Ysgol Cybi

Polisi Prosesu Data Ysgolion / *Schools Data Processing Policy*

(Fersiwn 1, Hydref 2021 / *Version 1, October 2021*)

Ynglŷn â'r polisi hwn

Mae'r polisi hwn yn amlinellu'r hyn y mae angen i'r ysgol ei wneud i sicrhau ei bod yn deall y berthynas â phroseswyr data a bod y cytundebau angenrheidiol ar waith gydag unrhyw broseswyr data y mae'r ysgol yn ymgysylltu â nhw.

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

About this policy

This policy outlines what the school needs to do to ensure that it understands the relationship with data processors and that the necessary agreements are in place with any data processors that the school engages with.

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

Fersiwn / *Version*	**Dyddiad / *Date***	**Crynodeb o newidiadau / *Summary of changes***	**Dyddiad a Dderbyniwyd gan Fwrdd o Lywodraethwyr / *Date Accepted by Board of Governors***
F1/*V1*	Hydref 2021 / *October 2021*	Polisi newydd / *New policy.*	

Dyddiad yr adolygiad nesaf / *Date of next review*	
Bydd y polisi hwn yn cael ei adolygu yn: / *This policy will be reviewed in:*	Hydref 2024 / *October 2024*

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: Templed polisi ar y berthynas rhwng yr ysgol ac unrhyw broseswyr data a manylion ynglŷn â chytundebau sy'n seiliedig ar ddeddfwriaeth diogelu data sef *Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR)* a *Deddf Diogelu Data 2018.*

Document: *Policy template on the relationship between the school and any data processors and details regarding agreements based on data protection legislation namely the* UK General Data Protection Regulation (UK GDPR) *and the* Data Protection Act 2018.

Cyfrifoldeb: Cyfrifoldeb y Pennaeth yw sicrhau bod holl staff yr ysgol yn gweithredu ac yn cydymffurfio ac i sicrhau yr ymgynghorir â'r Swyddog Diogelu Data Ysgolion ynghylch defnyddio unrhyw systemau, rhaglenni ac apiau gan gyflenwyr allanol.

Responsibility: *It is the responsibility of the Headteacher to ensure implementation and compliance by all school staff and to ensure that the Schools Data Protection Officer is consulted regarding the use of any systems, programmes, apps by external suppliers.*

Cynnwys **Tudalen**

1. Datganiad Polisi

Mae'r polisi hwn yn nodi'r hyn y mae angen i'r ysgol fel rheolydd data ei wneud i sicrhau ei bod yn deall y berthynas â phroseswyr data a bod y cytundebau/contractau angenrheidiol ar waith gydag unrhyw broseswyr data y mae gan yr ysgol berthynas â hwy. Gall proseswyr data fod yn gyflenwyr allanol sy'n darparu systemau, rhaglenni, apiau a gwasanaethau i'r ysgol.

Mae'r ysgol wedi ymrwymo'n llwyr ei bod yn sicrhau cydymffurfiaeth lawn â deddfwriaeth diogelu data ac yn sicrhau ei bod yn bodloni ei gofynion cyfreithiol, statudol a rheoliadol o dan *UK GDPR* a *Deddf Diogelu Data 2018.*

Bydd yr ysgol yn ymgynghori ac yn gofyn am gyngor y Swyddog Diogelu Data Ysgolion sy'n ymwneud ag unrhyw gytundebau a pherthnasoedd â phroseswyr data a bydd yn cysylltu â'r Swyddog Diogelu Data Ysgolion cyn defnyddio unrhyw systemau, rhaglenni, apiau a gwasanaethau newydd a ddarperir gan sefydliad / cyflenwr allanol.

Bydd yr ysgol hefyd yn gofyn am gyngor y Swyddog Diogelu Data Ysgolion os bydd darparwr allanol yn mynd atyn nhw yn dweud bod yn rhaid iddynt gael cyfrif gyda'r darparwr er mwyn defnyddio unrhyw system, rhaglen neu ap sy'n bodoli eisoes gyda darparwr allanol arall sy'n bodoli eisoes.

2. Sgôp

Mae'r polisi hwn yn berthnasol i holl weithwyr yr ysgol a'r rhai sy'n gweithio ar ran yr ysgol, gan gynnwys llywodraethwyr ysgol, gwirfoddolwyr a chontractwyr, sy'n ymgysylltu â phroseswyr data ac sy'n ymrwymo i ddefnyddio unrhyw systemau, rhaglenni neu apiau sy'n prosesu gwybodaeth bersonol am ddisgyblion, rhieni neu staff ysgol.

3. Deddfwriaeth, Canllawiau a Pholisïau

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

Mae'r polisi hwn hefyd yn seiliedig ar godau ymarfer perthnasol ac ar ganllawiau a gyhoeddwyd gan Swyddfa'r Comisiynydd Gwybodaeth (ICO), gan gynnwys- *'Data controllers and data processors: what the difference is and what the governance implications are'.*

Dylid darllen y polisi hwn hefyd ar y cyd â'r *Polisi Diogelu Data Ysgolion*; *Polisi Asesiad Effaith Diogelu Data Ysgolion*; *Cyfnodau Cadw Ysgolion*; *Polisi Rheoli Cofnodion Ysgolion*; *Polisi Digwyddiadau Diogelwch Data Ysgolion* a *Pholisi Cais gan Wrthrych y Data Ysgolion*. Mae'r rhain i gyd ar gael ar tudalen Diogelu Data sydd ar Feicrowefan y Gwasanaeth Dysgu.

4. Diffiniadau

Data personol	Unrhyw wybodaeth ynglŷn ag unigolyn naturiol yr adnabyddir neu y gellir ei adnabod yn uniongyrchol neu'n anuniongyrchol drwy'r wybodaeth honno. Gellir ei storio'n ddigidol, ar gyfrifiadur, neu mewn systemau ffeilio ar bapur.
Data categori arbennig	Gwybodaeth ynglŷn â hil, tarddiad ethnig, barn wleidyddol, credoau crefyddol neu athronyddol, aelodaeth undeb llafur (neu ddiffyg aelodaeth), gwybodaeth enetig, gwybodaeth fiometreg (i adnabod unigolyn) unigolyn, a gwybodaeth ynglŷn ag iechyd, bywyd rhywiol neu ogwydd rhywiol unigolyn. Data categori arbennig yw data personol sydd angen amddiffyniad bellach oherwydd ei fod yn sensitif.
Prosesu gwybodaeth	Casglu, meddiannu, cofnodi, trefnu, strwythuro, storio, dargadw, diwygio, addasu, altro, adennill, ymgynghori, lledaenu, cyfyngu, datgelu, dinistrio, dileu gwybodaeth neu ei defnyddio neu wneud unrhyw beth â hi.
Digwyddiad diogelwch data	Digwyddiad diogelwch sy'n arwain at ddinistrio, colli, addasu, datgelu'n anawdurdodedig neu fynediad at ddata personol a drosglwyddir, a storir neu a brosesir mewn unrhyw ddull arall gan yr ysgol, yn ddamweiniol neu'n anghyfreithlon.
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 ddigwyddiadau diogelwch 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.
Is-brosesydd	Unrhyw drydydd parti a benodir i brosesu data personol ar ran y prosesydd data.
Gwrthrych y data	Yr unigolyn y mae'r wybodaeth bersonol yn ymwneud ag ef.
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.
Cofnodion o Weithgareddau Prosesu (ROPA)	Disgrifia ROPA yr union ddefnydd o ddata a'r mesurau technegol a sefydliadol sydd gan y rheolydd data ar waith ar gyfer diogelu data. Mae hefyd yn dogfennu pwy sy'n cael ei effeithio drwy brosesu ac mae'n dogfennu derbynnydd prosesu a rhestr o broseswyr data.
Asesiad Effaith Diogelu Data (DPIA)	Asesiad gan y rheolydd data o'r effaith a ragwelir drwy'r prosesu ar ddiogelu data personol, sy'n ofynnol o dan ddeddfwriaeth diogelu data ar gyfer unrhyw brosesu risg uchel.
Systemau Gwybodaeth	Cyfrifiaduron prosesu gwybodaeth neu systemau cyfathrebu data.
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.
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 Ddienw	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.
Storio cwmwl	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.
Ap	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.

