Polisi Diogelu Data 2022

Rheoliad Diogelu Data Cyffredinol (GDPR) a Deddf Diogelu Data 2018

Data Protection Policy 2022

General Data Protection Regulation (GDPR) and the Data Protection Act 2018

Ffederasiwn Ysgol Dyffryn Dulas ac Ysgol Pennal

1. Cyflwyniad

Er mwyn gweithredu'n effeithlon, mae'n rhaid i'r Ysgol gasglu a defnyddio gwybodaeth am bobl y mae'n gweithio â hwy. Gall y rhain gynnwys aelodau o'r cyhoedd, cyn-weithwyr, gweithwyr cyfredol a darpar weithwyr, disgyblion a chyflenwyr. Hefyd, efallai y bydd y gyfraith yn ei gwneud yn ofynnol i gasglu a defnyddio gwybodaeth er mwyn cydymffurfio â gofynion llywodraeth ganolog.

Mae'r ysgol wedi ymrwymo i sicrhau yr ymdrinnir â gwybodaeth bersonol yn briodol, ac mae'n sicrhau cydymffurfiaeth â deddfwriaeth diogelu data. Bydd yr Ysgol yn gwneud pob ymdrech i fodloni ei rhwymedigaethau o dan y ddeddfwriaeth a bydd yn adolygu gweithdrefnau yn gyson er mwyn sicrhau ei bod yn gwneud hynny.

Diffiniadau

Data Personol yw gwybodaeth sy'n ymwneud ag unigolyn byw y gellir ei adnabod sy'n cael ei brosesu fel data. Mae prosesu yn golygu casglu, defnyddio, datgelu, cadw neu waredu gwybodaeth. Mae'r egwyddorion diogelu data yn gymwys ar gyfer yr holl wybodaeth a ddelir yn electronig neu mewn ffeiliau strwythuredig sy'n dweud rhywbeth wrthych am unigolyn byw y gellir ei adnabod.
Mae'r egwyddorion hefyd yn ymestyn i'r holl wybodaeth sydd yn y cofnodion addysg. Enghreifftiau o hyn fyddai enwau staff a disgyblion, dyddiadau geni, cyfeiriadau, rhifau yswiriant cenedlaethol, marciau ysgol, gwybodaeth feddygol, canlyniadau arholiadau, asesiadau AAA ac adolygiadau datblygu staff.

Data Categori Arbennig yw gwybodaeth sy'n ymwneud â hil neu ethnigrwydd, barn wleidyddol, credoau crefyddol, aelodaeth undebau llafur, iechyd, geneteg, rhywioldeb, bywyd rhywiol a data biometrig.
Y gwahaniaeth rhwng prosesu data personol a data categori arbennig yw bod cyfyngiadau cyfreithiol mwy ar yr olaf gan ei fod yn ddata mwy sensitif.

Data Troseddol - mae Erthygl 10 y Rheoliad Diogelu Data Cyffredinol (GDPR) yn nodi'r rheoliadau ar gyfer prosesu data troseddol.

2. Sgôp

Mae'r polisi hwn yn berthnasol i holl weithwyr, llywodraethwyr, contractwyr, asiantaethau a chynrychiolwyr a staff dros dro sy'n gweithio i'r ysgol neu ar ei rhan.

Mae'r polisi hwn yn berthnasol i'r holl wybodaeth bersonol a grëwyd neu a ddelir gan yr Ysgol ym mha bynnag fformat (e.e. papur, electronig, e-bost, ffilm) a pha bynnag fodd y mae'n cael ei storio (er enghraifft, system/cronfa ddata TGCh, safle Sharepoint, strwythur ffeilio gyriant a rennir, e-bost, cabinet ffeilio, silffoedd a droriau ffeilio personol a dyfeisiau symudol gan gynnwys ffonau symudol, TCC).

Mae unrhyw wybodaeth sy'n cael ei chreu gan yr Ysgol a'i staff yn dod yn eiddo i'r ysgol.

Nid yw Deddfwriaeth Diogelu Data (DDD) yn berthnasol o ran cael mynediad at wybodaeth am unigolion sydd wedi marw.

3. Cyfrifoldebau

Y Llywodraethwyr sydd â chyfrifoldeb cyffredinol dros gydymffurfio gyda'r DDD.

Mae'r Pennaeth yn gyfrifol am sicrhau cydymffurfiaeth gyda'r DDD a'r polisi hwn o fewn gweithgareddau dyddiol yr ysgol. Mae'r Pennaeth yn gyfrifol am sicrhau y darperir hyfforddiant priodol i'r holl staff.

Mae pob aelod o staff neu gontractwyr sy'n dal neu'n casglu data personol yn gyfrifol am eu cydymffurfiaeth eu hunain gyda'r DDD a dylent sicrhau y cedwir ac y prosesir gwybodaeth bersonol yn unol â'r DDD.

