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

Ysgol Syr Hugh Owen

Llofnodwyd ar ran Cadeirydd y Llywodraethwyr:
Signed on behalf of the Chair of Governors:

Dyddiad Cymeradwyo: 06/03/2025

Dyddiad Adolygu: 06/03/2028

Cynnwys:

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.

Gweler rhestr o'r amodau yn Atodiad 1.

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.

Gweler manylion pellach ar sut i ymdrin â'r ceisiadau hyn yn Atodiad 2.

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, gan ddefnyddio' r ddogfen berthnasol yn Atodiad 3.
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.

Gweler y cyfnodau cadw perthnasol ar gyfer cofnodion ysgol yn Atodiad 4.

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. Gweler enghraifft o ffurflen ganiatâd yn Atodiad 6.

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. Gweler enghraifft Atodiad 5.

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. Teledu Cylch Cyfyng (TCC)

Mae dal a/neu gofnodi delweddau o unigolion y gellir eu hadnabod yn enghraifft o brosesu gwybodaeth bersonol ac felly mae angen cydymffurfio â'r DDD.

Bydd yr ysgol yn hysbysu staff, disgyblion ac ymwelwyr am y rheswm y mae'n casglu gwybodaeth bersonol ar ffurf delweddau TCC.
Bydd yr ysgol yn sicrhau fod ganddi gyfnod cadw penodol yn seiliedig ar yr angen posib i adolygu'r delweddau a bydd yn ystyried pwy sydd yn cael mynediad at y delweddau hyn a pham.

Bydd gan unigolion ac asiantaethau gorfodi'r gyfraith yr hawl i ofyn am weld y delweddau. Bydd holl geisiadau o'r fath yn cael eu cofnodi.

Gweler yma ganllaw Swyddfa'r Comisiynydd Gwybodaeth ar TCC:

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

16. Gwybodaeth Biometrig (olion bysedd) - DEWISOL

Mae Deddf Diogelu Rhyddidau 2012 yn cynnwys mesurau sy'n ymwneud â defnyddio systemau adnabod biometrig, h.y. systemau olion bysedd ac adnabod wynebau (*facial recognition*).
Dan y GDPR, cydnabyddir bod y math hwn o ddata yn ddata categori arbennig.

- Ar gyfer bob disgybl ysgol o dan 18 mlwydd oed, bydd yr ysgol yn gofyn am ganiatâd ysgrifenedig y rhieni cyn cofnodi a phrosesu manylion biometrig eu plentyn.
- Rhaid i holl ddata o'r fath gael ei drin yn briodol ac yn unol ag egwyddorion y DDD.
- Rhaid adnabod dulliau eraill o ddarparu gwasanaeth os yw rhiant neu ddisgybl yn gwrthod rhoi caniatâd.

Darperir ffurflen ganiatâd ar gyfer gwybodaeth biometrig yn Atodiad 7.

17. 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.

18. 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.

19. 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

20. 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

Atodiad 1

Amodau Erthygl 6 (crynodeb)

6(1)(a) – Caniatâd yr unigolyn;
6(1)(b) – Prosesu yn angenrheidiol ar gyfer contract;
6(1)(c) – Prosesu yn angenrheidiol i gydymffurfio â dyletswydd gyfreithiol;
6(1)(d) – Prosesu yn angenrheidiol er budd hanfodol yr unigolyn;
6(1)(e) - Prosesu yn angenrheidiol am ei fod yn ymgymryd â thasg sydd er budd cyhoeddus
6(1)(f) - Prosesu yn angenrheidiol ar gyfer buddion cyfreithlon y rheolwr data neu drydydd parti

Amodau Erthygl 9 (crynodeb)

9(2)(a) – Prosesu gyda chaniatâd penodol yr unigolyn;
9(2)(b) – Prosesu yn angenrheidiol o dan gyfraith cyflogaeth;
9(2)(c) – Prosesu yn angenrheidiol er mwyn amddiffyn budd hanfodol yr unigolyn;
9(2)(d) -Prosesu at ddefnydd grŵp categori arbennig (Sefydliad dielw gyda nôd wleidyddol, crefyddol neu undeb llafur);
9(2)(e) – Prosesu'n perthyn i wybodaeth wedi ei wneud yn gyhoeddus gan yr unigolyn;
9(2)(f) – Prosesu yn angenrheidiol i'r sefydliad amddiffyn hawliadau cyfreithiol;
9(2)(g) – Prosesu yn angenrheidiol er budd cyhoeddus sylweddol wedi ei seilio ar gyfraith;
9(2)(h) – Prosesu yn angenrheidiol ar gyfer ymateb i anghenion Iechyd Galwedigaethol a Gofal Cymdeithasol;
9(2)(i) – Prosesu'n angenrheidiol am resymau Iechyd Cyhoeddus;
9(2)(j) – Prosesu yn angenrheidiol ar gyfer pwrpas Archifol er budd y Cyhoedd; neu ar gyfer pwrpas ymchwil gwyddonol neu hanesyddol; neu i bwrpas ystadegol.

Mae rhagor o amodau Categori Arbennig yn Atodlen 1 Deddf Diogelu Data 2018.

Atodiad 2

Hawl i gael Mynediad at wybodaeth
Mae dau fath penodol o hawl i gael mynediad at wybodaeth a ddelir gan ysgolion am fyfyrwyr.
1. O dan y GDPR a Ddeddf Diogelu Data 2018, mae gan unrhyw unigolyn yr hawl i wneud cais i weld y wybodaeth bersonol a gedwir amdanynt.
2. Hawl y rhai hynny sydd â hawl i gael mynediad at gofnodion cwricwlaidd ac addysgol fel y'i diffinnir o fewn Rheoliadau Addysg (Gwybodaeth am Ddisgyblion) (Cymru) 2004.

Gweithredu cais
1) Gellir gwneud ceisiadau yn ysgrifenedig, drwy e-bost neu ar lafar. Os nad yw'r cais cyntaf yn adnabod y wybodaeth sydd ei angen yn glir, yna gwneir ymholiadau pellach.

2) Mae'n rhaid cael prawf o bwy yw'r sawl sy'n gofyn cyn datgelu unrhyw wybodaeth, a dylid cynnal gwiriadau ynghylch profi eu perthynas i'r plentyn.

Gellir profi pwy yw'r person trwy ofyn iddynt:

- Pasbort
- trwydded yrru
- biliau gwasanaeth gyda'r cyfeiriad presennol
- Tystysgrif Priodas / Geni
- P45/P60
- Datganiad Morgais neu Gerdyn Credyd

Nid yw'r rhestr yn gyflawn.
3) Mae gan bawb hawl i gael mynediad at wybodaeth a gedwir amdanynt. Fodd bynnag, o ran plant, mae hyn yn ddibynnol ar eu gallu i ddeall ac ar natur y cais (12 oed neu hŷn fel arfer). Dylai'r Pennaeth Ysgol drafod y cais gyda'r plentyn ac ystyried ei farn wrth wneud penderfyniad. Gall plentyn sydd â'r gallu i ddeall, wrthod cytuno i'r cais am ei gofnodion. 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.

4) Gall yr ysgol godi am ddarparu'r wybodaeth, yn ddibynnol ar yr hyn a ganlyn:

- Os yw'r wybodaeth y gofynnir amdani'n 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 rhywun ond yn gofyn am y cofnod addysgol, bydd modd ei weld am ddim, ond bydd y Pennaeth Ysgol yn codi ffi i dalu am gost llungopïo'r wybodaeth.

5) Y cyfnod a ganiateir i ymateb i gais, wedi iddo gael ei dderbyn yn ffurfiol, yw un mis **(nid dyddiau gwaith na dyddiau ysgol, ond dyddiau calendr, heb ystyried cyfnod gwyliau ysgol)**. Fodd bynnag, ni fydd y mis yn dechrau hyd y derbynnir y ffioedd neu eglurhad o'r wybodaeth y gofynnir amdani.

Os credir bod y cais yn gymhleth neu mae nifer o geisiadau, bydd yr ysgol yn hysbysu'r ymgeisydd o fewn un mis fod cyfnod y cais yn mynd i gael ei ymestyn a'r rheswm pam. Caniateir hyd at dau fis yn ychwanegol i ateb y cais o dan amgylchiadau o'r math.

Os yw ceisiadau yn amlwg yn ddi-sail neu'n ormodol (yn arbennig os ydynt yn rhai ailadroddus), bydd yr ysgol yn codi ffi rhesymol am y costau gweinyddol neu yn gwrthod delio efo'r cais.

