are in an area where a surveillance system is in operation.

The school will ensure that it has a set retention period based on the possible need to review the footage and will consider who is allowed access to this footage and why.

Individuals and law enforcement agencies will have the right to request access to the images. All such requests will be logged.

The school will follow *'In the picture: A data protection code of practice for surveillance cameras and personal information'*.

31. Biometric Information (if relevant)

This type of information is considered as special category data. All such data must be handled appropriately and in accordance with the *GDPR* and the *Data Protection Act 2018 principles*.

Examples of biometric identification systems include fingerprinting and facial recognition systems (e.g. students using fingerprints to receive school dinners instead of paying with cash).

The school will obtain the written consent of pupils/parents/those with parental responsibility before recording and processing the pupil's biometric details. The consent form is available on Addysg Môn.

Pupils/parents/those with parental responsibility can object to participation in the school's biometric recognition systems, or withdraw consent at any time, and the school will make sure that any relevant data already captured is deleted. Alternative methods of service provision must be identified if a parent/those with parental responsibility or pupil does not provide consent.

32. International Data Transfers

No personal or special category data may be transferred outside of the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway. This can be discussed further with the Schools Data Protection Officer if needed.

33. Training

The Headteacher and the Schools Data Protection Officer will ensure that staff are adequately trained regarding their data protection responsibilities. Headteachers, school governors and individuals whose roles require regular access to personal information, or who are responsible for implementing this policy, will receive additional training to help them understand their duties and how to comply with them. All school staff will need to ensure that they have completed the mandatory *GDPR* e-learning module training.

The Headteacher will keep a record of attendance and a register of who has completed any data protection training and when they have completed it.

34. Breach of the Policy

Non-compliance with this policy by members of school staff could lead to serious consequences.

This can lead to putting both the individuals whose personal information is being processed and the school at risk.

There is a risk of significant civil and criminal sanctions for the individual and the school authorities taken by third parties. An individual can commit a criminal offence under the *GDPR*, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the school.

Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could result in dismissal for gross misconduct.

If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

35. Review of Policy and Oversight Arrangements

This policy will be reviewed by the Schools Data Protection Officer on an annual basis. The policy will be approved by the Learning Service 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 protection can be obtained from the ICO website: https://ico.org.uk/

ATODIAD A / APPENDIX A

Rhestr Termau, Diffiniadau a Deddfwriaeth Diogelu Data Ysgolion Dwyieithog

Schools Data Protection Bilingual Glossary, Definitions and Legislation

Diffiniad	**Geiriau a Termau / *Words and Terms***	***Definition***
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 personol** ***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.*
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.	**Data categori arbennig** ***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.*
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.	**Prosesu gwybodaeth** ***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.*
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.	**Rheolydd data** ***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.
Yn cynnwys gweithwyr sydd â'u gwaith yn ymwneud â data personol. Mae gan ddefnyddwyr data ddyletswydd i ddiogelu'r wybodaeth y maent yn ymdrin â hi drwy ddilyn polisïau diogelu data a diogelwch bob amser. Mae staff a gyflogir gan ysgolion yn ddefnyddwyr data.	**Defnyddwyr data** ***Data users***	*Includes employees whose work involves using personal data. Data users have a duty to protect the information they handle by following data protection and security policies at all times. Staff employed within schools are data users.*
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.	**Proseswyr data** ***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.*
Yr unigolyn y mae'r wybodaeth bersonol yn ymwneud ag ef neu hi.	**Gwrthrych y data** ***Data subject***	*The individual to whom the personal information relates.*
Mae DPO yn helpu i fonitro cydymffurfiaeth fewnol, hysbysu a chynghori ar rwymedigaethau diogelu data, rhoi cyngor ynghylch Asesiadau Effaith Diogelu Data (DPIAau) a gweithredu fel pwynt cyswllt ar gyfer gwrthrychau data a'r awdurdod goruchwylio.	**Swyddog Diogelu Data** ***Data Protection Officer***	*A DPO assists to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.*
Toriad diogelwch sy'n arwain at ddinistrio, colli, addasu, datgelu neu fynediad anawdurdodedig at ddata personol a drosglwyddir, a storir neu a brosesir mewn unrhyw ddull arall, yn ddamweiniol neu'n anghyfreithlon.	**Digwyddiad Diogelwch Data** ***Data breach***	*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 information.*
Gan y gwrthrych data yn golygu unrhyw arwydd rhydd, penodol, gwybodus a diamwys o ddymuniadau gwrthrych y data y mae ef neu hi, drwy ddatganiad neu	**Caniatâd** ***Consent***	*Of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or*