Dylai pob aelod o staff ddangos eu bod wedi darllen, deall a derbyn y Polisi hwn.

4. Y Gofynion

Mae'r DDD yn nodi fod yn rhaid i unrhyw un sy'n prosesu data personol gydymffurfio â chwe egwyddor arfer dda; gorfodir yr arferion hyn yn gyfreithiol.

Yng nghyd-destun gwybodaeth bersonol:

Mae Erthygl 5(1) y GDPR yn nodi fel a ganlyn ynghylch data personol;

a) dylid ei brosesu mewn dull cyfreithiol, teg a thryloyw
b) dim ond ar gyfer un neu ragor o ddibenion penodol, clir a chyfreithlon y dylid cael gafael ar y wybodaeth ac ni ddylid ei phrosesu ymhellach mewn unrhyw ffordd nad yw'n cyd-fynd â'r diben neu'r dibenion hynny;
c) bydd y wybodaeth yn ddigonol, yn berthnasol ac nid yn ormodol o'i gymharu â diben neu ddibenion ei phrosesu;
d) bydd y wybodaeth yn gywir a, pan fo hynny'n briodol, yn hollol gyfredol;
e) ni ddylid cadw'r wybodaeth yn hirach nag sydd yn rhaid ar gyfer y diben neu'r dibenion hynny;
f) bydd y wybodaeth yn cael ei chadw'n ddiogel, h.y. ei gwarchod gan raddfa briodol o ddiogelwch.

Fel Rheolydd Data, mae gofyn i'r ysgol gadw Cofnod o weithgareddau prosesu/Cofrestr Asedau, sy'n cynnwys;

- Disgrifiad o'r categorïau o Ddata Personol a Chategorïau o Destunau Data
- Dibenion y prosesu
- Y categorïau o dderbynyddion y mae data personol wedi cael ei datgelu iddynt, neu y bydd data personol yn cael ei datgelu iddynt

Mae gofyn i'r Ysgol dalu ffi flynyddol i Swyddfa'r Comisiynydd Gwybodaeth (ICO).
Gallai methu â gwneud hynny arwain at gosb ariannol.

5. Hysbysiadau Preifatrwydd

Pryd bynnag y cesglir gwybodaeth am unigolion, bydd yr ysgol yn darparu'r wybodaeth a ganlyn:

- Pwy yw rheolydd y data, e.e. yr ysgol;
- Pwrpas casglu'r wybodaeth;
- Y sail gyfreithlon pam yr ydym yn casglu'r wybodaeth
- Unrhyw bwrpasau eraill y gellir ei ddefnyddio;
- Gyda phwy y bydd, neu gellir, rhannu'r wybodaeth;
- Pa mor hir y cedwir y wybodaeth
- Manylion ynghylch hawliau'r unigolion
- Manylion ynghylch y Swyddog Diogelu Data

Mae'n rhaid i hyn ddigwydd ar yr amser y dechreuir casglu gwybodaeth am unigolyn.

Os yw'r wybodaeth yn cael ei chasglu'n uniongyrchol gan blentyn, rhaid i'r hysbysiad preifatrwydd gael ei gyflwyno mewn iaith glir, plaen a phriodol i'w hoedran.

6. Amodau ar gyfer Prosesu

Dim ond pan fo un o amodau Atodlen 6 y GDPR wedi cael eu bodloni y gellir prosesu data personol. Gellir ond prosesu data categori arbennig pan fo amod yn Atodlen 9 y GDPR wedi cael ei fodloni yn ogystal ag un yn Atodlen 6.

7. Datgelu Data

Mae hi'n drosedd i gael neu ddatgelu gwybodaeth am unigolyn yn fwriadol neu'n fyrbwyll heb achos cyfiawn.

- Ni ddylai'r ysgol ddatgelu unrhyw beth am gofnod y disgybl fyddai'n debygol o beri niwed sylweddol i'w iechyd corfforol neu feddyliol nac i iechyd corfforol neu feddyliol unrhyw berson arall.

- Lle mae amheuaeth neu wrthdaro o ran y gofynion statudol, dylid ceisio cyngor.

- Wrth roi gwybodaeth i unigolyn, yn enwedig ar y ffôn, yn bwysicaf oll, mae'n rhaid gwirio pwy yw'r unigolyn hwnnw. Os oes amheuaeth, dylid gofyn cwestiynau i'r unigolyn, rhai na all neb ond ef/hi eu hateb. Ni ddylid darparu gwybodaeth i bartïon eraill, hyd yn oed os ydynt yn perthyn. Er enghraifft: yn achos rhieni sydd wedi ysgaru, mae'n bwysig nad yw gwybodaeth ynghylch y naill barti yn cael ei rhoi i'r llall am nad oes ganddynt hawl i'w derbyn.