6) Mae DDD yn caniatáu eithriadau o ran darparu gwybodaeth benodol; **felly bydd yr holl wybodaeth yn cael ei hadolygu cyn ei datgelu**.

7) Mae gwybodaeth trydydd parti yn wybodaeth sydd wedi cael ei darparu gan eraill, megis yr Heddlu, yr Awdurdod Lleol, gweithiwr proffesiynol Gofal Iechyd neu ysgol arall. Fel arfer, rhaid cael caniatâd cyn datgelu gwybodaeth gan drydydd parti. Mae angen cadw at yr amserlen yr un fath.

8) Ni ddylid datgelu unrhyw wybodaeth all beri niwed sylweddol i iechyd corfforol neu feddyliol neu gyflwr emosiynol y disgybl nac unrhyw unigolyn arall. Ni ddylid ychwaith ddatgelu gwybodaeth fyddai'n dangos fod y plentyn mewn peryg o gael ei gam-drin, neu unrhyw wybodaeth sy'n ymwneud ag achosion llys.

9) Dylid ceisio mwy o gyngor os oes unrhyw bryder ynghylch datgelu gwybodaeth.

10) Pan fo gwybodaeth wedi cael ei golygu (ei duo neu ei dileu), dylid cadw copi cyflawn o'r wybodaeth a ddarparwyd i sefydlu beth gafodd ei olygu a pham, rhag ofn i rywun gyflwyno cwyn.

11) Dylai'r wybodaeth a ddatgelir fod yn eglur, felly bydd angen egluro unrhyw godau neu dermau technegol. Os yw'r wybodaeth a gynhwysir yn anodd i'w darllen neu'n annarllenadwy, dylid ei theipio eto.

12) Gellir darparu gwybodaeth yn yr ysgol gydag aelod staff ar gael i helpu ac egluro materion pe bai angen, neu gellid ei ddarparu wrth drosglwyddo'r wybodaeth wyneb yn wyneb. Dylid ystyried barn yr ymgeisydd wrth benderfynu sut i ddarparu'r wybodaeth. Os oes rhaid defnyddio systemau'r post yna rhaid defnyddio post cofrestredig.

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 gweithdrefn gwynion yr ysgol ai peidio. Bydd y Comisiynydd Gwybodaeth yn ymdrin â chwynion nad ydynt yn briodol i gael eu hystyried dan weithdrefn gwynion yr ysgol. Bydd manylion cyswllt y ddau yn cael eu cynnwys gyda'r wybodaeth sy'n cael ei datgelu.

Cysylltiadau
Os oes gennych unrhyw ymholiadau neu bryderon ynghylch y polisïau / gweithdrefnau hyn, cysylltwch â'r Pennaeth Ysgol.
Gellir dod o hyd i ragor o gyngor a gwybodaeth gan Swyddfa'r Comisiynydd Gwybodaeth ('ICO'), www.ico.gov.uk

Atodiad 3

Ffurflen Archwilio i achosion o Dorri Rheolau Diogelwch Data

1. Rhaid cwblhau'r ffurflen hon pryd bynnag y bydd diogelwch data personol wedi ei beryglu, fel bod gan yr ysgol dystiolaeth o'r camau y mae wedi eu cymryd i unioni pethau. Gall y camau a gymerir gan yr ysgol gynnwys cyfeirio ei hun i'r Comisiynydd Gwybodaeth. O'r herwydd, mae'n bwysig cwblhau'r ffurflen hon yn gywir fel bod modd rhoi sylw i holl ffeithiau ac amgylchiadau'r achos ac i gymryd camau cadarnhaol i liniaru a gostwng risgiau i unigolion a'r ysgol.

2. Dylid cwblhau'r ffurflen hon ochr yn ochr â'r canllawiau ar gyfer ymchwilio i achosion o dorri diogelwch data a fwriedir i fod o gymorth i'r swyddog fydd yn ymchwilio.

3. Nodwch fod tair rhan i'r ffurflen os gwelwch yn dda.

Rhan A	i'w chwblhau a'i llofnodi gan y **swyddog sy'n ymchwilio**.
Rhan B	i'w chwblhau gan aelod o'r **uwch dim rheoli/Pennaeth**
Rhan C	i'w chwblhau gan y **Swyddog Diogelu Data**

Rhan A
Y swyddog sy'n ymchwilio ddylai gwblhau a llofnodi'r rhan hon.

Amdanoch chi	
• Enw	
• Cyfeiriad E-bost	
• Rhif Ffôn Cyswllt	
Manylion am yr achos o dorri'r rheolau Diogelwch Data	
• Pa bryd y digwyddodd yr achos?	
• Pa bryd y darganfuwyd yr achos?	
• Rhowch grynodeb byr o'r achos os gwelwch yn dda	
• Amlinellwch os gwelwch yn dda beth oedd y data personol.	
• Yn eich barn chi, ydi data personol unrhyw unigolyn wedi ei beryglu o ganlyniad i'r achos?	

○ Pa mor ddifrifol ydi'r risg i'r unigolion?	
• Tua faint o bobl sydd wedi eu heff-eithio?	
• Ydi'r unigolion hyn wedi cael gwybod am yr achos? ○ Os ydynt sut, pa bryd a gan bwy? ○ Os nad ydynt, esboniwch pam os gwelwch yn dda.	
• A gymerwyd unrhyw gamau i os-twng/lleddfu'r effaith ar y bobl a eff-eithir? ○ Rhowch fanylion os gwelwch yn dda.	
• Yn eich barn chi, pa gamau y gellid eu cyflwyno i sicrhau na fyddai'r un peth yn digwydd eto?	
• Oes gennych unrhyw sylwadau pell-ach am yr achos?	
A fyddech cystal â llofnodi a dyddio'r rhan hon. Llofnod:	Dyddiad:

Rhan B

Aelod o'r uwch dim rheoli (neu addasu fel bo'n berthnasol) ddylai gwblhau'r rhan hon.

Amdanoch chi	
• Enw	
• Cyfeiriad E-bost	
• Rhif Ffôn Cyswllt	
Manylion am yr achos o dorri'r Rheolau Diogelwch data	
• Pa gamau y gellir eu cymryd i rwystro achosion tebyg yn y dyfodol? ○ Os yw'n berthnasol, pa bryd ydych yn bwriadu cyflwyno'r newidiadau angenrheidiol i'ch arferion gwaith?	
• Ydych chi'n ystyried bod angen hyfforddi a datblygu unrhyw aelod o'r staff sy'n gysylltiedig â'r achos?	
• Ydych chi'n ystyried bod angen cymryd camau disgyblu?	
A fyddech cystal â llofnodi a dyddio'r rhan hon. Llofnod:	Dyddiad:

Rhan C

Y Swyddog Diogelu Data ddylai gwblhau'r rhan hon.

Nodwch a ddylid cyfeirio'r achos i Swyddfa'r Comisiynydd Gwybodaeth ac a yw'r ymateb i'r achos a nodir yn Rhan B yn gymesur ac yn ddigonol.
Dyddiad ar gyfer adolygu canlyniadau(fel arfer 3 mis ar ôl cwblhau'r ymchwiliad).

Atodiad 4

1. Rheolaeth yr Ysgol

Mae'r adran hon yn cynnwys cyfnodau cadw sy'n gysylltiedig â rheolaeth gyffredinol yr ysgol. Mae hyn yn ymdrin â gwaith y Corff Llywodraethu, y Pennaeth a'r tîm uwch reolwyr, y broses fynediad a gweinyddiaeth weithredol.