5. Cyfrifoldebau

5.1. Corff Llywodraethu Ysgol

Mae'r corff llywodraethu ysgol yn gyfrifol am:

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

5.2. Pennaeth (a/neu Berson sy'n Gyfrifol am Ddiogelu Data yn yr Ysgol)

Mae'r Pennaeth a/neu'r person sy'n gyfrifol am ddiogelu data yn yr ysgol yn gyfrifol am:

- sicrhau a hyrwyddo dealltwriaeth a chydymffurfiaeth â'r polisi hwn a pholisïau statudol a rheoleiddiol eraill sy'n ymwneud â diogelu data;
- sicrhau bod gan yr ysgol sail gyfreithiol dros brosesu data personol a data categori arbennig;

- sicrhau bod staff yn cadarnhau gyda'r Swyddog Diogelu Data Ysgolion fod cytundebau priodol ar waith cyn defnyddio/prynu systemau, rhaglenni neu apiau newydd gan ddarparwyr allanol;
- sicrhau bod diwydrwydd dyladwy wedi digwydd ar broseswyr data;
- adrodd unrhyw ddigwyddiad diogelwch data i'r Swyddog Diogelu Data Ysgolion mor fuan â phosib;
- sicrhau yr ymgynghorwyd â'r Swyddog Diogelu Data Ysgolion ynghylch yr angen i gwblhau Asesiad Effaith Diogelu Data (DPIA);
- dogfennu manylion unrhyw gytundebau/contractau gyda phroseswyr data yng Nghofnodion Gweithgareddau Prosesu'r Ysgol (ROPA);
- bod yn gwbl ymwybodol o'r holl systemau, rhaglenni, apiau a gwasanaethau a ddarperir gan broseswyr data sy'n cael eu defnyddio gan yr ysgol yn ei chyfanrwydd;
- sicrhau bod manylion am broseswyr data yn cael eu cynnwys yn Hysbysiad Preifatrwydd yr ysgol.

5.3. Holl staff yr Ysgol

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

- sicrhau dealltwriaeth a chydymffurfiaeth â'r polisi hwn;
- cadarnhau gyda'r Pennaeth/Swyddog Diogelu Data Ysgolion fod sail gyfreithiol dros brosesu data personol a data categori arbennig a bod cytundeb priodol ar waith cyn defnyddio/agor cyfrif/prynu systemau, rhaglenni, apiau neu wasanaethau newydd gan ddarparwyr allanol;
- darparu manylion unrhyw systemau, rhaglenni neu apiau a ddefnyddir i'r Pennaeth i'w dogfennu;
- adrodd unrhyw ddigwyddiad diogelwch data i'r Pennaeth mor fuan â phosib.

5.4. Swyddog Diogelu Data Ysgolion

Mae'r Swyddog Diogelu Data Ysgolion (Cyngor Sir Ynys Môn) yn gyfrifol am:

- rhoi cyngor ac arweiniad i ysgolion ynghylch telerau cytundebau rhwng yr ysgol a phroseswyr data;
- rhoi cyngor ac arweiniad i ysgolion ynghylch sail gyfreithiol ar gyfer prosesu data personol a data categori arbennig;
- trafod unrhyw delerau cytundebau â phroseswyr data ar ran yr ysgolion pan fydd ysgolion yn gofyn am y gefnogaeth yma;
- cefnogi a darparu cyngor os bydd digwyddiad diogelwch data;
- cefnogi a chynghori ysgolion mewn perthynas â chwblhau Asesiad Effaith Diogelu Data (DPIA);
- cefnogi a chynghori ysgolion ynghylch cynnal gwiriadau diwydrwydd dyladwy ar broseswyr data.

6. Cyfrifoldebau'r Rheolydd Data

Mae'r ysgol fel y rheolwr data'n gyfrifol am ddata personol sy'n cael ei brosesu gan yr ysgol. Mae'r ysgol yn gyfrifol am sicrhau bod gwybodaeth bersonol yn cael ei thrin yn

gyfreithlon, yn deg ac yn dryloyw; bod pobl yn cael eu hamddiffyn rhag niwed a bod eu hawliau gwybodaeth yn cael eu cynnal.

Mae'r ysgol yn pennu'r dibenion ar gyfer sut caiff data personol ei brosesu, neu sut dylid ei brosesu. Mae hyn yn golygu bod yr ysgol yn arfer rheolaeth gyffredinol dros 'pam' a 'sut' gweithgaredd prosesu data.

Dim ond yr ysgol fel rheolydd data a all wneud y penderfyniadau canlynol ynghylch prosesu data:

- casglu'r data personol yn y lle cyntaf a'r sail gyfreithiol dros wneud hynny;
- pa eitemau o ddata personol i'w casglu, h.y. cynnwys y data;
- y diben neu'r dibenion y mae'r data i'w ddefnyddio ar eu cyfer;
- pa unigolion i gasglu data amdanynt;
- a ddylid datgelu'r data, ac os felly, i bwy;
- a yw mynediad i wrthrych y data a hawliau unigolion eraill yn berthnasol i. e. cymhwyso eithriadau; a
- am ba hyd i gadw'r data neu a ddylid gwneud diwygiadau nad ydynt yn rhai arferol i'r data.