Dylid ond rhoi data perthnasol, cyfrinachol i:

- *aelodau staff eraill ar sail yr angen i wybod;*
- *rhieni/gwarcheidwaid perthnasol; sefydliadau eraill os yn angenrheidiol er lles y cyhoedd, e.e. atal trosedd;*
- *awdurdodau eraill, megis yr Awdurdod Addysg Lleol ac ysgolion pan fydd disgyblion yn symud iddynt a lle mae gofynion cyfreithiol*
- *sefydliadau sy'n cydweithredu â'r ysgol neu sy'n rhan o brotocol rhannu gwybodaeth*

8. Hawliau unigolion

8.1 Mynediad at wybodaeth amdanynt eu hunain

Mae gan unigolion hawl i ofyn am gopi o'r holl wybodaeth sy'n cael ei chadw amdanynt gan yr ysgol, a chyfeirir at hyn yn gyffredinol fel mynediad testun (SAR). Gall yr unigolyn fod yn ddisgybl, yn rhiant neu'n aelod o staff.

Gellir cael mynediad at Ddata Disgyblion mewn dwy ffordd;

Mae Deddfwriaeth Diogelu Data 2018 yn rhoi hawl i ddisgyblion a'r rhai sydd â chyfrifoldeb rhiant, i gael mynediad at ddata personol.

(i) Darparu data i blant

SAR - Mewn perthynas â gallu plentyn i wneud cais, mae'r canllawiau a ddarperir gan yr ICO yn nodi, erbyn i blentyn fod yn 12 oed, bod disgwyl iddynt fod yn ddigon aeddfed i ddeall natur y cais. Wrth gwrs, gall plentyn fod yn ddigon aeddfed cyn hynny; a dylid pennu hynny fesul achos.

Os nad yw'r plentyn yn deall natur y cais, mae rhywun sydd â chyfrifoldeb rhiant am y plentyn, neu warcheidwad, yn meddu ar yr hawl i wneud cais ar ran y plentyn a derbyn ymateb.

(ii) Hawliau rhieni

SAR - Gall oedolyn sydd â chyfrifoldeb rhiant gael mynediad at y wybodaeth am eu plentyn, os ystyrir nad yw'r plentyn eto'n ddigon aeddfed. Rhaid iddynt fedru profi eu cyfrifoldeb fel rhiant ac mae gan yr Ysgol hawl i ofyn am y ddogfennaeth briodol i brofi hyn yn ogystal â phrawf o bwy yw'r person sy'n gwneud y cais a phwy yw'r plentyn. Gall plentyn sydd â'r gallu i ddeall wrthod cytuno i gais y rhieni am ei gofnodion. Dylai Pennaeth yr ysgol drafod y cais gyda'r plentyn ac ystyried ei farn wrth wneud penderfyniad. Os penderfynir nad oes gan y plentyn y gallu sydd ei angen, bydd unigolyn sydd â chyfrifoldeb rhiant am y plentyn, neu warcheidwad, yn gwneud y penderfyniad ar ran y plentyn.

Addysgiadol - yn ogystal, mae gan rieni eu hawl annibynnol eu hunain dan Reoliadau Gwybodaeth am Ddisgyblion (Cymru) 2011 i gael mynediad at gofnodion addysgol swyddogol eu plant. Nid oes gan fyfyrwyr hawl i atal eu rhieni rhag cael copi o'u cofnod ysgol.

Gwybodaeth Ychwanegol

Pan dderbynnir cais SAR, rhaid ymdrin ag ef yn brydlon; rhaid cyflwyno ateb cyn gynted â phosib o fewn cyfnod o un mis. Gellir ymestyn y cyfnod o hyd at ddeufis, os yw'r cais yn gymhleth neu'n niferus.

Os pennir bod cais SAR yn afresymol ar y sail ei fod yn amlwg yn ormodol ac yn ddi-sail ('manifestly excessive and unfounded'):
Mae'r term ‘yn amlwg yn ddi-sail’ ('manifestly unfounded') yn cael ei ddiffinio fel un sydd ddim yn ddidwyll ac sydd heb unrhyw wir ddiben. Mae'r term ‘gormodol’ ('excessive') yn cael ei ddiffinio fel cais sydd wedi cael ei gyflwyno yn flaenorol.
Os mai dyma yw'r achos, gall yr Ysgol wrthod ymateb i SAR ond mae'n rhaid iddi fedru arddangos pam fod y cais yn ddi-sail neu’n ormodol.

Rhaid ymateb i Geisiadau am Gofnodion Addysgol ymhen 15 diwrnod ysgol o dderbyn cais ysgrifenedig gan riant.

Gall yr ysgol godi tâl am ddarparu'r wybodaeth, yn ddibynnol ar yr isod:
• Os yw'r wybodaeth y gofynnir amdani yn cynnwys y cofnod addysgol, bydd y ffi a godir yn ddibynnol ar nifer y tudalennau a ddarperir.
• Pe bai'r wybodaeth y gofynnir amdani yn wybodaeth bersonol, nad yw'n cynnwys unrhyw wybodaeth sydd wedi'i chynnwys mewn cofnodion addysgol, ni chodir ffi.
• Os yw'r cais ond yn gofyn am y cofnod addysgol, bydd modd ei weld am ddim, ond gall Pennaeth yr Ysgol godi ffi i dalu am gost llungopïo'r wybodaeth. Gellir codi ffi o hyd at £50, ar raddfa symudol, am gopïau o gofnod addysgol disgybl.