1.1 Y Corff Llywodraethu					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
1.1.1	Rhaglenni ar gyfer cyfarfodydd y Corff Llywodraethu	Efallai y bydd materion diogelu data os yw'r cyfarfod yn ymdrin â materion cyfrinachol sy'n ymwneud â staff		Dylid cadw un copi â'r brif gyfres o gofnodion. Gellir gwaredu pob copi arall. Parhaus	GWAREDU'N DDIOGEL[1]
1.1.2	Cofnodion cyfarfodydd y Corff Llywodraethu:	Efallai y bydd materion diogelu data os yw'r cyfarfod yn ymdrin â materion cyfrinachol sy'n ymwneud â staff		Gweler isod	
	Prif Gyfres (wedi'u llofnodi)			PARHAUS	Os nad oes modd i'r ysgol eu storio yna gellir eu cynnig i'r Gwasanaeth Archifau Sirol
	Copïau Archwilio[2]			Dyddiad y cyfarfod + 3 blynedd	Os yw'r cofnodion hyn yn cynnwys unrhyw wybodaeth sensitif, bersonol, rhaid iddynt gael eu llarpio.
1.1.3	Adroddiadau a gyflwynwyd i'r Corff Llywodraethu	Efallai y bydd materion diogelu data os yw'r cyfarfod yn ymdrin â materion cyfrinachol sy'n ymwneud â staff		Dylid cadw adroddiadau am o leiaf 6 blynedd. Fodd bynnag, os yw'r cofnodion yn cyfeirio'n uniongyrchol at adroddiadau unigol, yna dylid cadw'r adroddiadau yn barhaus.	GWAREDU'N DDIOGEL neu gadw â'r copi o'r cofnodion sydd wedi'i lofnodi
1.1.4	Papurau cyfarfod sy'n ymwneud â'r cyfarfod rhieni blynyddol a gynhaliwyd dan adran 33 Deddf Addysg 2002	Nag oes	Deddf Addysg 2002, Adran 33	Dyddiad y cyfarfod + o leiaf 6 blynedd	GWAREDU'N DDIOGEL
1.1.5	Offerynnau'r Llywodraeth yn cynnwys Erthyglau Cyweithio	Nag oes		PARHAUS	Dylid cadw'r rhain yn yr ysgol tra bo'r ysgol ar agor ac yna'u cynnig i'r Gwasanaeth Archifau Sirol pan fo'r ysgol yn cau.

[1] Yn y cyd-destun hwn, dylid ystyried fod GWAREDU'N DDIOGEL yn golygu gwaredu gan ddefnyddio biniau gwastraff cyfrinachol, neu larpio'r wybodaeth gan ddefnyddio llarpiwr sy'n trawstorri os oes cyfleuster o'r fath ar gael yn yr ysgol.

[2] Dyma'r copïau y gallai Clerc y Llywodraethwyr ddymuno ei gadw fel y gall unrhyw un sy'n gwneud cais weld yr holl wybodaeth briodol heb fod angen i'r clerc argraffu a choladu copïau wedi'u golygu o'r cofnodion bob tro y derbynnir cais.

1.1.6	Ymddiriedolaethau a Chynhysgaethau a reolir gan y Corff Llywodraethu	Nag oes		PARHAUS	Dylid cadw'r rhain yn yr ysgol tra bo'r ysgol ar agor ac yna'u cynnig i'r Gwasanaeth Archifau Sirol pan fo'r ysgol yn cau.
1.1.7	Cynlluniau gweithredu a grëwyd ac a weinyddwyd gan y Corff Llywodraethu	Nag oes		Oes y cynllun gweithredu + 3 blynedd	GWAREDU'N DDIOGEL
1.1.8	Dogfennau polisi a grëwyd ac a weinyddwyd gan y Corff Llywodraethu	Nag oes		Oes y polisi + 3 blynedd	GWAREDU'N DDIOGEL
1.1.9	Cofnodion sy'n ymwneud â chwynion yr ymdriniwyd â hwy gan y Corff Llywodraethu	Oes		Dyddiad datrysiad y gŵyn + o leiaf 6 blynedd ac yna adolygu o ran cadw pellach pan fo anghydfod cynhennus	GWAREDU'N DDIOGEL
1.1.10	Adroddiadau Blynyddol a grëwyd yn unol â gofynion yr Deddf Addysg 2002	Nag oes	Deddf Addysg 2002	Dyddiad yr adroddiad + 10 mlynedd	GWAREDU'N DDIOGEL
1.1.11	Cynigion sy'n ymwneud â newid statws ysgol a gynhelir yn cynnwys Ysgolion Statws Arbenigol ac Academïau	Nag oes		Dyddiad derbyn neu wrthod y cynnig + 3 blynedd	GWAREDU'N DDIOGEL

Noder y gellir canfod yr holl wybodaeth am gadw cofnodion sy'n ymwneud â recriwtio Penaethiaid yn yr adran Adnoddau Dynol isod.

1.2 Y Pennaeth a'r Tîm Uwch Reolwyr					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
1.2.1	Llyfrau log o weithgarwch yn yr ysgol yn cael eu cadw gan y Pennaeth (Os yn berthnasol)	Efallai y bydd materion diogelu data os yw'r llyfr log yn cyfeirio at ddisgyblion neu aelodau staff unigol		Dyddiad y cofnod diwethaf yn y llyfr + o leiaf 6 blynedd ac yna adolygu	Gall rhain fod â gwerth hanesyddol parhaol a dylid eu cynnig i'r Gwasanaeth Archifau Sirol os yw'n briodol
1.2.2	Cofnodion cyfarfodydd y Tîm Uwch Reolwyr a chyfarfodydd cyrff gweinyddol mewnol eraill	Efallai y bydd materion diogelu data os yw'r cofnodion yn cyfeirio at ddisgyblion neu aelodau staff unigol		Dyddiad y cyfarfod + 3 blynedd ac yna adolygu	GWAREDU'N DDIOGEL
1.2.3	Adroddiadau a grëwyd gan y Pennaeth neu'r Tîm Uwch Reolwyr	Efallai y bydd materion diogelu data os yw'r adroddiad yn cyfeirio at ddisgyblion neu aelodau staff unigol		Dyddiad yr adroddiad + o leiaf 3 blynedd ac yna adolygu	GWAREDU'N DDIOGEL

1.2.4	Cofnodion a grëwyd gan benaethiaid, dirprwy benaethiaid, penaethiaid blwyddyn ac aelodau staff eraill sydd â chyfrifoldebau gweinyddol	Efallai y bydd materion diogelu data os yw'r cofnodion yn cyfeirio at ddisgyblion neu aelodau staff unigol		Blwyddyn academaidd gyfredol + 6 blynedd ac yna adolygu	GWAREDU'N DDIOGEL
1.2.5	Gohebiaeth a grëwyd gan benaethiaid, dirprwy benaethiaid, penaethiaid blwyddyn ac aelodau staff eraill sydd â chyfrifoldebau gweinyddol	Efallai y bydd materion diogelu data os yw'r ohebiaeth yn cyfeirio at ddisgyblion neu aelodau staff unigol		Dyddiad yr ohebiaeth + 3 blynedd ac yna adolygu	GWAREDU'N DDIOGEL
1.2.6	Cynlluniau Datblygu Proffesiynol	Oes		Oes y cynllun + 6 blynedd	GWAREDU'N DDIOGEL
1.2.7	Cynlluniau Datblygu Ysgol	Nag oes		Oes y cynllun + 3 blynedd	GWAREDU'N DDIOGEL

1.3 Y Broses Fynediad					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
1.3.1	Holl gofnodion sy'n ymwneud â chreu a gweithredu'r Polisi Mynediad Ysgolion	Nag oes	*School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeal panels* Rhagfyr 2014	Oes y polisi + 3 blynedd ac yna adolygu	GWAREDU'N DDIOGEL
1.3.2	Mynediad – os llwyddwyd i gael mynediad	Oes	*School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators*	Dyddiad y mynediad + blwyddyn	GWAREDU'N DDIOGEL

			and admission appeal panels Rhagfyr 2014		
1.3.3	Mynediad – os na lwyddwyd i gael mynediad	Oes	*School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeal panels* Rhagfyr 2014	Datrysiad yr achos + blwyddyn	GWAREDU'N DDIOGEL
1.3.4	Y Gofrestr Fynediad	Oes	*School Attendance: Departmental advice for maintained schools, academies, independent schools and local authorities* Hydref 2014	Rhaid cadw pob cofnod yn y gofrestr fynediad am gyfnod o dair blynedd wedi dyddiad y cofnod[3]	ADOLYGU Efallai y bydd ysgolion yn dymuno ystyried cadw'r gofrestr fynediad yn barhaol gan fod ysgolion yn aml yn derbyn ymholiadau gan gyn-ddisgyblion er mwyn cadarnhau'r dyddiadau pan fuont yn mynychu'r ysgol.
1.3.5	Mynediadau – Ysgolion Uwchradd – Achlysurol	Oes		Y flwyddyn gyfredol + blwyddyn	GWAREDU'N DDIOGEL
1.3.6	Prawf o'u cyfeiriad wedi'i ddarparu gan rieni fel rhan o'r broses fynediad	Oes	*School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators*	Y flwyddyn gyfredol + blwyddyn	GWAREDU'N DDIOGEL