6.1. <u>Sail Gyfreithiol dros Brosesu</u>
Rhaid i'r ysgol fod yn fodlon bod ganddi **sail gyfreithiol** dros brosesu data personol. Rhaid prosesu data personol yn deg ac yn gyfreithlon yn unol â hawliau'r unigolyn. Ni fydd yr ysgol ond yn prosesu gwybodaeth bersonol pan fydd o leiaf un o amodau *Erthygl 6 o UK GDPR* wedi'u bodloni:

- 6(1)(a)- **cydsyniad yr unigolyn** - mae'r unigolyn wedi rhoi caniatâd clir i'r ysgol 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 am eu bod wedi gofyn am gymryd camau penodol cyn ymrwymo i gontract;
- 6(1)(c)- **mae prosesu yn angenrheidiol er mwyn cydymffurfio â dyletswydd gyfreithiol** - mae'r prosesu yn angenrheidiol er mwyn i'r ysgol gydymffurfio â'r gyfraith (heb gynnwys rhwymedigaethau cytundebol);
- 6(1)(d)- **mae prosesu yn angenrheidiol er budd hanfodol yr unigolyn neu berson naturiol arall**- mae'r prosesu yn angenrheidiol er mwyn diogelu bywyd rhywun;
- 6(1)(e)- **mae prosesu yn angenrheidiol gan ei fod yn ymgymryd â thasg er budd y cyhoedd neu arfer awdurdod swyddogol -** mae'r prosesu yn angenrheidiol er mwyn i'r ysgol gyflawni tasg er budd y cyhoedd neu er budd swyddogol yr ysgol, ac mae gan y dasg neu'r swyddogaeth sail glir yn y gyfraith;
- 6(1)(f)- **mae prosesu yn angenrheidiol at ddibenion buddiannau cyfreithlon y rheolydd data neu'r trydydd parti**- mae'r prosesu yn angenrheidiol ar gyfer buddiannau cyfreithlon neu fuddiannau cyfreithlon trydydd parti oni bai bod rheswm da dros ddiogelu data personol yr unigolyn sy'n diystyru'r buddiannau cyfreithlon hynny *(nid yw hyn yn berthnasol i awdurdodau cyhoeddus yn prosesu data i gyflawni tasgau swyddogol).*

Mae'r sail gyfreithlon ar gyfer prosesu **data categori arbennig** yn mynnu, yn ogystal â bodloni o leiaf un o amodau *Erthygl 6 o UK GDPR*, fod yn rhaid bodloni amod yn *Erthygl 9 o UK GDPR* hefyd. Ni fydd yr ysgol ond yn prosesu gwybodaeth bersonol sensitif os yw amod yn *Erthygl 9* wedi'i fodloni:

- 9(2)(a)- **prosesu gyda chydsyniad penodol ac eglur yr unigolyn -** oni waherddir dibyniaeth ar gydsyniad gan gyfraith yr UE neu'r Aelod-wladwriaeth;
- 9(2)(b)- **mae prosesu yn angenrheidiol o dan gyfraith cyflogaeth -** neu gyfraith nawdd cymdeithasol, neu gytundeb cyfunol;
- 9(2)(c)- **mae prosesu yn angenrheidiol er mwyn diogelu buddiannau hanfodol yr unigolyn –** gwrthrych y data nad yw'n gallu rhoi cydsyniad yn gorfforol neu'n gyfreithiol;
- 9(2)(d)- **prosesu ar gyfer defnyddio grŵp categori arbennig (sefydliad di-elw sydd â nod gwleidyddol neu grefyddol neu undeb llafur);**
- 9(2)(e)- **mae prosesu yn ymwneud â gwybodaeth a gyhoeddir gan yr unigolyn;**
- 9(2)(f)- **mae prosesu yn angenrheidiol fel y gall y sefydliad amddiffyn hawliadau cyfreithiol -** neu pan fo'r llysoedd yn gweithredu yn rhinwedd eu swydd farnwrol;
- 9(2)(g)- **mae prosesu yn 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 prosesu yn angenrheidiol er mwyn ymateb i anghenion lechyd Galwedigaethol a Gofal Cymdeithasol –** yn angenrheidiol at ddibenion meddygaeth ataliol neu alwedigaethol, ar gyfer asesu capasiti gwaith y cyflogai, diagnosis meddygol, darparu iechyd neu ofal cymdeithasol neu driniaeth 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 yn angenrheidiol am resymau lechyd y Cyhoedd -** megis diogelu rhag bygythiadau trawsffiniol difrifol i iechyd neu sicrhau safonau uchel mewn gofal iechyd a chynhyrchion meddyginiaethol neu ddyfeisiau meddygol;
- 9(2)(j)- **mae prosesu yn angenrheidiol at ddibenion archifo er budd y cyhoedd; neu at ddibenion ymchwil wyddonol neu hanesyddol; neu at ddibenion ystadegol.**

Bydd yr ysgol yn cofnodi ei phenderfyniad ynghylch pa sail gyfreithlon sy'n berthnasol yng Nghofnodion Gweithgareddau Prosesu (ROPA) yr ysgol, er mwyn helpu i ddangos cydymffurfiaeth â'r egwyddorion diogelu data.

7. Proseswyr Data

Prosesydd data yw unrhyw berson sy'n prosesu data personol ar ran rheolydd data (ac eithrio cyflogai'r rheolydd data).

Gall yr ysgol ddefnyddio sefydliadau/darparwyr allanol i brosesu gwybodaeth bersonol ar ei rhan. Cyfeirir at y sefydliadau hyn fel proseswyr data.

Mae angen i'r ysgol fel rheolydd data ddeall ei rhwymedigaethau'n llawn a hyrwyddo arfer dda o ran ymgysylltu â phroseswyr data.

Ni ddylai'r ysgol ond dibynnu ar broseswyr data sy'n darparu digon o warantau mewn perthynas â mesurau rheoli priodol a chydymffurfiaeth â deddfwriaeth diogelu data. Dylai'r ysgol ddewis prosesydd data a all ddarparu digon o warantau mewn perthynas â mesurau diogelwch technegol a sefydliadol sy'n llywodraethu'r prosesu i fynd rhagddo.

Gall proseswyr data fod yn:

- ddarparwyr sy'n darparu gwasanaeth i'r ysgol fel cwmnïau sy'n darparu systemau, rhaglenni neu apiau penodol (e.e. MyConcern, Class Dojo ac ati);
- darparwyr sy'n darparu gwasanaeth TG i'r ysgol (e.e. darparwr gwasanaeth cwmwl);
- darparwyr sy'n darparu gwasanaethau cyflogres.

7.1. Gweithgareddau a Chyfrifoldebau'r Prosesydd Data
Mae gweithgareddau prosesydd yn gyfyngedig i'r agweddau mwy 'technegol' ar weithrediad, megis storio, adalw neu ddileu data. Er y gall yr ysgol ofyn i'r prosesydd data gyflawni rhai agweddau ar y prosesu, yr ysgol fel rheolwr data sydd â'r cyfrifoldeb cyffredinol o hyd.

O fewn telerau'r cytundeb gyda'r ysgol a'i chontract, gall prosesydd data benderfynu:

- pa systemau TG neu ddulliau eraill i'w defnyddio i gasglu data personol;
- sut i storio'r data personol;
- manylion y diogelwch sy'n gysylltiedig â'r data personol;
- y modd a ddefnyddir i drosglwyddo'r data personol o un sefydliad i'r llall;
- y modd a ddefnyddir i adalw data personol am unigolion penodol;
- y dull o sicrhau y glynir wrth gyfnodau cadw; ac
- y modd a ddefnyddir i ddileu neu waredu'r data.