Wrth ddarparu gwybodaeth, rhaid i'r ysgol hefyd ddarparu'r un manylion i'r unigolion hynny a'r rhai ddarparwyd mewn hysbysiad preifatrwydd.

8.2 Yr hawl i wneud cais bod gwybodaeth anghywir yn cael ei chywiro

Mae gan bob unigolyn yr hawl i hysbysu'r ysgol os ydyw o'r farn fod y wybodaeth amdanynt wedi cael ei chofnodi'n anghywir.

Efallai na fydd modd newid neu ddileu'r wybodaeth ar bob achlysur, ond dylid cywiro unrhyw beth sy'n ffeithiol anghywir;

Yn y cyfamser, dylid rhoi hysbysiad ar ffeil y person yn nodi bod amheuaeth am ei chywirdeb.

8.3 Yr hawl i wneud cais i wybodaeth gael ei dileu

Mae gan bob unigolyn, mewn rhai amgylchiadau, yr hawl i wneud cais i ddileu gwybodaeth amdano ei hun. Bydd yr ysgol yn ystyried pob cais ar sail unigol.

8.4 Yr hawl i wrthwynebu neu i gyfyngu ar y prosesu

Mae gan bob unigolyn yr hawl i wrthwynebu i'w gwybodaeth gael ei phrosesu dan yr amgylchiadau a ganlyn:

- Mae'r wybodaeth yn cael ei phrosesu ar sail tasg gyhoeddus neu fuddiant dilys;
- Lle mae marchnata uniongyrchol;
- Prosesu yn sgil gwaith ymchwil neu ystadegau.

Bydd yr ysgol yn cydymffurfio â'r cais oni bai:

- Bod rhesymau cryf a chyfreithlon dros brosesu;
- Mae angen sefydlu, gweithredu neu amddiffyn hawliadau cyfreithiol.

O ran cyfyngu ar brosesu, mae hawl i wneud hynny os;

- yw unigolion yn daer fod y data yn anghywir ac felly, rhaid cyfyngu arno yn ystod yr ymchwiliad
- oes unigolion wedi gwrthwynebu;
- yw'r prosesu yn anghyfreithiol a
- lle nad yw'r ysgol angen y data ond mae unigolion ei angen er mwyn amddiffyn hawliad cyfreithiol.

Bydd angen hysbysu unrhyw drydydd parti sydd wedi derbyn y data o'r angen i gyfyngu ar y prosesu, ac i hysbysu'r unigolion pwy yw'r trydydd bartïon hyn.

9. Diogelwch

9.1 Cofnodion papur

Lle bynnag y bo'n bosib, dylid defnyddio ystafelloedd storio, cabinetau cryf, a systemau storio diogel eraill y gellir eu cloi, i storio cofnodion papur. Ni ddylid gadael papurau sy'n cynnwys gwybodaeth bersonol gyfrinachol ar ddesgiau mewn swyddfeydd ac ystafelloedd dosbarth, ar fyrddau ystafelloedd staff nac wedi'u gosod ar hysbysfyrddau lle mae modd i unrhyw un eu gweld. Dylid cymryd gofal penodol os oes rhaid mynd â'r dogfennau o'r ysgol.

9.2 Cofnodion Electronig

Dylid cadw pob dyfais cludadwy electronig mor ddiogel â phosib. Os oes gwybodaeth bersonol ynddynt, dylid eu cadw dan glo oni bai eu bod yn cael eu defnyddio.

Dylid defnyddio meddalwedd amgryptio i amddiffyn pob dyfais gludadwy a chyfryngau symudadwy, megis gliniaduron a dyfeisiadau USB (neu ffurf arall i gadw gwybodaeth nad ydyw'n rhan o'r cyfrifiadur ei hun), sy'n cadw gwybodaeth bersonol a chyfrinachol. Rhaid i bob dyfais gael ei diogelu gan gyfrinair.

Rhaid cael gwared ar ddata yn ddiogel cyn gynted ag y caiff ei drosglwyddo neu phan nad oes ei angen mwyach.

Dylid annog defnyddio cyfrineiriau cryf, h.y. o leiaf wyth nod a chynnwys symbolau arbennig os yw unrhyw gyfarpar electronig yn dal gwybodaeth bersonol gyfrinachol. Ni ddylid rhannu cyfrineiriau o gwbl a dylid defnyddio cyfrineiriau gwahanol ar gyfer systemau a dyfeisiau gwahanol.