[3] *School Attendance: Departmental advice for maintained schools, academies, independent schools and local authorities* Hydref 2014

			and admission appeal panels Rhagfyr 2014		
1.3.7	Ffurflen Wybodaeth Ategol yn cynnwys gwybodaeth ychwanegol megis crefydd, cyflyrau meddygol, ac ati (e.e. Ffurflen Casglu Gwybodaeth Disgyblion SIMS)	Oes		Gweler isod	
	Os llwyddwyd i gael mynediad			Dylid ychwanegu'r wybodaeth i ffeil y disgybl (e.e. i SIMS / ffeil bapur y disgybl)	GWAREDU'N DDIOGEL
	Os na lwyddwyd i gael mynediad			Hyd nes i'r broses apêl gael ei chwblhau	GWAREDU'N DDIOGEL

1.4 Gweinyddiaeth Weithredol

	Disgrifiad Cyffredinol o'r Ffeil	Materion Diogelu Data	Gofynion Cyfreithiol	Cyfnod Cadw [Gweithredol]	Gweithred ar ddiwedd oes weinyddol y cofnod
1.4.1	Cyfres gyffredinol o ffeiliau	Nag oes		Y flwyddyn gyfredol + 5 mlynedd ac yna ADOLYGU	GWAREDU'N DDIOGEL
1.4.2	Cofnodion yn ymwneud â chreu a chyhoeddi llawlyfr neu brosbectws yr ysgol (Os yn berthnasol)	Nag oes		Y flwyddyn gyfredol + 3 blwyddyn	GWAREDU SAFONOL
1.4.3	Cofnodion yn ymwneud â chreu a dosbarthu cylchlythyrau i staff, rhieni neu ddisgyblion (Os yn berthnasol)	Nag oes		Y flwyddyn gyfredol + blwyddyn	GWAREDU SAFONOL
1.4.4	Cylchlythyrau ac eitemau eraill ag oes weithredol fyr	Nag oes		Y flwyddyn gyfredol + blwyddyn	GWAREDU SAFONOL
1.4.5	Llyfr Ymwelwyr a Thaflenni Arwyddo i Mewn	Oes		Y flwyddyn gyfredol + 6 blynedd ac yna ADOLYGU	GWAREDU'N DDIOGEL
1.4.6	Cofnodion sy'n ymwneud â chreu a rheoli Cymdeithasau Rhieni ac Athrawon a/neu Cymdeithasau Cyn-ddisgyblion	Nag oes		Y flwyddyn gyfredol + 6 blynedd ac yna ADOLYGU	GWAREDU'N DDIOGEL

2. Adnoddau Dynol

Mae'r adran hon yn ymdrin â'r holl faterion rheoli Adnoddau Dynol yn yr ysgol.

2.1 Recriwtio					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
2.1.1	Holl gofnodion sy'n arwain at benodi pennaeth newydd	Oes		Dyddiad y penodiad + 6 blynedd (i'w gadw yn y Swyddfa Addysg Ardal – dim copi yn yr ysgol)	GWAREDU'N DDIOGEL
2.1.2	Holl gofnodion sy'n arwain at benodi aelod newydd o staff – ymgeiswyr aflwyddiannus	Oes		Dyddiad penodi'r ymgeisydd llwyddiannus + 6 mis (Swyddfa Addysg Ardal i gadw copi - Ysgolion i waredu yn ddiogel)	GWAREDU'N DDIOGEL
2.1.3	Holl gofnodion sy'n arwain at benodi aelod newydd o staff – ymgeisydd llwyddiannus	Oes		Dylid ychwanegu'r holl wybodaeth berthnasol i ffeil bersonol yr aelod staff (gweler isod) a dylid cadw'r holl wybodaeth arall am 6 mis.	GWAREDU'N DDIOGEL
2.1.4	Gwybodaeth archwilio cefndir cyn cyflogi - Gwiriadau DBS (Gwybodaeth archwilio cyflogaeth)	Oes	*DBS Update Service Employer Guide June 2012: Keeping children safe in education*. Gorffennaf 2015 (Canllawiau Statudol gan yr Adran Addysg) Adrannau 73, 74	Ni ddylid cadw copïau o dystysgrifau DBS.	
2.1.5	Casglu prawf adnabod fel rhan o'r broses o wirio datgeliad DBS uwch "*portable*"	Oes		Ni ddylid cadw copïau o dogfennau prawf adnabod fel rhan o'r broses o wirio datgeliad DBS uwch "*portable*"	
2.1.6	Gwybodaeth archwilio cefndir cyn cyflogi – Tystiolaeth sy'n profi'u hawl i weithio yn y Deyrnas Gyfunol[4]	Oes	*An employer's guide to right to work checks* [Swyddfa Gartref, Mai 2015]	Anfon yr wybodaeth i'r awdurdod	

[4] Mae angen i gyflogwyr wneud "copi clir" o'r dogfennau a ddangosir iddynt fel rhan o'r broses hon.

2.2 Rheoli Staff Gweithredol					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
2.2.1	Ffeil Bersonol yr Aelod Staff	Oes	Deddf Cyfyngiadau 1980 (Adran 2)	Terfyn y gyflogaeth +25 (Er gwybodaeth: Er bod Toolkit yr IRMS yn nodi: Terfyn y gyflogaeth + 6 blynedd, mae Cyngor Gwynedd wedi gwneud asesiad risg ac wedi penderfynu cadw ffeiliau personol unrhyw aelod staff sydd angen DBS am 25 mlynedd yn dilyn terfyn y gyflogaeth)	GWAREDU'N DDIOGEL
2.2.2	Amserlenni Cyflog	Oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
2.2.3	Gwerthusiad blynyddol / cofnodion asesu	Oes		Y flwyddyn gyfredol + 5 mlynedd	GWAREDU'N DDIOGEL
2.3 Rheoli'r Prosesau Disgyblu a Chwynion					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
2.3.1	Honiad o natur amddiffyn plant yn erbyn aelod o staff, yn cynnwys honiadau di-sail[5]	Oes	*"Keeping children safe in education: Statutory guidance for schools and colleges, March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children, March 2015"*	Hyd oedran ymddeol arferol person neu 10 mlynedd o ddyddiad yr honiad, pa un bynnag fo hiraf ac yna ADOLYGU. Noder y dylid tynnu honiadau y canfyddir eu bod yn faleisus o'r ffeiliau Personél. Os oes sail iddynt, dylid eu cadw ar y ffeil a darparu copi i'r person dan sylw.	GWAREDU'N DDIOGEL Rhaid llarpio'r cofnodion hyn.

[5] Cynhaliwyd yr adolygiad hwn fel yr oedd yr Ymchwiliad Annibynnol i Gam-drin Plant yn Rhywiol yn mynd rhagddo. Oherwydd hyn, argymhellir y dylid cadw'r holl gofnodion sy'n ymwneud â cham-drin plant hyd nes i'r Ymchwiliad gael ei gwblhau. Yna, bydd yr adran hon yn cael ei hadolygu eto i roi ystyriaeth i unrhyw argymhellion y gallai'r Ymchwiliad ei wneud o ran cadw cofnodion.

2.3.2	Camau Disgyblu	Oes			
	Rhybudd Llafar			Dyddiad y rhybudd[6] + 6 mis	GWAREDU'N DDIOGEL [Os rhoddir rhybuddion ar ffeiliau personol, yna rhaid eu chwynnu o'r ffeil]
	Rhybudd Ysgrifenedig – lefel 1			Dyddiad y rhybudd + 6 mis	
	Rhybudd Ysgrifenedig – lefel 2			Dyddiad y rhybudd + 12 mis	
	Rhybudd Terfynol			Dyddiad y rhybudd + 18 mis	
	Achos di-sail			Os yw'r mater yn ymwneud ag amddiffyn plant yna gweler uchod, fel arall, gwaredu ar derfyn yr achos	GWAREDU'N DDIOGEL

2.4 Iechyd a Diogelwch					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
2.4.1	Datganiadau Polisi Iechyd a Diogelwch	Nag oes		Oes y polisi + 3 blynedd	GWAREDU'N DDIOGEL
2.4.2	Asesiadau Risg Iechyd a Diogelwch	Nag oes		Oes yr asesiad risg + 3 blynedd (Manylion isod ynglŷn â ffurflenni asesiadau risg sydd yn cael ei yrru gyda HS11)	GWAREDU'N DDIOGEL
2.4.3	Cofnodion sy'n ymwneud â damwain / anaf yn y gwaith	Oes		Dyddiad y digwyddiad + 12 mlynedd. O ran damweiniau difrifol, bydd angen gweithredu cyfnod cadw ychwanegol	GWAREDU'N DDIOGEL
2.4.4	Adrodd am Ddamweiniau (e.e. HS11)	Oes	Rheoliadau Nawdd Cymdeithasol (Hawliadau a Thaliadau) 1979 Rheoliad 25. Deddf Gweinyddu Nawdd Cymdeithasol 1992 Adran 8. Deddf Cyfyngiadau 1980		
	Oedolion			Dyddiad y digwyddiad + 6 blynedd	GWAREDU'N DDIOGEL

[6] Pan fo'r rhybudd yn ymwneud â materion amddiffyn plant, gweler uchod. Os yw'r camau disgyblu'n ymwneud â mater amddiffyn plant, cysylltwch â'ch Swyddog Diogelu Plant am gyngor pellach.