drwy gam cadarnhaol clir, yn arwydd o gytundeb i brosesu data personol sy'n ymwneud ag ef neu hi. Mae'r baich o ddangos caniatâd ar y rheolydd data.		*by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The burden of demonstrating consent is on the data controller.*
Gwybodaeth bersonol yn ymwneud ag euogfarnau, troseddau, honiadau, achosion troseddol, a mesurau diogelwch cysylltiedig.	**Gwybodaeth am gofnodion troseddol** ***Criminal records information***	*Personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.*
Data personol sy'n gysylltiedig ag iechyd corfforol neu feddyliol person naturiol, gan gynnwys darpariaeth gwasanaethau gofal iechyd, sy'n datgelu gwybodaeth am statws iechyd ef neu hi.	**Data ynghylch iechyd** ***Data concerning health***	*Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.*
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.	**Ffugenwau** ***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.*
Cael gwared â gwybodaeth a ellir ei defnyddio i adnabod rhywun oddi ar rywbeth (megis data cyfrifiadur) fel na ellir gwybod beth oedd y ffynhonnell wreiddiol na'i hadnabod.	**Gwybodaeth Dienw** ***Anonymised***	*To remove identifying information from something (such as computer data) so that the original source cannot be known or identified.*
Data personol sy'n ymwneud â nodweddion genetig person a etifeddwyd neu a gaffaelwyd sy'n rhoi gwybodaeth unigryw am ffisioleg neu iechyd y person naturiol hwnnw ac sy'n deillio, yn benodol, o ddadansoddiad	**Data genetig** ***Genetic data***	*Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a*

o sampl biolegol gan y person naturiol dan sylw.		*biological sample from the natural person in question*.
Data personol sy'n deillio o brosesu technegol penodol sy'n ymwneud â nodweddion corfforol, ffisiolegol neu ymddygiadol person naturiol, sy'n caniatáu neu'n cadarnhau adnabyddiaeth unigryw'r person naturiol hwnnw, megis delweddau wyneb neu ddata dactyloscopig. Mae cydnabyddiaeth ôl bys yn enghraifft o ddata dactyloscopig.	**Data biometrig** ***Biometric data***	*Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. Fingerprint recognition is an example of dactyloscopic data.*
Negeseuon a ddosberthir drwy ddulliau electronig gan un defnyddiwr cyfrifiadur i un neu fwy o dderbynwyr drwy rwydwaith. Yn ogystal â chynnwys testunol, mae e-bost yn caniatáu i'r anfonwr anfon ffotograffau, fideo neu glipiau sain ar ffurf neu ffeiliau digidol.	**E-bost** ***E-mail***	*Messages distributed by electronic means from one computer user to one or more recipients via a network. In addition to textual content, e-mail allows the sender to send photographs, video or sound clips in digital form or files.*
Y gyrchfan y cyflwynir negeseuon post electronig iddi. Mae'n cyfateb i flwch llythyrau yn y system bost.	**Blwch Post** ***Mailbox***	*The destination to which electronic mail messages are delivered. It is the equivalent of a letter box in the postal system.*
Meddalwedd sydd wedi'i gynllunio'n benodol i darfu, difrodi neu gael mynediad heb awdurdod i system gyfrifiadurol.	**Drwgwedd** ***Malware***	*Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.*
Term rhithwir ar gyfer mentro neu anfon negeseuon ymfflamychol mewn e-bost.	**Fflamio** ***Flaming***	*A virtual term for venting or sending inflammatory messages in an e-mail.*
Negeseuon amherthnasol neu ddigymell a anfonir dros y rhyngrwyd/e-bost, fel arfer at nifer fawr o ddefnyddwyr, at ddibenion hysbysebu, *'phishing'*, lledaenu drwgwedd, ac ati.	**Sbam** ***Spam***	*Irrelevant or unsolicited messages sent over the internet/e-mail, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.*
Monitro symudiadau ac ymddygiad unigolion; gall hyn gynnwys fideo, sain neu ffilm fyw. At ddibenion y polisi	**Gwyliadwraeth** ***Surveillance***	*Monitoring the movements and behaviour of individuals; this can include video, audio or live footage.*