Mae'n hanfodol fod yr awdurdodaethau mynediad cywir ar gyfer ffeiliau a systemau yn eu lle, a dylid gwirio a diweddaru'r awdurdodaethau hynny yn rheolaidd.

9.3 E-bost

Dylid anfon busnes swyddogol yr ysgol drwy ddefnyddio cyfrif e-bost swyddogol yr ysgol. Ni ddylid defnyddio cyfrifon e-bost personol i ymgymryd â busnes swyddogol yr ysgol nac i gefnogi'r gwaith hwnnw,

Dylai gohebiaeth e-bost fod yn broffesiynol a dylid cymryd gofal arbennig gyda chynnwys yr e-bost a gwirio pwy yw'r derbynyddion er mwyn lleihau'r risg o dorri rheolau diogelwch data.

9.4 Dyfeisiau Symudol

Yr Ysgol, fel y Rheolydd Data, sy'n parhau i reoli'r Data Ysgol swyddogol sy'n cael ei storio ar ddyfeisiau symudol personol, waeth pwy fo perchennog y ddyfais.

Ni ddylid defnyddio dyfeisiau Symudol Personol oni bai y pennir fod hyn yn gwbl angenrheidiol. Dylid rhannu unrhyw wybodaeth bersonol a gofnodir ar y ddyfais dan sylw gyda'r Ysgol a dylid cadarnhau fod y wybodaeth wedi'i dileu.

10. Tor-rheolau Data

Mae tor-rheolau data yn golygu bod gwybodaeth bersonol wedi cael ei chyfaddawdu neu ei cholli, a allai fod wedi digwydd o ganlyniad i ddigwyddiad seibr; data wedi ei adael mewn lleoliad anniogel; data wedi ei bostio at y derbynyddion anghywir; colli neu ddwyn gwaith papur neu ddyfais anniogel, ac ati.

Rhaid i'r ysgol adrodd am unrhyw dor-rheolau data i'r Swyddog Diogelu Data Ysgolion (SDD) ar unwaith.
Bydd y SDD yn ymchwilio ac yn cymryd unrhyw gamau adferol priodol.
Rhaid adrodd am dor-rheolau data difrifol i Swyddfa'r Comisiynydd Gwybodaeth o fewn 72 awr o ganfod y tor-rheol.

11. Cadw Data a Rheoli Cofnodion

Dylid cadw cofnodion mewn modd fel y gallai'r unigolyn dan sylw eu hymchwilio. Dylid hefyd gadw mewn cof ei bod yn bosib y bydd y llysoedd neu unrhyw swyddog cyfreithiol yn ymchwilio'r data rywdro yn y dyfodol. Felly, dylai fod yn gywir, diduedd, diamwys ac yn hawdd ei ddehongli/darllen.

Pan geir gwybodaeth gan ffynhonnell allanol, dylid cofnodi manylion y ffynhonnell a'r dyddiad y derbyniwyd y wybodaeth.

Dylid ond cadw gwybodaeth cyn hired ag y bo angen, ar gyfer dibenion cyfreithiol neu fusnes.

Os cedwir unrhyw wybodaeth gyfrinachol ar gofnodion papur, dylid eu llarpio;
Dylid dileu neu ddinistrio atgofion electronig.

12. Gwefan/Cyfryngau Cymdeithasol

Bydd unrhyw berson sydd â'u manylion, neu fanylion plentyn, i'w cynnwys ar wefan yr ysgol neu ar safleoedd cyfryngau cymdeithasol yr ysgol angen rhoi caniatâd ysgrifenedig.

Bydd y caniatâd yn cael ei gofnodi'n briodol, gan gynnwys y dyddiad y rhoddwyd y caniatâd ac enw'r sawl a roddodd y caniatâd, gan ddefnyddio system MIS yr ysgol.

Bydd unigolion yn cael gwybod yn iawn am ganlyniadau lledaenu eu data dros y byd.

13. Ffotograffau

Mae'n bosib y bydd ffotograffau a dynnir er defnydd ysgol swyddogol wedi'u cynnwys gan y DDD a bydd yr Ysgol yn dweud wrth ddisgyblion a staff pam eu bod yn cael eu tynnu.

Mae ffotograffau a dynnir er defnydd personol yn unig wedi'u heithrio o'r DDD.

Bydd ffurflen ganiatâd ar gyfer ffotograffau yn cael ei chyflwyno fel rhan o'r gwaith papur mynediad i ysgolion.

Bydd y caniatâd yn cael ei gofnodi'n briodol, gan gynnwys y dyddiad y rhoddwyd y caniatâd ac enw'r sawl a roddodd y caniatâd, gan ddefnyddio system MIS yr ysgol.

14. Rhannu Gwybodaeth

Wrth rannu gwybodaeth bersonol, bydd yr ysgol yn sicrhau bod:

- ganddi'r hawl i'w rhannu;
- diogelwch digonol (gan gymryd natur y wybodaeth i ystyriaeth) yn ei le i'w amddiffyn; ac
- yn darparu amlinelliad mewn hysbysiad preifatrwydd am bwy sy'n derbyn gwybodaeth bersonol gan yr ysgol.