Mae gan brosesydd data y rhyddid i ddefnyddio ei wybodaeth dechnegol i benderfynu sut i gyflawni rhai gweithgareddau ar ran yr ysgol. Fodd bynnag, ni all gymryd unrhyw un o'r penderfyniadau trosfwaol, er enghraifft beth fydd y data personol yn cael ei ddefnyddio ar ei gyfer na beth yw cynnwys y data.

7.2. Ymgysylltu â Phroseswyr Data
Dylai staff yr ysgol gymryd gofal wrth gofrestru i ddefnyddio unrhyw systemau, rhaglenni neu apiau addysgol a ddarperir gan sefydliad/darparwr allanol a sicrhau ei bod yn glir sut mae gwybodaeth bersonol yn cael ei defnyddio a'i phrosesu gan mai'r ysgol fel y rheolwr data sy'n gyfrifol yn y pen draw am y data personol.

Dylid rhoi gofal arbennig pan fydd systemau, rhaglenni neu apiau eisiau mynediad neu eisiau tynnu data o systemau ysgolion eraill megis SIMS. Rhaid ystyried y risgiau cyn comisiynu'r darparwr.

Mae'r ysgol yn gyfrifol am asesu bod y prosesydd data yn gymwys i brosesu'r data personol yn unol â gofynion *UK GDPR.*

Dylai'r ysgol fel rheolydd data gynnal gwiriadau diwydrwydd dyladwy i warantu y bydd y prosesydd data yn gweithredu mesurau technegol a sefydliadol priodol i fodloni gofynion *UK GDPR.* Dylai'r diwydrwydd dyladwy fod yn gymesur â risg y prosesu cyn cytuno ar gontract gyda phrosesydd data.

Dylai'r ysgol ddewis cyflenwyr sy'n dylunio eu cynnyrch neu eu gwasanaethau gyda diogelu data mewn golwg - 'diogelu data yn ôl dyluniad'.

Bydd yr ysgol yn cynnwys manylion unrhyw gytundebau gyda phroseswyr data yng Nghofnodion Gweithgareddau Prosesu (ROPA) yr ysgol.

Gall yr ysgol hefyd nodi yn Hysbysiad Preifatrwydd yr ysgol fanylion proseswyr data (fel trydydd partïon) fel gwybodaeth am bwy y bydd eu data personol yn cael ei rannu gyda neu gyda phwy y gellir ei rannu.

8. Cytundebau / Contractau Prosesu Data

Mae Cytundeb neu Gontract Prosesu Data yn gontract cyfreithiol rwymol rhwng y rheolydd data a'r prosesydd data sy'n nodi hawliau a rhwymedigaethau pob parti sy'n ymwneud â diogelu data personol.

Rhaid i'r ysgol fod â chontract/cytundeb ysgrifenedig ar waith fel ei bod yn ymrwymo i gontract rhwymol neu weithred gyfreithiol arall gyda phrosesydd data. Mae gan y Swyddog Diogelu Data Ysgolion dempled y gellir ei ddefnyddio fel Cytundeb Prosesu Data (DPA)/contract gyda phroseswyr data.

Mae cael contract ysgrifenedig yn helpu pawb i ddeall pwrpas y rhannu; beth fydd yn digwydd ar bob cam a pha gyfrifoldebau sydd ganddynt. Mae cael contract ysgrifenedig yn helpu'r ysgol a'r prosesydd data i ddangos cydymffurfiaeth a deall eu rhwymedigaethau, eu cyfrifoldebau a'u hatebolrwydd.

Mae'n bwysig bod yr ysgol ac unrhyw broseswyr data sy'n ymwneud â gweithgaredd prosesu data yn sefydlu eu rolau a'u cyfrifoldebau yn gynnar, yn enwedig cyn i'r prosesu ddechrau. Bydd hyn yn helpu i sicrhau nad oes bylchau mewn cyfrifoldebau.

Rhaid i gontractau a chytundebau â phroseswyr data gynnwys nifer o ddarpariaethau gorfodol, a rhaid i'r prosesydd data gydymffurfio â'u rhwymedigaethau fel prosesydd data o dan y contract. Dylai contractau/cytundebau sicrhau:

- mai dim ond ar gyfarwyddiadau ysgrifenedig yr ysgol y caiff y sefydliad weithredu;
- bod y rhai sy'n prosesu'r data yn ddarostyngedig i ddyletswydd hyder;
- y cymerir camau priodol i sicrhau diogelwch prosesu;
- mai dim ond gyda chydsyniad blaenorol yr ysgol ac o dan gontract ysgrifenedig y mae is-gontractwyr yn ymwneud â hwy;

- bydd y sefydliad yn cynorthwyo'r ysgol i ddarparu mynediad i wrthrych y data ac yn caniatáu 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 (DPIA);
- 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 cytuno i archwiliadau ac arolygiadau; rhoi pa wybodaeth bynnag sydd ei hangen ar yr ysgol i sicrhau eu bod ill dau'n bodloni eu rhwymedigaethau diogelu data, ac yn dweud wrth yr ysgol ar unwaith os gofynnir iddo wneud rhywbeth sy'n torri cyfraith diogelu data.

Cyn yr ymrwymir ag unrhyw gytundeb newydd sy'n ymwneud â phrosesu gwybodaeth bersonol gan sefydliad allanol, neu os caiff y cytundeb presennol ei newid, dylai'r ysgol ofyn i'r Swyddog Diogelu Data Ysgolion i gymeradwyo ei delerau.

Bydd y Swyddog Diogelu Data Ysgolion yn sicrhau bod cytundebau wedi'u diffinio'n glir ar waith rhwng yr ysgol a'r sefydliad i sicrhau bod data'n cael ei ddiogelu'n briodol ac yn rhoi eglurder ar rolau a chyfrifoldebau. Gall y Swyddog Diogelu Data Ysgolion drafod telerau gyda'r prosesydd data ar ran yr ysgol.

8.1. Gweithredu ar Gyfarwyddiadau Ysgrifenedig yr Ysgol

Dim ond ar gyfarwyddiadau'r ysgol fel rheolydd data y gall proseswyr data weithredu.

Dylai'r ysgol fel y rheolwr data roi cyfarwyddiadau cytundebol i'r prosesydd data gan ddweud beth y gall neu na all y prosesydd data ei wneud gyda'r data, gyda'r contract yn ei gwneud yn ofynnol i'r prosesydd data weithredu ar gyfarwyddiadau'r ysgol yn unig.

Mae llawer o ddarparwyr systemau, rhaglenni ac apiau yn gofyn i'r ysgol lofnodi cytundeb gyda nhw yn hytrach na'r ysgol yn cyhoeddi cytundeb gyda'r darparwr. Yn yr achos hwn, rhaid i'r ysgol fel rheolwr data fod yn fodlon bod telerau'r contract yn bodloni disgwyliadau'r ysgol ac na ddylent gytuno i'r telerau os nad ydynt yn bodloni manylion yr ysgol yn llawn. Yr ysgol fel y rheolwr data sy'n gyfrifol yn y pen draw am y data personol a rhaid iddi fod yn fodlon bod y prosesydd data yn cydymffurfio'n llawn â safonau diogelu data.