hwn, dim ond fideos fydd yn berthnasol.		*For the purpose of this policy, only video footage will be applicable.*
Unrhyw ddefnydd o wyliadwriaeth nad yw ei hawdurdod yn dod o dan *Ddeddf Rheoleiddio Pwerau Ymchwilio 2000.*	**Gwyliadwraeth Agored** ***Overt surveillance***	*Any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.*
Unrhyw ddefnydd o wyliadwriaeth nad yw'n cael ei rannu'n fwriadol â'r gwrthrychau y mae'n eu recordio. Ni fydd gwrthrychau'n cael gwybod am wyliadwriaeth o'r fath.	**Gwyliadwraeth Cudd** ***Covert surveillance***	*Any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.*
Cyfrifiaduron prosesu gwybodaeth neu systemau cyfathrebu data.	**Systemau Gwybodaeth** ***Information Systems***	*Information processing computers or data communication systems.*
Cadw'r wybodaeth yn gyflawn, yn gywir ac yn ddilys.	**Cywirdeb** ***Integrity***	*The preservation of the complete, accurate and validated state of information.*
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.	**Risg** ***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.*
Adnabyddiad a dadansoddiad o risgiau i amcanion busnes y sefydliad.	**Asesiad Risg** ***Risk Assessment***	*The identification and analysis of risks to the organisation's business objectives.*
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.	**Effaith** ***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.*
Pa mor debygol yw'r risg o ddigwydd – ansicrwydd, siawns a thebygolrwydd.	**Tebygolrwydd** ***Likelihood***	*How likely is it that the risk will occur- uncertainty, chance and probability.*
Mesur sy'n addasu risg.	**Rheolaeth** ***Control***	*Measure that is modifying risk.*
Achos potensial o ddigwyddiad dieisiau, y gall	**Bygythiad**	*Potential cause of an unwanted incident, which*

arwain at niwed i system neu sefydliad.	***Threat***	*can result in harm to a system or organisation.*
Heb hawl cyfreithlon.	**Anawdurdodedig** ***Unauthorised***	*Without a legitimate right.*
Trydydd parti yw rhywun nad yw'n rheolwr data, yn brosesydd data nac yn wrthrych i'r data.	**Gwybodaeth Trydydd Parti** ***Third-party information***	*A third party is somebody who is not the data controller, the data processor or the data subject.*
Mae storio cwmwl yn fodel cyfrifiadura cwmwl lle caiff data ei storio ar weinyddion o bell a gyrchir o'r rhyngrwyd, neu "gwmwl". Mae'n cael ei gynnal, ei weithredu a'i reoli gan ddarparwr gwasanaeth storio cwmwl ar weinyddion storio sy'n cael eu hadeiladu ar dechnegau rhithiol.	**Storio cwmwl** ***Cloud storage***	*Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the internet, or "cloud." It is maintained, operated and managed by a cloud storage service provider on storage servers that are built on virtualisation techniques.*
Mae'r gair "ap" yn dalfyriad ar gyfer *"application"* yn y Saesneg. Mae'n ddarn o feddalwedd sy'n gallu rhedeg drwy borwr gwe neu all-lein ar gyfrifiadur, ac ar ffôn clyfar, tabled neu ddyfeisiau electronig eraill.	**Ap** ***App***	*The word "app" is an abbreviation for "application." It is a piece of software that can run through a web browser or offline on a computer, and on a smartphone phone, tablet or other electronic devices.*
Unrhyw blatfform ar-lein sy'n cynnig rhyngweithio amser real rhwng y defnyddiwr ac unigolion neu grwpiau eraill. Mae enghreifftiau'n cynnwys, ond heb fod yn gyfyngedig i lwyfannau cyfathrebu, fforymau trafod ar-lein, blogiau, mannau cydweithredol, gwasanaethau rhannu cyfryngau, apiau micro-flogio a defnyddio gwe-gamerâu.	**Cyfryngau cymdeithasol** ***Social media***	*Any online platform that offers real-time interaction between the user and other individuals or groups. Examples include, but are not limited to communication platforms, online discussion forums, blogs, collaborative spaces, media sharing services, micro-blogging applications and the use of webcams.*
Unrhyw ddefnydd o gyfryngau cymdeithasol neu dechnoleg cyfathrebu i fwlio unigolyn neu grŵp.	**Bwlio seibr** ***Cyber bullying***	*Any use of social media or communication technology to bully an individual or group.*