Bydd unrhyw ddata personol a anfonir at drydydd parti er prosesu (cwmni allanol) wedi'i gynnwys dan gytundeb prosesu data.

Bydd angen cwblhau DPIA (asesiad risg) CYN defnyddio unrhyw gwmni newydd a/neu CYN cychwyn unrhyw fath newydd o brosesu. Bydd yr asesiad yn nodi risgiau ac yn nodi mesurau lliniaru ar gyfer y risgiau hynny. Dylid anfon yr asesiad risg at y Swyddog Diogelu Data Ysgolion er mwyn ei awdurdodi.

Nid yw GDPR y DU yn eich atal rhag rhannu data personol gydag awdurdodau gorfodi'r gyfraith (a adwaenir dan gyfraith diogelu data fel "awdurdodau cymwys"), sy'n gweithredu eu swyddogaethau gorfodi'r gyfraith statudol. Os bydd cais am wybodaeth yn cael ei dderbyn gan yr Heddlu, yna dylai hefyd gynnwys ffurflen SA3 wedi'i chwblhau sy'n cynnwys yr holl wybodaeth berthnasol. Dylid anfon y cais ymlaen at y Swyddog Diogelu Data Ysgolion er mwyn ei awdurdodi.

15. Torri'r polisi

Gall methiant aelodau staff i gydymffurfio â gofynion y DDD arwain at drydydd partïon yn cymryd camau difrifol yn erbyn awdurdodau'r ysgol. Felly, mae diffyg cydymffurfiaeth gan aelod o staff yn cael ei ystyried fel mater disgyblu a all, yn ddibynnol ar yr amgylchiadau, arwain at ddiswyddiad. Dylid nodi y gall unigolyn gyflawni trosedd o dan y Ddeddf, er enghraifft, gan gael gafael ar/neu ddatgelu data personol er ei (d)dibenion ef/hi ei hun heb ganiatâd y rheolydd data.

16. Cwynion

Dylid cyflwyno cwynion am y gweithdrefnau uchod i Gadeirydd y Corff Llywodraethu fydd yn penderfynu a yw hi'n briodol ymdrin â'r gŵyn yn unol â threfn gwyno'r ysgol ai peidio. Bydd y Comisiynydd Gwybodaeth yn ymdrin â chwynion nad yw hi'n briodol i ymdrin â hwy drwy drefn gwyno'r ysgol. Bydd manylion cyswllt y ddau yn cael eu cynnwys gyda'r wybodaeth sy'n cael ei datgelu.

17. Cysylltiadau

Os oes gennych unrhyw ymholiadau neu bryderon ynghylch y polisïau / gweithdrefnau hyn, cysylltwch â Phennaeth yr ysgol yn y lle cyntaf, neu â'r Swyddog Diogelu Data Ysgolion.

Gellir dod o hyd i ragor o gyngor a gwybodaeth gan Swyddfa'r Comisiynydd Gwybodaeth ('ICO'), www.ico.gov.uk

18. Adnoddau Defnyddiol

Pecyn penodol ar gyfer ysgolion gan Swyddfa'r Comisiynydd Gwybodaeth: https://ico.org.uk/for-organisations/education/

Hwb: https://hwb.gov.wales/resources/resource/def9bffd-1fba-4902-9834-3ecca60bb7e7/cy

1. Introduction

In order to operate efficiently, the School has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, pupils and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government.

The school is committed to ensuring that personal information is properly managed and that it ensures compliance with data protection legislation. 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.

Definitions

Personal Data is information which relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in
structured files that tells you something about an identifiable living individual.
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 and staff development reviews.

Special Category Data is information that relates to race and ethnicity, political opinions, religion, trade union membership, health, genetics, sexuality, sex life, and biometric data.
The difference between processing personal data and special category data is that there are greater legal restrictions on the latter as they are more sensitive.

Criminal Data - Article 10 of the General Data Protection Regulation (GDPR) sets out the regulations to process criminal data.

2. Scope

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

This policy applies to all personal information created or held by the School in whatever format (e.g. paper, electronic, email, film) and however it is stored, (for example ICT system/database, sharepoint site, shared drive filing structure, email, filing cabinet, personal filing shelves, drawers and mobile devices including mobile phones CCTV).
Any information created by the School and it's staff becomes the property of the school.
Data Prptection Legislation (DPL) does not apply to access to information about deceased individuals.

3. Responsibilities

The Governors have overall responsibility for compliance with DPL.

The Headteacher is responsible for ensuring compliance with DPL and this policy within the day to day activities of the school. The Headteacher is responsible for ensuring that appropriate training is provided for all staff.

All members of staff or contractors who hold or collect personal data are responsible for their own compliance with DPL and must ensure that personal information is kept and processed in line with DPL.