Os yw'r prosesydd data yn gweithredu y tu allan i gyfarwyddiadau neu broses yr ysgol at eu dibenion eu hunain, byddant yn camu y tu allan i'w rôl fel prosesydd data ac yn dod yn rheolwr data ar gyfer y prosesu hwnnw.

Gall y Swyddog Diogelu Data Ysgolion gefnogi'r ysgol i adolygu cytundebau a ddarperir gan broseswyr data a gall negydu telerau gyda'r prosesydd data ar ran yr ysgol.

8.2. Dyletswydd Hyder

Mae angen i'r ysgol fod yn fodlon bod y sawl sy'n prosesu data yn ddarostyngedig i ddyletswydd hyder.

Dylai cytundebau nodi bod yn rhaid i unrhyw staff sy'n gweithio i'r prosesydd data gadw at gyfrinachedd a dylai'r prosesydd data ddatgan a yw staff wedi derbyn hyfforddiant deddfwriaeth diogelu data.

8.3. Mesurau Diogelwch Priodol

Mae gan yr ysgol ddyletswydd i sicrhau bod trefniadau diogelwch y prosesydd data o leiaf yn cyfateb i'r diogelwch y byddai'n ofynnol i'r ysgol ei gael pe bai'n prosesu'r data ei hun.

Mae angen i'r ysgol fod yn fodlon bod y prosesydd yn mabwysiadu mesurau diogelwch technegol a sefydliadol sy'n cynnwys amgryptio, ffugenwi, gwydnwch systemau prosesu a ffeilio data personol wrth gefn er mwyn gallu adfer y system.

Disgwylir i'r prosesydd data fod â mesurau diogelwch ar waith sy'n cynnwys diogelu data personol rhag dinistr neu golled ddamweiniol neu anghyfreithlon, addasiad, datgeliad heb awdurdod neu fynediad.

Felly, mae angen i'r ysgol sicrhau bod y cytundeb gyda'r prosesydd data yn cynnwys manylion am y mesurau a gymerir gan y prosesydd data i sicrhau diogelwch y prosesu a bod y mesurau hyn yn hyfedr.

8.4. Dim ond gyda Chysyniad Blaenorol yr Ysgol yr Ymgysylltir ag Is-gontractwyr

Dim ond gyda chydsyniad blaenorol yr ysgol ac o dan gontract ysgrifenedig y dylai proseswyr data ymgysylltu ag is-gontractwyr. Gall proseswyr data ddefnyddio is-gontractwr i ddarparu eu gwasanaethau/elfennau o'u gwasanaethau, ond dylai'r prosesydd data ofyn am gydsyniad yr ysgol fel y rheolwr data cyn is-gontractio unrhyw un o'i gwasanaethau. Enghraifft o hyn yw is-gontractio i ddarparwr gwasanaeth cwmwl.

Mae angen i'r ysgol fod yn ymwybodol os dyma'r achos a dylid rhoi cyfle iddi wrthwynebu'r defnydd o is-broseswyr.

Dylai'r contract ysgrifenedig rhwng yr ysgol a'r prosesydd data nodi a yw'r prosesydd data yn defnyddio unrhyw is-gontractwyr a dylai roi manylion pwy yw'r is-gontractwyr fel bod yr ysgol yn glir beth sy'n digwydd i'r data personol a phwy sy'n prosesu'r data personol.

Os yw'r prosesydd data yn defnyddio is-brosesydd i helpu i brosesu data personol ar gyfer yr ysgol, mae angen iddo gael contract ysgrifenedig ar waith gyda'r is-brosesydd. Rhaid i'r prosesydd data roi contract ar waith gyda'r is-brosesydd gyda thelerau sy'n cynnig lefel gyfartal o ddiogelwch ar gyfer data personol â'r rhai yn y contract rhwng y prosesydd data a'r ysgol fel y rheolydd data.

8.5. Cynorthwyo'r Ysgol i Ddarparu Mynediad i Wrthrych y Data a Chaniatáu i Unigolion Arfer eu Hawliau

Mae angen i gytundebau nodi y bydd y prosesydd data yn cynorthwyo'r ysgol i ddarparu mynediad i wrthrych y data ac yn caniatáu i unigolion arfer eu hawliau mewn perthynas â diogelu data.

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

1. Yr hawl i gael gwybod;
2. Yr hawl i gael mynediad;
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 mewn perthynas â gwneud penderfyniadau a phroffilio awtomataidd.

Mae angen i'r ysgol fod yn fodlon y bydd y prosesydd data yn cynorthwyo'r ysgol i ganiatáu i unigolion arfer eu hawliau diogelu data.

8.6. Dileu neu Ddychwelyd Data Personol i'r Ysgol
Mae angen cymalau ar gontractau sy'n nodi y bydd prosesydd data yn dileu neu'n dychwelyd yr holl wybodaeth bersonol i'r ysgol ar ddiwedd y contract.

Os bydd yr ysgol yn terfynu contract gyda phrosesydd data, mae angen iddo sicrhau bod yr holl ddata personol a gedwir o fewn y system, y rhaglen neu'r ap naill ai'n cael ei ddileu gan y prosesydd data neu'n cael ei ddychwelyd i'r ysgol.

Os caiff yr wybodaeth ei dileu gan y prosesydd data, mae angen cadarnhad ysgrifenedig sy'n nodi bod yr holl ddata personol wedi'i ddileu a'r dyddiad y gwnaed hyn.

8.7. Cynorthwyo'r Ysgol gyda Diogelwch Prosesu; Hysbysu am Ddigwyddiadau Diogelwch Data ac Asesiad Effaith Diogelu Data (DPIA)
Rhaid i gytundebau nodi y bydd y prosesydd data yn cynorthwyo'r ysgol i gyflawni ei rhwymedigaethau mewn perthynas â diogelwch prosesu, hysbysu am ddigwyddiadau diogelwch data ac Asesiadau Effaith Diogelu Data (DPIA).

Mae angen i'r cytundeb ddatgan bod gan y prosesydd data gyfrifoldeb i hysbysu'r ysgol fel y rheolydd data heb oedi gormodol (cyn gynted â phosibl) os daw'n ymwybodol bod digwyddiad diogelwch data yn cael ei ganfod. Nid oes eithriad i hyn a rhaid i'r prosesydd data roi gwybod am yr holl ddigwyddiadau diogelwch data i'r ysgol, waeth beth fo'u maint.