Disgrifiad	**Termau a Dogfennau / *Terms and Documents***	***Description***
Mae'r Rhestr o Asedau Gwybodaeth yn cynnwys gwybodaeth am ba ddata a gedwir, lle caiff ei storio, sut y caiff ei ddefnyddio, pwy sy'n gyfrifol ac unrhyw reoliadau neu amserlenni cadw pellach a allai fod yn berthnasol.	**Rhestr o Asedau Gwybodaeth** ***Information Asset Register***	*The information asset register contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.*
Mae angen i'r ROPA gynnwys yr holl ofynion perthnasol a nodir yn Erthygl 30 o'r GDPR. Mae'r ROPA yn rhestru pob gweithgaredd prosesu unigol; yn disgrifio union ddefnydd y data; y mesurau technegol a threfniadol sydd ar waith i ddiogelu'r data; pwy a effeithir gan y prosesu; dadansoddi risg a phroseswyr data posibl.	**Cofnodion o Weithgareddau Prosesu (ROPA)** ***Records of Processing Activities (ROPA)***	*The ROPA needs to contain all the relevant requirements set out in Article 30 of the GDPR. The ROPA lists every single processing activity; describes the exact usage of the data; the technical and organisational measures that are in place for the protection of the data; who is affected by the processing; risk analysis and possible data processors.*
Mae Hysbysiad Preifatrwydd yn rhoi gwybod i unigolion am yr wybodaeth bersonol sy'n cael ei chasglu ac sy'n cael ei chadw amdanynt a sut y gallent ddisgwyl i'w gwybodaeth bersonol gael ei defnyddio ac at ba ddibenion. Rhaid i'r Hysbysiad Preifatrwydd fod yn benodol i'r gweithgaredd sy'n gofyn am wybodaeth bersonol.	**Hysbysiad Preifatrwydd** ***Privacy Notice***	*A Privacy Notice informs individuals about the personal information that is collected and is held about them and how they can expect their personal information to be used and for what purposes. The Privacy Notice must be specific to the activity which requires personal information.*
Mae DPIA yn ofyniad cyfreithiol ar gyfer prosesu gweithgareddau sy'n debygol o fod yn risg uchel. Bydd DPIA yn cael ei wneud cyn dechrau'r prosesu, lle mae prosesu'n debygol o arwain at risg uchel i hawliau a rhyddid unigolyn (e.e. lle mae'r ysgol yn bwriadu	**Asesiadau Effaith Diogelu Data (DPIAau)** ***Data Protection Impact Assessments (DPIA)***	*DPIAs are a legal requirement for processing activities that are likely to be high risk. A DPIA is performed before commencing the processing, where processing is likely to result in a high risk to an individual's rights and freedoms (e.g. where the*