	Plant			Dyddiad geni'r plentyn + 25 mlynedd ADYaCH: Dyddiad Geni'r plentyn + 35 mlynedd	GWAREDU'N DDIOGEL
2.4.5	Rheoli Sylweddau sy'n Beryglus i Iechyd (COSHH)	Nag oes	Rheoliadau Rheoli Sylweddau sy'n Berygl i Iechyd 2002. OS 2002 Rhif 2677 Rheoliad 11; Dylid cadw cofnodion a gedwir dan Reoliadau 1994 a 1999 fel pe na byddai Rheoliadau 2002 wedi dod i rym. Rheoliad 18(2)	Y flwyddyn gyfredol + 40 mlynedd	GWAREDU'N DDIOGEL
2.4.6	Proses o fonitro ardaloedd ble mae'n debygol fod gweithwyr a phobl wedi dod i gysylltiad ag asbestos	Nag oes	Rheoliadau Rheoli Asbestos yn y Gwaith 2012 OS 1012 Rhif 632 Rheoliad 19	Gweithred olaf + 40 mlynedd	GWAREDU'N DDIOGEL
2.4.7	Proses o fonitro ardaloedd ble mae'n debygol fod gweithwyr a phobl wedi dod i gysylltiad ag ymbelydredd	Nag oes		Gweithred olaf + 50 mlynedd	GWAREDU'N DDIOGEL
2.4.8	Llyfrau Log Rhagofalon Tân	Nag oes		Y flwyddyn gyfredol + 6 mlynedd	GWAREDU'N DDIOGEL

2.5 Cyflogres a Phensiynau					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
2.5.1	Cofnodion Tâl Mamolaeth	Oes	Rheoliadau Tâl Mamolaeth (Cyffredinol) Statudol 1986 (OS1986/1960), adolygwyd 1999 (OS1999/567)	Y flwyddyn gyfredol + 3 blynedd	GWAREDU'N DDIOGEL
2.5.2	Cofnodion a gedwir dan Reoliadau Cyn-	Oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL

	lluniau Buddion Ym-ddeol (Pwerau Gwyb-odaeth) 1995				

3 Rheolaeth Ariannol yr Ysgol

Mae'r adran hon yn ymdrin â holl agweddau rheolaeth ariannol yr ysgol yn cynnwys gweinyddu prydau ysgol.

3.1 Rheoli Risg ac Yswiriant					
	Disgrifiad Cyffredinol o'r Ffeil	Materion Diogelu Data	Gofynion Cyfreithiol	Cyfnod Cadw [Gweithredol]	Gweithred ar ddiwedd oes weinyddol y cofnod
3.1.1	Tystysgrif Yswiriant Atebolrwydd Cyf-logwr	Nag oes		Cau'r ysgol + 40 mlynedd	GWAREDU'N DDIOGEL
3.2 Rheoli Asedau					
	Disgrifiad Cyffredinol o'r Ffeil	Materion Diogelu Data	Gofynion Cyfreithiol	Cyfnod Cadw [Gweithredol]	Gweithred ar ddiwedd oes weinyddol y cofnod
3.2.1	Rhestrau eiddo o ddodrefn ac offer	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
3.2.2	Ffurflenni adrodd am fwrgleriaeth, dwyn a fandaliaeth	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL

3.3 Cyfrifon a Chyfriflenni yn cynnwys Rheoli Cyllideb					
	Disgrifiad Cyffredinol o'r Ffeil	Materion Diogelu Data	Gofynion Cyfreithiol	Cyfnod Cadw [Gweithredol]	Gweithred ar ddiwedd oes weinyddol y cofnod
3.3.1	Cyfrifon Blynyddol	Nag oes		Y flwyddyn gyf-redol + 6 blyn-edd	GWAREDU SAFONOL
3.3.2	Benthyciadau a grantiau a reolir gan yr ysgol	Nag oes		Dyddiad y taliad diwethaf ar y benthyciad + 12 mlynedd ac yna ADOLYGU	GWAREDU'N DDIOGEL
3.3.3	Ceisiadau am Grantiau Myfyrwyr	Oes		Y flwyddyn gyf-redol + 3 blyn-edd	GWAREDU'N DDIOGEL
3.3.4	Holl gofnodion sy'n ymwneud â chreu a rheoli cyllidebau yn cynnwys y datganiad Cyllideb Blynyddol a'r papurau cefndirol	Nag oes		Oes y gyllideb + 6 blynedd (Er gwybodaeth: Er bod Toolkit yr IRMS yn nodi: Oes y gyllideb + 3 blynedd, mae Cyngor Gwyn-edd yn argymell eu cadw am 6 blynedd i gyd-fynd a chyf-nodau cadw deunyddiau cyll-idol arall)	GWAREDU'N DDIOGEL
3.3.5	Anfonebau, derbyn-ebau, llyfrau archeb, nodiadau danfon	Nag oes		Y flwyddyn ar-iannol gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
3.3.6	Cofnodion sy'n ym-wneud â chasglu a bancio arian	Nag oes		Y flwyddyn ar-iannol gyfredol + 6 blynedd	GWAREDU'N DDIOGEL

3.3.7	Cofnodion sy'n ymwneud ag adnabod a chasglu dyledion	Nag oes		Y flwyddyn ariannol gyfredol + 6 blynedd	GWAREDU'N DDIOGEL

3.4 Rheoli Cytundebau					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
3.4.1	Holl gofnodion sy'n ymwneud â rheoli contractau dan sêl	Nag oes	Deddf Cyfyngiadau 1980	Taliad olaf ar y contract + 12 mlynedd	GWAREDU'N DDIOGEL
3.4.2	Holl gofnodion sy'n ymwneud â rheoli contractau dan lofnod	Nag oes	Deddf Cyfyngiadau 1980	Taliad olaf ar y contract + 6 blynedd	GWAREDU'N DDIOGEL
3.4.3	Cofnodion sy'n ymwneud â rheoli contractau	Nag oes		Y flwyddyn gyfredol + 2 flynedd	GWAREDU'N DDIOGEL

3.5 Cronfa'r Ysgol					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
3.5.1	Cronfa'r Ysgol – Llyfrau Siec	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
3.5.2	Cronfa'r Ysgol – Llyfrau Talu i Mewn	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
3.5.3	Cronfa'r Ysgol – Cyfriflyfr	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
3.5.4	Cronfa'r Ysgol – Anfonebau	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
3.5.5	Cronfa'r Ysgol – Derbynebau	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
3.5.6	Cronfa'r Ysgol – Cyfriflenni Banc	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
3.5.7	Cronfa'r Ysgol – Teithiau ysgol	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL

3.6 Rheoli Prydau Ysgol					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
3.6.1	Cofrestrai Prydau Ysgol am Ddim	Oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
3.6.2	Cofrestrai Prydau Ysgol	Oes		Y flwyddyn gyfredol + 3 blynedd	GWAREDU'N DDIOGEL
3.6.3	Taflenni Crynhoi Prydau Ysgol	Nag oes		Y flwyddyn gyfredol + 3 blynedd	GWAREDU'N DDIOGEL

4. Rheoli Eiddo

Mae'r adran hon yn ymdrin â rheoli adeiladau ac eiddo.