Mae DPIA yn ddull strwythuredig o nodi risgiau diogelu data sy'n gysylltiedig â phrosesu data personol; i helpu'r ysgol i nodi a lleihau'r risgiau ac ar gyfer gweithredu rheolaethau priodol i'w rheoli. Mae DPIA yn ofyniad cyfreithiol ar gyfer prosesu sy'n debygol o fod yn risg uchel. Dylai prosesydd data roi ei fewnbwn i DPIA lle bo'n briodol. Efallai y bydd angen i'r ysgol ofyn i'r prosesydd data am wybodaeth a chymorth. Dylai cytundebau nodi y gallai fod yn ofynnol i broseswyr data helpu i gwblhau DPIAau.

Bydd y Swyddog Diogelu Data Ysgolion yn cynorthwyo â digwyddiadau diogelwch data a chreu DPIAau.

8.8. Cytuno i Archwiliadau ac Arolygiadau
Mae angen i'r ysgol allu dangos ei bod yn cydymffurfio â chyfreithiau diogelu data a bydd angen i'r prosesydd data ddangos eu bod hefyd yn cydymffurfio.

Mae'r ICO yn disgwyl i reolwyr data gymryd camau rhesymol i sicrhau bod diogelwch yn cael ei gynnal. Un enghraifft o hyn yw cynnal archwiliad rheolaidd o drefniadau diogelwch y prosesydd data. Bydd angen i'r ysgol fel rheolydd data hefyd gadarnhau bod y prosesydd data'n cydymffurfio â'r holl delerau ac amodau cytundebol. Dylai gwiriadau cydymffurfio fod yn gymesur â'r risgiau prosesu.

Rhaid i gytundebau nodi y bydd y prosesydd data yn cytuno i archwiliadau ac arolygiadau.

Mae angen i gytundebau nodi y bydd y prosesydd data yn rhoi'r holl wybodaeth sydd ei hangen ar yr ysgol i sicrhau eu bod ill dau'n bodloni eu rhwymedigaethau diogelu data. Mae angen i gytundebau nodi y bydd y prosesydd data yn dweud wrth yr ysgol ar unwaith os gofynnir iddo wneud rhywbeth sy'n torri cyfraith diogelu data.

9. Materion Gorfodi

Mae'r rheolydd data a'r prosesydd data yn gyfrifol am gydymffurfio'n rhagweithiol â'r ddeddfwriaeth diogelu data. Mae'r gwahaniaeth rhwng rheolydd data a phrosesydd data yn arbennig o bwysig yng nghyd-destun gorfodi o dan ddeddfwriaeth diogelu data. Er enghraifft, os oes digwyddiad diogelwch data mae'n hanfodol i'r ysgol; y prosesydd data dan sylw a'r ICO allu penderfynu ble mae'r cyfrifoldeb.

Mae deddfwriaeth diogelu data yn nodi'n glir mai'r rheolydd data sy'n gyfreithiol gyfrifol am brosesu data personol y mae'n ymgymryd ag ef ei hun ac sy'n cael ei wneud ar ei ran gan brosesydd data. Mae'n bwysig bod yr ysgol yn rhoi'r mesurau angenrheidiol ar waith i ddiogelu ei gweithrediad prosesu data rhag unrhyw natur fregus a allai godi o ddefnyddio prosesydd data.

Mae deddfwriaeth diogelu data yn rhoi'r hawl i unrhyw berson sydd wedi dioddef difrod materol neu ansylweddol o ganlyniad i dorri *UK GDPR* gael iawndal gan y rheolwr data neu'r prosesydd data am y difrod a ddioddefwyd.

O ran atebolrwydd, dim ond am y prosesu y maent yn ei wneud y bydd proseswyr data yn atebol, neu lle maent wedi gweithredu'n groes i gyfarwyddyd yr ysgol fel rheolydd data. Gall proseswyr data hefyd fod yn atebol os ydynt wedi methu â chydymffurfio â darpariaethau *UK GDPR* sy'n ymwneud yn benodol â phroseswyr data.

Bydd yr ICO yn ystyried graddau cyfrifoldeb y rheolydd data neu'r prosesydd data wrth benderfynu a fydd unrhyw ddirwy yn cael ei gosod a maint y ddirwy. Rhoddir ystyriaeth ddyledus i unrhyw weithdrefnau neu ddulliau arfer gorau a bydd yr ICO yn asesu i ba raddau y gwnaeth y rheolwr data yr hyn y gallai/y dylai i gydymffurfio â deddfwriaeth diogelu data.

Mae'n bwysig bod contract/cytundeb ar waith rhwng yr ysgol a phrosesydd data er mwyn nodi ble mae'r atebolrwydd pan fu torri hawliau diogelu data unigolyn.

10. Torri'r Polisi

Gallai methiant i gydymffurfio 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 gan drydydd partïon.

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 gweithiwr nad yw'n gyflogai yn mynd yn groes i'r polisi hwn, efallai y bydd eu contract yn cael ei derfynu ar unwaith.

11. Adolygiad o Drefniadau Polisi a Goruchwylio

Caiff y polisi hwn ei adolygu gan y Swyddog Diogelu Data Ysgolion bob tair blynedd, oni bai bod newidiadau i ddeddfwriaeth, codau ymarfer, canllawiau neu gyngor comisiynydd, neu wendidau newydd yn ei gwneud yn ofynnol i'r polisi gael ei ddiweddaru'n gynt.

Caiff y polisi ei gymeradwyo gan Uwch Dîm Rheoli'r Gwasanaeth Dysgu a chaiff ei fabwysiadu gan gorff llywodraethu'r ysgol. Bydd Tîm Arweinyddiaeth a chorff llywodraethu'r ysgol yn monitro cydymffurfiaeth â'r polisi hwn a gweithdrefnau cysylltiedig.

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

Ffôn: 01248 751833

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

Gellir cael rhagor o wybodaeth ynglŷn â rheolwyr data a phroseswyr data ar wefan Swyddfa'r Comisiynydd Gwybodaeth: https://ico.org.uk/

Content **Page**

1. Policy Statement

This policy sets out what the school as a data controller needs to do to ensure that it understands the relationship with data processors and that the necessary agreements/contracts are in place with any data processors that the school has a relationship with. Data processors can be external suppliers that provide the school with systems, programs, apps and services.

The school is fully committed that it ensures full compliance with data protection legislation and ensures that it is meeting its legal, statutory and regulatory requirements under the *UK GDPR* and the *Data Protection Act 2018.*

The school will consult and seek the advice of the Schools Data Protection Officer relating to any agreements and relationships with data processors and will contact the Schools Data Protection Officer before using any new systems, programmes, apps and services that are provided by an external organisation/supplier.

The school will also seek the advice of the Schools Data Protection Officer if an external provider approaches them stating that they must have an account with the provider in order to use any existing system, programme or app with another existing external provider.

2. Scope

This policy applies to all employees of the school and those working on behalf of the school, including school governors, volunteers and contractors, who engage with data processors and sign-up to the use of any systems, programmes or apps that process personal information regarding pupils, parents or school staff.