defnyddio math newydd o dechnoleg).		*school is planning to use a new form of technology).*
Mae cytundeb prosesu data yn gontract cyfreithiol rwymol sy'n nodi hawliau a rhwymedigaethau pob parti (rheolwr data a phrosesydd data) sy'n ymwneud â diogelu data personol. Mae angen cytundeb prosesu data ar y rheolwr data gydag unrhyw bartïon sy'n gweithredu fel proseswyr data ar eu rhan.	**Cytundeb Prosesu Data (DPA)** ***Data Processing Agreement (DPA)***	*A data processing agreement is a legally binding contract that states the rights and obligations of each party (data controller and data processor) concerning the protection of personal data. The data controller needs a data processing agreement with any parties that act as data processors on their behalf.*
Mae'r WASPI yn ffordd i sefydliadau sy'n ymwneud yn uniongyrchol ag iechyd, addysg, diogelwch, atal troseddu a lles cymdeithasol pobl yng Nghymru, rannu gwybodaeth bersonol yn effeithiol ac yn gyfreithlon.	**Cytundeb Rhannu Gwybodaeth Bersonol Cymru (WASPI)** ***Wales Accord on the Sharing of Personal Information (WASPI)***	*WASPI is a tool to help share personal information effectively and lawfully between organisations directly concerned with the health, education, safety, crime prevention and social well-being of people in Wales.*
Mae ISP yn cynorthwyo rhannu gwybodaeth bersonol yn rheolaidd a chyfartal rhwng rheolyddion data am reswm penodedig.	**Protocol Rhannu Gwybodaeth (ISP)** ***Information Sharing Protocol (ISP)***	*ISPs support, regular and reciprocal sharing of personal information between data controllers for a specified purpose.*
Mae DDA yn cynorthwyo datgelu gwybodaeth un ffordd o un rheolydd data i un neu fwy o reolyddion data am reswm penodedig.	**Gytundeb Datgelu Data (DDA)** ***Data Disclosure Agreement (DDA)***	*DDAs support one way disclosures of information from a data controller to one or more data controllers.*
Dogfen sydd yn darparu digon o sicrwydd fod trydydd parti yn cydymffurfio â chyfraith diogelu data pan yn dinistrio cofnodion ar ran yr ysgol.	**Tystysgrif Dinistr** ***Certificate of Destruction***	*A document that provides sufficient guarantees that a third party complies with data protection law when disposing of records on behalf of the school.*

Disgrifiad	**Sefydliad / *Organisation***	***Description***
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. Ffôn: 0303 123 1113 Cyfeiriad: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Mae cyngor ac arweiniad ar gael drwy eu gwefan: www.ico.org.uk **Swyddfa ICO Cymru** Ffôn: 0330 414 6421 E-bost: wales@ico.org.uk Cyfeiriad: Swyddfa'r Comisiynydd Gwybodaeth – Cymru Yr Ail Lawr, Tŷ Churchill, Ffordd Churchill, Caerdydd, CF10 2HH	**Swyddfa'r Comisiynydd Gwybodaeth (ICO)** ***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.* *Telephone: 0303 123 1113* *Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF* *Advice and guidance is available via their website www.ico.org.uk* ***ICO Wales Office*** *Telephone: 0330 414 6421* *E-mail: wales@ico.org.uk* *Address: Information Commissioner's Office – Wales, 2nd Floor, Churchill House, Churchill Way, Cardiff, CF10 2HH*

Deddfwriaeth, Deddfau a Chanllawiau	***Laws, Acts and Guidance***
Rheoliad Diogelu Data Cyffredinol (GDPR)	*The General Data Protection Regulation (GDPR)*
Deddf Diogelu Data 2018	*Data Protection Act 2018*
Surveillance Camera Commissioner's Code of Practice	*Surveillance Camera Commissioner's Code of Practice*
Information Commissioner's Office (ICO) 'Subject access code of practice: Dealing with requests from individuals for personal information'	*Information Commissioner's Office (ICO) 'Subject access code of practice: Dealing with requests from individuals for personal information'*
Right of access: detailed guidance	*Right of access: detailed guidance*
Deddf Rhyddid Gwybodaeth 2000	*Freedom of Information Act 2000*
Rheoliadau Addysg (Gwybodaeth am Ddisgyblion) (Cymru) 2004	*The Education (Pupil Information) (Wales) Regulations 2004*
Llywodraeth Cymru - Deddf Gwasanaethau Cymdeithasol a Llesiant (Cymru) 2014, Gweithio Gyda'n Gilydd i Ddiogelu Pobl, Rhannu gwybodaeth i ddiogelu plant, Canllaw anstatudol i ymarferwyr, Gorffennaf 2019	*Welsh Government- Social Services and Well-being (Wales) Act 2014, Working Together to Safeguard People, Information sharing to safeguard children, Non-statutory guide for practitioners, July 2019*
Reoliadau Diogelu Data (Ffioedd a Gwybodaeth) 2018	*Data Protection (Charges and Information) Regulations 2018*