4.1 Rheoli Eiddo					
	Disgrifiad Cyffredinol o'r Ffeil	Materion Diogelu Data	Gofynion Cyfreithiol	Cyfnod Cadw [Gweithredol]	Gweithred ar ddiwedd oes weinyddol y cofnod
4.1.1	Gweithredoedd eiddo mae'r ysgol yn berchen arnynt	Nag oes		PARHAOL Dylai'r rhain ddilyn yr eiddo oni bai bod yr eiddo wedi'i gofrestru gyda'r Gofrestrfa Dir	
4.1.2	Cynlluniau eiddo mae'r ysgol yn berchen arnynt	Nag oes		Dylid cadw'r rhain tra bod yr eiddo yn berchen i'r ysgol a dylid eu trosglwyddo i unrhyw berchnogion newydd os bydd yr adeilad yn cael ei osod neu'i werthu.	
4.1.3	Les eiddo sy'n cael ei lesu i'r ysgol neu gan yr ysgol	Nag oes		Terfyn y les + 6 blynedd	GWAREDU'N DDIOGEL
4.1.4	Cofnodion sy'n ymwneud â lesu eiddo ysgol	Nag oes		Y flwyddyn ariannol gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
4.2 Cynnal a Chadw					
	Disgrifiad Cyffredinol o'r Ffeil	Materion Diogelu Data	Gofynion Cyfreithiol	Cyfnod Cadw [Gweithredol]	Gweithred ar ddiwedd oes weinyddol y cofnod
4.2.1	Holl gofnodion sy'n ymwneud â gwaith cynnal a chadw ar yr ysgol a gwblheir gan gontractwyr	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
4.2.2	Holl gofnodion sy'n ymwneud â gwaith cynnal a chadw ar yr ysgol a gwblheir gan staff yr ysgol yn cynnwys llyfrau log cynnal a chadw	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL

5. Rheoli Disgyblion

Mae'r adran hon yn cynnwys yr holl gofnodion a grëwyd yn ystod yr amser mae disgybl yn ei dreulio yn yr ysgol. Am wybodaeth ynghylch adrodd am ddamweiniau, gweler Iechyd a Diogelwch uchod.

5.1 Cofnod Addysgiadol y Disgybl					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
5.1.1	Cofnod Addysgiadol y Disgybl yn ofynnol dan Reoliadau Addysg (Gwybodaeth Disgybl) (Lloegr) 2005	Oes	Rheoliadau Addysg (Gwybodaeth Disgybl) (Lloegr) 2005 OS 2005 Rhif 1437		
	Meithrin			Cadw tra mae'r plentyn yn y dosbarth meithrin.	Dylai'r ffeil ddilyn y disgybl pan fydd ef/hi'n gadael y dosbarth meithrin i'r ysgol gynradd / perthnasol.
	Cynradd			Cadw tra mae'r plentyn yn yr ysgol gynradd (E.e. Canlyniadau, Adroddiadau Rhieni, Targedau, Asesiadau / Profion Cenedlaethol / Mewnol, Asesiad sylfaen)	Dylai'r ffeil ddilyn y disgybl pan fydd ef/hi'n gadael yr ysgol gynradd. Bydd hyn yn cynnwys: • symud i ysgol gynradd arall • symud i ysgol uwchradd • symud i uned cyfeirio disgyblion • os fydd y plentyn yn marw yn ystod ei gyfnod yn yr ysgol gynradd, dylid dychwelyd y ffeil i'r Awdurdod Lleol er mwyn ei chadw am y cyfnod cadw statudol. Os bydd y disgybl yn trosglwyddo i ysgol annibynnol, yn trosglwyddo i addysg gartref neu'n gadael y wlad, dylid dychwelyd y ffeil i'r Awdurdod Lleol er mwyn ei chadw am y cyfnod cadw statudol. Fel arfer, nid oes gan Ysgolion Cynradd ddigon o ofod storio i gadw.cofnodion ar gyfer disgyblion nad ydynt wedi trosglwyddo yn y ffordd arferol. Mae'n gwneud mwy o synnwyr i drosglwyddo'r cofnod i'r Awdurdod Lleol gan ei bod yn fwy tebygol y bydd y disgybl yn gwneud cais am y cofnod i'r Awdurdod Lleol.

	Uwchradd		Deddf Cyfyngiadau 1980 (Adran 2)	Dyddiad geni'r disgybl + 25 mlynedd (Manylion ADYaCh / Amddiffyn Plant isod)	GWAREDU'N DDIOGEL
5.1.2	Canlyniadau Arholiadau – Copïau'r Disgybl	Oes			
	Cyhoeddus			Dylid ychwanegu'r wybodaeth hon i ffeil y disgybl	Dylid dychwelyd yr holl dystysgrifau na chasglwyd i'r bwrdd arholi.
	Mewnol			Dylid ychwanegu'r wybodaeth hon i ffeil y disgybl	
Cynhaliwyd yr adolygiad hwn fel yr oedd yr Ymchwiliad Annibynnol i Gam-drin Plant yn Rhywiol yn mynd rhagddo. Oherwydd hyn, argymhellir y dylid cadw'r holl gofnodion sy'n ymwneud â cham-drin plant hyd nes i'r Ymchwiliad gael ei gwblhau. Yna, bydd yr adran hon yn cael ei hadolygu eto i roi ystyriaeth i unrhyw argymhellion y gallai'r Ymchwiliad ei wneud o ran cadw cofnodion.					
5.1.3	Gwybodaeth Amddiffyn Plant ar ffeil y disgybl	Oes	*"Keeping children safe in education: Statutory guidance for schools and colleges, March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children, March 2015"*	Os rhoddir unrhyw gofnodion sy'n ymwneud â materion amddiffyn plant ar ffeil y disgybl, dylent gael eu gosod mewn amlen dan sêl ac yna'u cadw am yr un cyfnod o amser â ffeil y disgybl. (A throsglwyddo'r ffeil i'r ysgol newydd / uwchradd)	GWAREDU'N DDIOGEL – RHAID llarpio'r cofnodion hyn
5.1.4	Gwybodaeth Amddiffyn Plant mewn ffeiliau ar wahân	Oes	*"Keeping children safe in education: Statutory guidance for schools and colleges, March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children, March 2015"*	Dyddiad geni'r plentyn + 25 mlynedd. Cytunwyd ar y cyfnod cadw mewn ymgynghoriad â'r Grŵp Diogelu Plant gyda'r ddealltwriaeth y byddai prif gopi'r wybodaeth hon i'w chanfod yng nghofnodion Gwasanaethau Cymdeithasol yr Awdurdod Lleol	GWAREDU'N DDIOGEL – RHAID llarpio'r cofnodion hyn

Gweler cyfnodau cadw mewn perthynas â honiadau a wnaed yn erbyn oedolion yn yr adran Adnoddau Dynol o'r atodlen gadw hon.

5.2 Presenoldeb					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
5.2.1	Cofrestrau Presenoldeb	Oes	*School Attendance: Departmental advice for maintained schools, academies, independent schools and local authorities* Hydref 2014	Diwedd y flwyddyn addysgol gyfredol +3 blynedd. (Er gwybodaeth, mae'r toolkit yn nodi: Rhaid cadw pob cofnod yn y gofrestr am gyfnod o dair blynedd wedi'r dyddiad pan wnaed y cofnod)	GWAREDU'N DDIOGEL
5.2.2	Gohebiaeth yn ymwneud ag absenoldebau awdurdodedig		Deddf Addysg 1996 Adran 7	Y flwyddyn ariannol gyfredol + 2 flynedd	GWAREDU'N DDIOGEL
5.3 Anghenion Addysgol Arbennig / ADYaCh					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
5.3.1	Ffeiliau ac adolygiadau Anghenion Addysgol Arbennig / ADYach a Chynlluniau Addysg Unigol	Oes	Deddf Cyfyngiadau 1980 (Adran 2)	Dyddiad geni'r disgybl +35 (Er gwybodaeth: Er bod Toolkit yr IRMS yn nodi: Dyddiad geni'r disgybl + 25 mlynedd, mae penderfyniad wedi bod o fewn Gwasanaeth ADYaCh Integredig yw cadw am 35 mlynedd o ddyddiad geni'r plentyn) Gwybodaeth angen ei drosglwyddo o ysgol gynradd i uwchradd	ADOLYGU NODER: Y cyfnod cadw hwn yw'r cyfnod cadw lleiaf y dylid cadw unrhyw ffeil disgybl. Mae rhai awdurdodau'n dewis cadw ffeiliau ADY am gyfnod hirach i amddiffyn eu hunain yn erbyn achos "methiant i ddarparu addysg ddigonol". Mae elfen o ddadansoddi risg fusnes yn gysylltiedig ag unrhyw benderfyniad i gadw'r cofnodion am gyfnod hwy na'r cyfnod cadw lleiaf a dylai hyn gael ei ddogfennu.
5.3.2	Datganiad a gedwir dan adran 234 Deddf Addysg 1990 ac unrhyw newidiadau a wnaed i'r datganiad	Oes	Deddf Addysg 1996 Deddf Anghenion Addysgol Arbennig ac Anableddau 2001 Adran 1	Dyddiad geni'r disgybl + 35 mlynedd [Fel arfer, byddai hwn yn cael ei gadw yn ffeil y disgybl] (Er gwybodaeth: Er bod Toolkit yr	GWAREDU'N DDIOGEL oni bai fod y ddogfen yn destun *"legal hold".*