3. Legislation, Guidance and Policies

The main data protection legislation that this policy complies with is that of the *UK General Data Protection Regulation (UK 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), including- *'Data controllers and data processors: what the difference is and what the governance implications are'.*

This policy should also be read in conjunction with the *Schools Data Protection Policy; Schools Data Protection Impact Assessment (DPIA) Policy; Schools Retention Schedule*; *Schools Records Management Policy*; *Schools Data Breach Policy* and *Schools Data Subject Access Request Policy*. These are all available on the Data Protection page on the Learning Service Microsite.

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.
Processing information	Collecting, obtaining, recording, organising, structuring, storing, retaining, amending, adapting, altering, retrieving, consulting, disseminating, restricting, disclosing, destroying, erasing information or using or doing anything with it.
Data 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.
Sub-processor	Any third party appointed to process personal data on behalf of the data processor.
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.
Records of Processing	ROPA describes the exact usage of data and the technical and organisational measures that the data controller has in place

Activities (ROPA)	for the protection of data. It also documents who is affected by processing and it documents the recipient of a processing and a list of data processors.
Data Protection Impact Assessment (DPIA)	An assessment by the data controller of the impact of the envisaged processing on the protection of personal data, which is required under data protection legislation for all high risk processing.
Information Systems	Information processing computers or data communication systems.
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.
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.
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.
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.

5. Responsibilities

5.1. School Governing Body

The school governing body has the responsibility for:

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

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 and promoting understanding and compliance with this policy and other statutory and regulatory policies relating to data protection;
- ensuring that the school has a legal basis for processing personal data and special category data;

- ensuring that staff confirm with the Schools Data Protection Officer that there are appropriate agreements in place before using/purchasing new systems, programmes or apps from external providers;
- ensuring due diligence has taken place on data processors;
- reporting a data breach to the Schools Data Protection Officer as soon as possible;
- ensuring that the Schools Data Protection Officer has been consulted regarding the need to complete a Data Protection Impact Assessment (DPIA);
- documenting details of any agreements/contracts with data processors in the school's Records of Processing Activities (ROPA);
- being fully aware of all systems, programmes, apps and services that are provided by data processors that are in use by the school in its entirety;
- ensuring that details regarding data processors are included in the school's Privacy Notice.

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:

- ensuring understanding and compliance with this policy;
- confirming with the Headteacher/Schools Data Protection Officer that there is a legal basis for processing personal data and special category data and that there is an appropriate agreement in place before using/opening an account/purchasing new systems, programmes, apps or services from external providers;
- providing details of any systems, programmes or apps used to the Headteacher for documenting;
- reporting any data breach to the Headteacher as soon as possible.

5.4. Schools Data Protection Officer

The (Isle of Anglesey County Council) Schools Data Protection Officer is responsible for:

- providing advice and guidance to schools regarding terms of agreements between the school and data processors;
- providing advice and guidance to schools regarding legal basis for processing personal data and special category data;
- negotiating any terms of agreements with data processors on behalf of the schools when schools asks for this support;
- supporting and providing advice in the event of a data breach;
- supporting and advising schools in relation to completing a Data Protection Impact Assessment (DPIA);
- supporting and advising schools regarding conducting due diligence checks on data processors.

6. Data Controller's Responsibilities

The school as the data controller is ultimately responsible for personal data that is processed by the school. The school is responsible for making sure personal information is handled lawfully, fairly, and transparently; that people are protected from harm and that their information rights are upheld.

The school determines the purposes for which and the manner in which any personal data are, or are to be processed. This means that the school exercises overall control over the 'why' and the 'how' of a data processing activity.

It is only the school as a data controller that can make the following decisions regarding processing data:

- to collect the personal data in the first place and the legal basis for doing so;
- which items of personal data to collect i.e. the content of the data;
- the purpose or purposes the data are to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, who to;
- whether subject access and other individuals' rights apply i.e. the application of exemptions; and
- how long to retain the data or whether to make non-routine amendments to the data.

6.1. Legal Basis for Processing
The school must be satisfied that is has a **legal basis** for processing personal data. 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* the *UK 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 lawful basis for processing **special category data** requires that in addition to satisfying at least one of the conditions of *Article 6 of* the *UK GDPR*, a condition in *Article 9 of the UK GDPR* must also be satisfied. 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.**

The school will document its decision as to which lawful basis applies in the school's Records of Processing Activities (ROPA), to help demonstrate compliance with the data protection principles.

7. Data Processors

A data processor is any person who processes personal data on behalf of a data controller (other than the employee of the data controller).

The school can use external organisations/providers to process personal information on its behalf. These organisations are referred to as data processors.

The school as a data controller needs to fully understand its obligations and promote good practice when it comes to engaging with data processors.

The school should only rely on data processors that provide sufficient guarantees in relation to appropriate control measures and data protection legislation compliance. The school should choose a data processor that can provide sufficient guarantees in respect of technical and organisational security measures governing the processing to be carried out.

Data processors can be:

- providers who provide a service to the school such as companies who provide specific systems, programmes or applications (e.g. MyConcern, Class Dojo etc.);
- providers that provide an IT service for the school (e.g. cloud service provider);
- providers that provide payroll services.

7.1. Data Processor's Activities and Responsibilities
A data processor's activities are limited to the more 'technical' aspects of an operation, such as data storage, retrieval or erasure. Although the school can ask the data processor to carry out certain aspects of the processing, overall responsibility remains with the school as the data controller.

Within the terms of the agreement with the school, and its contract, a data processor may decide:

- what IT systems or other methods to use to collect personal data;
- how to store the personal data;
- the detail of the security surrounding the personal data;
- the means used to transfer the personal data from one organisation to another;
- the means used to retrieve personal data about certain individuals;
- the method for ensuring a retention schedule is adhered to; and
- the means used to delete or dispose of the data.

A data processor has the freedom to use its technical knowledge to decide how to carry out certain activities on the school's behalf. However, it cannot take any of the over-arching decisions, for example what the personal data will be used for or what the content of the data is.

7.2. Engaging with Data Processors
Care should be taken by school staff when signing up to using any educational systems, programmes or apps supplied by an external organisation/provider and ensure that it is clear how personal information is used and processed as the school as the data controller has the ultimate responsibility for the personal data.

Particular care should be given when systems, programmes or apps want access or want to extract data from other school systems such as SIMS. The risks must be considered before commissioning the provider.

The school is responsible for assessing that the data processor is competent to process the personal data in line with *UK GDPR's* requirements.

The school as a data controller should undertake due diligence checks to guarantee the data processor will implement appropriate technical and organisational measures to meet *UK GDPR* requirements. The due diligence should be proportionate to the risk of the processing before agreeing a contract with a data processor.

The school should choose suppliers that design their products or services with data protection in mind- 'data protection by design'.

The school will include details of any agreements with data processors in the school's Records of Processing Activities (ROPA).

The school may also state in the school's Privacy Notice details of data processors (as third parties) as information regarding who their personal data will or may be shared with.

8. Data Processing Agreements / Contracts

A Data Processing Agreement (DPA) or contract is a legally binding contract between the data controller and data processor that states the rights and obligations of each party concerning the protection of personal data.