All members of staff should demonstrate that they have read, understood and accepted this Policy.

4. The Requirements

DPL stipulates that anyone processing personal data must comply with six principles of good practice; these principles are legally enforceable.

In the context of personal information:

Article 5(1) GDPR states that personal data;

a. should be processed in a legal, fair and transparent manner
b. should only be acquired for one or more specific, clear and lawful purposes, and it should not be further processed in any manner incompatible with that purpose or those purposes;
c. will be adequate, relevant and non-excessive in relation to the purpose or purposes for which it is processed;
d. will be accurate, and where appropriate, completely up-to-date;
e. should not be kept for longer than needed for that purpose or those purposes;
f. will be processed safely, i.e. protected by an appropriate degree of security.

As Data Controller, the school, are required to maintain a Record of processing activities/Asset Register containing;

- Description of the categories of Personal Data and Categories of Data Subjects
- The purposes of the processing
- The categories of recipients to whom personal data have been or will be disclosed

The School is required to pay an annual fee to the Information Commissioner's Office (ICO).
Failure to do so could lead to a financial penalty.

5. Privacy Notices

Whenever information is collected about individuals, the school will provide the following information:

- The identity of the data controller, e.g. the school;
- 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;
- With who the information will or may be shared with;
- How long the information is kept
- Details about the rights of individuals
- Details about the Data Protection Officer

This must happen at the time that information first starts to be gathered on an individual.

If information is collected directly from a child, the privacy notice must be presented in clear, plain, age appropriate language.

6. Conditions for Processing

Processing of personal information may only be carried out where one of the conditions of Article 6, GDPR has been satisfied.
Processing of special category data may only be carried out if a condition in Article 9, GDPR is met as well as one in Article 6.

7. Disclosure of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause.

- The school should 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.

- Where there is doubt or statutory requirements conflict, advice should be sought.

- When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if they are related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled.

Relevant, confidential data should only be given to:

- *other staff members on a need to know basis;*
- *relevant parents/guardians; 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 or that are part of an information sharing protocol*

8. Individuals' rights

8.1 Access to information about themselves

Individuals have the right, to request a copy of all information retained about them by the school which is commonly referred to as subject access (SAR). The individual may be a pupil, a parent or a staff member.

Accessing Pupil Data can be done in two ways;

The data Protection Legislation 2018 gives pupils and those with parental responsibility the right of access to personal data.

(i) Provision of data to children

SAR - In relation to the capacity of a child to make a request, guidance provided by the ICO states that by the age of 12 a child can be expected to have sufficient maturity to understand the nature of the request. A child may of course reach sufficient maturity earlier; each child should be judged on a case by case basis.

If the child does not understand the nature of the request, someone with parental responsibility for the child, or a guardian, is entitled to make the request on behalf of the child and receive a response.

ii. Parents' rights

SAR - An adult with parental responsibility can access the information about their child, provided that the child is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the School is entitled to request relevant documentation to evidence this as well as the identities of the person making the request and the child.
A child with competency to understand can refuse to consent to the parents request for their records. The Headteacher should discuss the request with the child and take their views into account when deciding. Where the child is not deemed to be competent, an individual with parental responsibility or guardian shall make the decision on behalf of the child.

Educational - Parents have their own independent right under The Pupil Information (Wales) Regulations 2011 to inspect the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their school records.

Additional Information

When a SAR request is received, it must be dealt with promptly; an answer must be presented as soon as possible within a month. The period can be extended by up to two months if a request is complex or numerous.

If a SAR request may be deemed unreasonable on the grounds it is 'manifestly excessive and unfounded.
The term 'manifestly unfounded' is defined as not being genuine and with no real purpose. The term 'excessive' is defined as a request that has been submitted previously
If this is the case, the School can refuse to respond to a SAR but must be able to demonstrate why the request is unfounded or excessive.

Requests for Educational Records must be answered within 15 school days of receiving a written request by a parent.

The school may make a charge for the provision of information, dependent upon the following:
• Should the information requested contain the educational record, then the amount charged will be dependent upon the number of pages provided.
• Should the information requested be personal information that does not include any information contained within educational records, no fee is charged
• if the information requested is only the educational record, viewing will be free, but a charge for the cost of photocopying the information can be made by the Headteacher. A fee of up to £50, on a sliding scale may be charged for copies of a pupil's educational record.

When providing information, the school must also provide the same details to the individuals as those provided in a privacy notice.

8.2 The right to request that inaccurate information is corrected

Every individual has the right to inform the school if they believe that information about them has been recorded incorrectly.
It may be possible that one will be unable to change or delete the information on every occasion, but anything that is factually incorrect should be corrected;
In the meantime, a notice should be placed on the person's file to note that there is doubt regarding accuracy.

8.3 The right to request that information is deleted

Every individual, in some circumstances, has the right to make a request to delete information about themselves. The school will consider every request on an individual basis.