				IRMS yn nodi: Dyddiad geni'r disgybl + 25 mlynedd, mae penderfyniad wedi bod o fewn Gwasanaeth ADYaCh Integredig yw cadw am 35 mlynedd o ddyddiad geni'r plentyn)	
5.3.3	Cyngor a gwybodaeth a ddarperir i rieni ynghylch anghenion addysgol (e.e. Adroddiadau Iechyd a gwasanaethau arbenigol)	Oes	Deddf Anghenion Addysgol Arbennig ac Anableddau 2001 Adran 2	Dyddiad geni'r disgybl + 35 mlynedd [Fel arfer, byddai hwn yn cael ei gadw yn ffeil y disgybl] (Er gwybodaeth: Er bod Toolkit yr IRMS yn nodi: Dyddiad geni'r disgybl + 25 mlynedd, mae penderfyniad wedi bod o fewn Gwasanaeth ADYaCh Integredig yw cadw am 35 mlynedd o ddyddiad geni'r plentyn)	GWAREDU'N DDIOGEL oni bai fod y ddogfen yn destun *"legal hold".*
5.3.4	Strategaeth Hygyrchedd Unigolyn (e.e. Asesiadau Risg / Cynlluniau meddygol/ PEEP)	Oes	Deddf Anghenion Addysgol Arbennig ac Anableddau 2001 Adran 14	Dyddiad geni'r disgybl + 35 mlynedd [Fel arfer, byddai hwn yn cael ei gadw yn ffeil y disgybl] (Er gwybodaeth: Er bod Toolkit yr IRMS yn nodi: Dyddiad geni'r disgybl + 25 mlynedd, mae penderfyniad wedi bod o fewn Gwasanaeth ADYaCh Integredig yw cadw am 35 mlynedd o ddyddiad geni'r plentyn)	GWAREDU'N DDIOGEL oni bai fod y ddogfen yn destun *"legal hold".*

6. Rheoli Cwricwlwm

6.1 Gwybodaeth Ystadegol a Rheoli					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
6.1.1	Dychweliadau Cwricwlwm (E.e. Taflenni canlyniadau diwedd flwyddyn)	Nag oes		Y flwyddyn gyfredol + 3 blynedd	GWAREDU'N DDIOGEL
6.1.2	Canlyniadau Arholiadau (Copi Ysgolion)	Oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
	Cofnodion Profion Cenedlaethol	Oes			
	Canlyniadau			Dylai canlyniadau'r Profion Cenedlaethol gael eu cofnodi ar ffeil addysgiadol y plentyn ac felly byddant yn cael eu cadw hyd nes y bydd y plentyn yn 25 mlwydd oed. Efallai y bydd yr ysgol yn dymuno cadw cofnod cyfansawdd o ganlyniadau Profion Cenhedlaethol flwyddyn gyfan. Gellid eu cadw am y flwyddyn gyfredol + 6 blynedd fel y gellir gwneud cymariaethau addas.	GWAREDU'N DDIOGEL
	Papurau Arholiad / Profion Cenhedlaethol			Dylid cadw'r papurau arholiad hyd nes y bydd unrhyw brosesau apêl/dilysu wedi'u cwblhau	GWAREDU'N DDIOGEL
6.1.3	Adroddiadau Nifer Derbyn Cyhoeddedig (PAN) (Mynediad)	Oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
6.1.4	Data Ychwanegu Gwerth a Chyd-destunol (E.e. ffeiliau asesu / monitro cynnydd)	Oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL

6.1.5	Ffurflenni Hunan Werthuso (Hunan arfarnu)	Oes		Y flwyddyn gyf-redol + 6 blyn-edd	GWAREDU'N DDIOGEL
6.2 Gweithredu'r Cwricwlwm					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
6.2.1	Cynlluniau Gwaith	Nag oes		Y flwyddyn gyf-redol + blwyddyn	Gall fod yn briodol adolygu'r cofnodion hyn ar ddiwedd pob blwyddyn a phennu cyf-nod cadw ychwanegol neu WAREDU'N DDIOGEL
6.2.2	Amserlen	Nag oes		Y flwyddyn gyf-redol + blwyddyn	
6.2.3	Llyfrau Cofnod Dos-barth	Nag oes		Y flwyddyn gyf-redol + blwyddyn	
6.2.4	Llyfrau Marcio	Nag oes		Y flwyddyn gyf-redol + blwyddyn	
6.2.5	Cofnod o'r Gwaith Cartref a osodwyd	Nag oes		Y flwyddyn gyf-redol + blwyddyn	
6.2.6	Gwaith Disgyblion	Nag oes		Dylai gwaith y disgybl cael ei ddychwelyd i'r disgybl ar ddi-wedd y flwyddyn acad-emaidd. Dylid cadw gwaith a gwbl-hawyd at ddi-benion arholi yn unol â gofynion cymhwyster/y bwrdd arholi penodol. Bydd y pen-naeth yn gyfrifol am sicrhau bod gwaith o'r fath wedi ei farcio yn unol â pholisi'r ysgol, a'i ar-chwilio er mwyn sicrhau na ellir ei ddefnyddio fel tystiolaeth mewn unrhyw gamau cyfreith-iol y gellid eu cymryd yn y dyf-odol. Os nad yw hyn yn bolisi gan yr ysgol yna ei gwaredu ar ôl	GWAREDU'N DDIOGEL

				flwyddyn gyf-redol + blwyddyn	

7. Gweithgareddau Allgyrsiol

7.1 Ymweliadau Addysgiadol y tu allan i'r Ystafell Ddosbarth					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Gofynion Cyfreithiol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
7.1.1	Cofnodion a grëwyd gan ysgolion i gael cymeradwyaeth i gynnal Ymweliad Addysgiadol y tu allan i'r Ystafell Ddosbarth – Ysgolion Cynradd	Nag oes	Gwefan *Outdoor Education Advisers' Panel National Guidance* http://oeapng.info yn enwedig Adran 3 – "*Legal Framework and Employer Systems"* ac Adran 4 – *"Good Practice"*	Dyddiad yr ymweliad + 14 mlynedd	GWAREDU'N DDIOGEL
7.1.2	Cofnodion a grëwyd gan ysgolion i gael cymeradwyaeth i gynnal Ymweliad Addysgiadol y tu allan i'r Ystafell Ddosbarth – Ysgolion Uwchradd	Nag oes	Gwefan *Outdoor Education Advisers' Panel National Guidance* http://oeapng.info yn enwedig Adran 3 – "*Legal Framework and Employer Systems"* ac Adran 4 – *"Good Practice"*	Dyddiad yr ymweliad + 10 mlynedd	GWAREDU'N DDIOGEL
7.1.3	Ffurflenni Caniatâd gan Rieni ar gyfer tripiau ysgolion ble na fu unrhyw ddigwyddiad mawr	Oes		Hyd at ddiwedd y trip	Er y gellid cadw'r ffurflenni caniatâd am Dyddiad Geni + 22 mlynedd, mae'r disgwyliad y bydd eu hangen yn isel ac nid oes gan y mwyafrif o ysgolion gapasiti storio i gadw pob ffurflen ganiatâd unigol a ddosbarthwyd gan yr ysgol ar gyfer y cyfnod hwn o amser.
7.1.4	Ffurflenni Caniatâd gan Rieni ar gyfer tripiau ysgolion ble y bu digwyddiad mawr	Oes	Deddf Cyfyngiadau 1980 (Adran 2)	Dyddiad Geni'r disgybl oedd ynghlwm â'r digwyddiad + 25 mlynedd. Mae angen cadw'r ffurflenni caniatâd ar gyfer pob disgybl oedd ar y trip er mwyn dangos fod y rheolau wedi'u dilyn ar gyfer pob disgybl	

7.2 Bws Cerdded					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Darpariaethau Statudol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**

7.2.1	Cofrestrai Bws Cerdded	Oes		Dyddiad y gofrestr + 3 blynedd. Mae hyn yn cymryd ystyriaeth o'r ffaith os bydd digwyddiad sy'n gofyn am adroddiad damwain, bydd y gofrestr yn cael ei chyflwyno gyda'r adroddiad damwain ac yn cael ei chadw am y cyfnod o amser sydd ei angen er mwyn adrodd am ddamwain	GWAREDU'N DDIOGEL [Os bydd y cofnodion hyn yn cael eu cadw'n electronig, dylid dinistrio unrhyw gopïau wrth gefn ar yr un pryd]