The school must have a written contract/agreement in place so that it enters in to a binding contract or other legal act with a data processor. The Schools Data Protection Officer has a template that can be used as a Data Processing Agreement (DPA)/contract with data processors.

Having a written contract helps everyone to understand the purpose of the sharing; what will happen at each stage and what responsibilities they have. Having a written contract helps the school and the data processor to demonstrate compliance and understand their obligations, responsibilities and liabilities.

It is important that the school and any data processors involved in a data processing activity establish their roles and responsibilities at an early stage, particularly before the processing commences. This will help to ensure that there are no gaps in responsibilities.

Contracts and agreements with data processors must contain a number of compulsory provisions, and the data processor must comply with their obligations as a data processor under the contract. Contracts/agreements should 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 should 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. The Schools Data Protection Officer can negotiate terms with the data processor on behalf of the school.

8.1. Acting on the Written Instructions of the School
Data processors may act only on the written instructions of the school as a data controller.

The school as the data controller should issue contractual instructions to the data processor saying what the data processor can or cannot do with the data, with the contract requiring the data processor to only act on the school's instructions.

Many system, programme and app providers ask that the school signs an agreement with them rather than the school issuing an agreement with the provider. In this case, the school as the data controller must be satisfied that the terms of the contract meets the expectations of the school and must not agree to the terms if they do not fully satisfy the school's expecations. The school as the data controller is ultimately responsible for the personal data and must be satisfied that the data processor is fully compliant with data protection standards.

If the data processor acts outside of the school's instructions or process for their own purposes, they will step outside their role as a data processor and become a data controller for that processing.

The Schools Data Protection Officer can support the school with reviewing agreements provided by data processors and can negotiate terms with the data processor on behalf of the school.

8.2. Duty of Confidence
The school needs to be satisfied that those processing data are subject to a duty of confidence.

Agreements should state that any staff working for the data processor must adhere to confidentiality and the data processor should state whether staff have received data protection legislation training.

8.3. Appropriate Security Measures
The school has a duty to ensure that the data processor's security arrangements are at least equivelant to the security the school would be required to have in place if it was processing the data itself.

The school needs to be satisfied that the processor adopts technical and organisational security measures that includes encryption, pseudonymisation, resilience of processing systems and backing up personal data in order to be able to reinstate the system.

It is expected that the data processor has security measures in place that includes protecting personal data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.

The school therefore needs to ensure that the agreement with the data processor contains details regarding the measures that are taken by the data processor to ensure the security of the processing and that these measures are proficient.

8.4. Sub-contractors are only Engaged with the Prior Consent of the School

Data processors should only engage sub-contractors with the prior consent of the school and under a written contract. Data processors may use a sub-contractor to deliver their services/elements of their services, but the data processor should seek the consent of the school as the data controller prior to sub-contracting out any of its services. An example of this is to sub-contract to a cloud service provider.

The school needs to be aware if this is the case and should be provided with the opportunity to object to using sub-processors.

The written contract between the school and the data processor should stipulate if the data processor uses any sub-contractors and should provide details of who the sub-contractors are so that the school is clear what happens to the personal data and who is processing the personal data.

If the data processor uses a sub-processor to assist in its processing of personal data for the school, it needs to have a written contract in place with the sub-processor. The data processor must put in place a contract with the sub-processor with terms that offer an equivelant level of protection for personal data as those in the contract between the data processor and the school as the data controller.

8.5. Assisting the School in Providing Subject Access and Allowing Individuals to Exercise their Rights

Agreements need to specify that the data processor will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection.

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 school needs to be satisfied that the data processor will assist the school in allowing individuals to exercise their data protection rights.

8.6. Deleting or Returning Personal Data to the School

Contracts need clauses that specify that a data processor will delete or return all personal information to the school at the end of the contract.

If the school terminates a contract with a data processor, it needs to ensure that all personal data held within the system, programme or app is either deleted by the data processor or returned to the school.

If the information is deleted by the data processor, written confirmation is needed detailing that all personal data has been deleted and the date that this has been undertaken.

8.7. Assisting the School with the Security of Processing; Notification of Data Breaches and Data Protection Impact Assessment (DPIA)

Agreements need to specify that the data processor 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 agreement needs to state that the data processor has a responsibility to inform the school as the data controller without undue delay (as soon as possible) if it becomes aware that a data breach is detected. There is no exemption to this and the data processor must report all data breaches to the school, regardless of their size.

A DPIA is a structured approach to identifying data protection risks associated with the processing of personal data; to help the school identify and minimise the risks and for implementing appropriate controls to manage them. A DPIA is a legal requirement for processing that is likely to be high risk. A data processor should provide their input in to a DPIA where appropriate. The school may need to ask the data processor for information and assistance. Agreements should state that data processors may be required to assist with completing DPIAs.

The Schools Data Protection Officer will assist with data breaches and creating DPIAs.

8.8. Submitting to Audits and Inspections

The school needs to be able to demonstrate compliance with data protection laws and will also need the data processor to demonstrate that they are also compliant.

The ICO expects that data controllers take reasonable steps to ensure security is maintained. An example of this is undertaking regular auditing of the data processor's security arrangements. The school as a data controller will also need to confirm that the data processor is complying with all contractual terms and conditions. Compliance checks should be proportionate to the processing risks.

Agreements need to specify that the data processor will submit to audits and inspections.

Agreements need to specify that the data processor will provide the school with all information necessary that it needs to ensure that they are both meeting their data protection obligations.

Agreements need to specify that the data processor will tell the school immediately if it is asked to do something infringing data protection law.

9. Enforcement Issues

Both the data controller and data processor are responsible for proactively complying with the data protection legislation. The distinction between a data controller and a data processor is particularly important in the context of enforcement under data protection legislation. For example, if there is a data breach it is essential for the school; the data processor involved and the ICO to be able to determine where responsibility lies.

Data protection legislation clearly states that the data controller is legally responsible for the processing of personal data it undertakes itself and that is undertaken on its behalf by a data processor. It is important that the school puts the necessary measures in place to protect its data processing operation from any vulnerability that may arise from the use of a data processor.

Data protection legislation provides any person who has suffered material or non-material damage as a result of an infringement of the *UK GDPR* the right to receive compensation from the data controller or data processor for the damage suffered.

In terms of liability, data processors will only be liable for the processing they carry out, or where they have acted contrary to the instruction of the school as a data controller. Data processors may also be liable if they have failed to comply with *UK GDPR* provisions specifically relating to data processors.

The ICO will consider the degree of responsibility of the data controller or data processor when determining whether any fine will be imposed and the size of the fine. Due account will be taken of any best-practice procedures or methods and the ICO will assess to what extent the data controller did what it could/should to comply with data protection legislation.

It is important that a contract/agreement is in place between the school and a data processor in order to identify where the liability lies when there has been an infringement of an individual's data protection rights.

10. 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.

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.

11. Review of Policy and Oversight Arrangements

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

The policy will be approved by the Learning 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 controllers and data processors, can be obtained from the ICO website: https://ico.org.uk/