8.4 The right to object to or restrict processing

Every individual has the right to object to their information being processed under the following circumstances:

- Information is being processed on the basis of public task or legitimate interests;
- Where there is direct marketing;
- Processing due to research or statistics.

The school will comply with the request unless:

- There are strong, lawful reasons for processing;

- There is a need to establish, exercise or defend legal claims.

In terms of limiting processing, there is a right to do so if;

- Individuals insist that data is incorrect and therefore, it must be limited during the investigation
- Individuals have objected;
- processing is illegal and
- where the school does not require the data but individuals require it in order to defend a legal claim.

There will be a 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.

9. Security

9.1 Paper records

Whenever possible, storage rooms, strong cabinets, and other lockable storage systems should be used to store paper records. Papers containing confidential 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 school

9.2 Electronic Records

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 laptops and USB devices (or another form of memory storage not part of the computer itself), which hold confidential personal information. All devices must be password protected.
Data must be disposed of securely once it has been transferred or is no longer required.

Strong passwords, i.e. at least eight characters long and containing special symbols, should be encouraged if any electronic equipment holds confidential personal information.Passwords should never be shared and different passwords should be used for separate systems and devices.

It is crucial that the correct access permissions for files and systems are in place with said permissions being checked and updated regularly.

9.3 E-Mail

Official School business must be sent using an official School e-mail account. Personal e-mail accounts must never be used to conduct or support official School business,

E-mail communication should be professional with special care given to the content of the email and checks made of recipients to reduce the risk of a data security breach.

9.4 Mobile Devices

The School, as Data Controller, remain in control of official School Data stored on personal mobile devices regardless of the ownership of the device.

Personal Mobile devices should not be used unless deemed completely necessary. Any personal information recorded on said device should be shared with the School and deletion confirmed.

10. Data Breach

A data breach means that personal information has been compromised or lost which could be as a result of a cyber incident; data left in insecure location; data posted to the wrong recipient; loss or theft of paperwork or insecure device etc.

The school must report any data breaches to the Schools Data Protection Officer (DPO) immediately
The DPO will investigate any and take appropriate remedial action.
Serious data breaches must be reported to the Information Commissioner's Office within 72 hours of identifying the breach.

11. Data Retention and Records Management

Records should be kept in such a way that the individual concerned can inspect them. It should also be borne in mind that at some time in the future the data may be inspected by the courts or any legal official. 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.

Information should only be kept as long as needed, for legal or business purposes.

If any confidential information is held on paper records, they should be shredded;
Electronic memories should be erased or destroyed.

12. **Website/Social Media**

Any person whose details, or child's details, are to be included on the school's website or school social media sites will be required to give written consent.

The consent will be recorded appropriately including date given and name of consent giver using the schools MIS system.

Individuals will be properly informed about the consequences of their data being disseminated worldwide.

13. Photographs

Photos taken for official school use may be covered by DPL and the School will advise pupils and staff why they are being taken.

Photos taken purely for personal use are exempt from DPL.

A consent form for photographs will be issued as part of the admissions paperwork.

The consent will be recorded appropriately including date given and name of consent giver using the schools MIS system.

14. **Sharing Information**

When sharing personal information, the school will ensure that:

- it is allowed to share it;
- adequate security (taking into account the nature of the information) is in place to protect it; and
- it will provide an outline in a privacy statement of who receives personal information from the school.

Any personal data passed to a third party for processing (namely an external company) will be covered by a data processing agreement.

DPIA (risk assessment) will need to be completed BEFORE using any new company and / or BEFORE initiating any new type of processing. The assessment will identify risks and identify mitigation measures for those risks. The risk assessment should be sent to the School Data Protection Officer for authorization. See Appendix 5 example.

The UK GDPR does not prevent you sharing personal data with law enforcement authorities (known under data protection law as “competent authorities”) who are discharging their statutory law enforcement functions. If a request for information from the Police is received it should be accompanied by a completed SA3 form containing all relevant information. The request should be forwarded to the School Data Protection Officer for authorisation.

15. Breach of the policy

Non-compliance with the requirements of DPL by the members of staff could lead to serious action being taken by third parties against the school authorities. Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal. It should be noted that an individual can commit a criminal offence under the Act, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the data controller.

16. **Complaints**

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school’s complaint procedure. Complaints which are not appropriate to be dealt with through the school’s complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

17. **Contacts**

If you have any queries or concerns regarding these policies / procedures then please contact the Headteacher in the first instance or the Schools Data Protection Officer.

Further advice and information can be obtained from the Information Commissioner’s Office ('ICO'), www.ico.gov.uk

18. **Useful Resources**

A pack specifically for schools from the Information Commissioner's Office:
https://ico.org.uk/for-organisations/education/

Hwb, National resources on on-line safety:
https://hwb.gov.wales/resources/resource/def9bffd-1fba-4902-9834-3ecca60bb7e7/cy