7.3 Swyddogion Cyswllt Teulu a Chymorthyddion Cyswllt Addysg yn y Cartref					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Darpariaethau Statudol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
7.3.1	Llyfrau Dydd	Oes		Y flwyddyn gyfredol + 2 flynedd ac yna adolygu	
7.3.2	Adroddiadau i asiantaethau allanol – pan fo'r adroddiad wedi'i gynnwys ar y ffeil achos a grëwyd gan yr asiantaeth allanol	Oes		Pan fo'r plentyn yn mynychu'r ysgol ac yna dylid eu dinistrio	
7.3.3	Ffurflenni cyfeirio	Oes		Pan fo'r cyfeiriad yn gyfredol	
7.3.4	Taflenni Manylion Cyswllt	Oes		Y flwyddyn gyfredol ac yna adolygu, os nad yw'r cyswllt yn parhau'n weithredol dylid eu dinistrio	
7.3.5	Cofnodion ar y gronfa ddata o gysylltiadau	Oes		Y flwyddyn gyfredol ac yna adolygu, os nad yw'r cyswllt yn parhau'n weithredol dylid eu dinistrio	
7.3.6	Cofrestrai Grŵp	Oes		Y flwyddyn gyfredol + 2 flynedd	

7.4 TRAC					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Darpariaethau Statudol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
7.4.1	Llyfrau Dydd	Oes	Prosiect Ewrop	2024	GWAREDU'N DDIOGEL
7.4.2	Adroddiadau i asiantaethau allanol – pan fo'r adroddiad wedi'i gynnwys ar y ffeil achos a grëwyd gan yr asiantaeth allanol	Oes		Dinistrio yn ddiogel yn dilyn y disgybl ymadael ar brosiect.	GWAREDU'N DDIOGEL
7.4.3	Ffurflenni cyfeirio	Oes	Prosiect Ewrop	2024	GWAREDU'N DDIOGEL
7.4.4	Taflenni Manylion Cyswllt	Oes	Prosiect Ewrop	2024	GWAREDU'N DDIOGEL
7.4.5	Cofnodion ar y gronfa ddata o gysylltiadau	Oes	Prosiect Ewrop	2024	GWAREDU'N DDIOGEL
7.4.6	Cofrestrai Grŵp	Oes	Prosiect Ewrop	2024	GWAREDU'N DDIOGEL

8. Llywodraeth Ganolog a'r Awdurdod Lleol

Mae'r adran hon yn ymdrin â chofnodion a grëwyd pan fo'r ysgol a'r awdurdod lleol yn rhyngweithio.

8.1 Awdurdod Lleol					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Darpariaethau Statudol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
8.1.1	Taflenni Trosglwyddo Uwchradd (Cynradd)	Oes		Y flwyddyn gyfredol + 2 flynedd	GWAREDU'N DDIOGEL
8.1.2	Dychweliadau Presenoldeb	Oes		Y flwyddyn gyfredol + blwyddyn	GWAREDU'N DDIOGEL
8.1.3	Dychweliadau Cyfrifiad Ysgol	Nag oes		Y flwyddyn gyfredol + 5 mlynedd	GWAREDU'N DDIOGEL
8.1.4	Cylchlythyrau ac unrhyw wybodaeth arall a anfonwyd o'r Awdurdod Lleol	Nag oes		Defnydd gweithredol	GWAREDU'N DDIOGEL

8.2 Llywodraeth Ganolog					
	Disgrifiad Cyffredinol o'r Ffeil	**Materion Diogelu Data**	**Darpariaethau Statudol**	**Cyfnod Cadw [Gweithredol]**	**Gweithred ar ddiwedd oes weinyddol y cofnod**
8.2.1	Adroddiadau a phapurau ESTYN	Nag oes		Oes yr adroddiad ac yna ADOLYGU	GWAREDU'N DDIOGEL
8.2.2	Dychweliadau i lywodraeth ganolog	Nag oes		Y flwyddyn gyfredol + 6 blynedd	GWAREDU'N DDIOGEL
8.2.3	Cylchlythyrau a gwybodaeth arall a anfonwyd o lywodraeth ganolog	Nag oes		Defnydd gweithredol	GWAREDU'N DDIOGEL

Atodiad 5

Data Protection Impact Assessment []

Version Number: (0.1 etc. for DRAFT; 1.0 for FINAL)	
Status: (DRAFT or FINAL)	
Author(s):	
Telephone and email address of author(s) :	
Date of current version:	
Information Asset Owner:	
Date Approved by Information Asset Owner:	

Table of contents

1. Document history

1.1 Revision history

Date	Version	Author	Revision Summary

1.2 Review by Data Protection Officer (DPO)

This DPIA has been reviewed by the DPO on these dates:

Date	Version Number of DPIA	DPO Comments

1.3 Approval

This document requires approval from **Information Asset Owner** named below:

Date	Version	Name

2. Screening Questions

To be completed by the task lead

Please complete the table below. **Answering "Yes" to any of the screening questions below represents a potential IG risk factor** that will have to be further analysed to ensure those risks are *identified*, *assessed* and *mitigated* wherever possible by working through **sections A**, **B** and **C** of this document.

Category	Screening question	Yes/No
Identity	Will the task involve the collection of new information identifiable about individuals?	
Identity	Will the task compel individuals to provide personal information about themselves?	
Multiple organisations	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Data	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
Data	Does the task involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?	
Data	Will the task result in you making decisions or taking action around individuals in ways which could have a significant impact on them?	
Data	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example health records, criminal records, or other information that people are likely to consider as private? Also vulnerable individuals eg children	
Data	Will the task require you to contact individuals in ways which they may find intrusive?	
Storage	Will the information/task be stored in the cloud? (I*f answer is yes please complete the questions on cloud (page 9 onwards)*	
Systems	Have you discussed technical requirements (*if applicable*) with IT?	
Systems	Has an *IT Technical Specification* been completed by the supplier / provider?	

3. Privacy Impact Assessment

Section A - Task Description

To be completed by the task lead

Please complete with as much information as possible as this will assist the DPO in assessing whether further action is required.

Task Name:	
Directorate/Department:	
Is this a change to an existing process?	
Assessment Completed by:	
Job Title:	
Date completed:	
Phone:	
E-mail:	
Information Asset Owner:	
Task/Change Outline - *What* is it that is being planned?	
Purpose / Objectives - *Why* is it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the task.	
What is the purpose of collecting the information within the system? For example research, audit, reporting, staff administration etc.	
Provide a description of the information flows. Even if detailed information is not available some indication must be provided; this may already be available through requirements gathering. Broadly speaking the aim is to establish: **who** the information will be made available to, **what** type of information, **why** the information is required, **how** it will be shared and **how often**.	

Provide details of how the proposal will have the potential to impact on the confidence service users have in the Council maintaining the confidentiality of their personal data. For example, it could be that specific information is being gathered or used that hasn't been used or gathered previously; the level of information held about an individual is increasing or information is being shared with another organisation through a shared system or database where it wasn't previously.
Provide details of any previous Data Protection Privacy Impact Assessment or other form of personal data compliance assessment done on this initiative. If this is a change to an existing system, a DPIA may have been undertaken during the task implementation.
Stakeholders - who is involved in this task/change? Please list stakeholders, including internal, external, organisations (public/private/third) and groups that may be affected by this system/change in the table below and detail any stakeholder activity taken.

Organisation	Engagement / Stakeholder Activity

Stakeholders - Has there been any consultation with data subjects (the individuals that the system or proposed change will affect or impact)?
☐**Yes** **How was this done?** …… ☐**No**

Data Types

In order to understand the potential risks to individual's privacy, it is important to know the types of data that will be held and/or shared. Even if exact detail is not known and initial indication will assist in the privacy impact assessment.

Personal	Tick (All that Apply)	Special Category	Tick (All that Apply)
Name	☐	**Racial / ethnic origin**	☐
Address (home or business)	☐	**Political opinions**	☐
Postcode	☐	**Religious beliefs**	☐
NHS No.	☐	**Trade union membership**	☐
Email address	☐	**Physical or mental health**	☐
Date of birth	☐	**Sexual life**	☐
Reference number If ticked, please detail:	☐	**Genetic data / Biometrics; DNA profile, fingerprints**	☐
Driving Licence [shows date of birth and first part of surname]	☒		
Bank, financial or credit card details	☐		
Mother's maiden name	☐		
National Insurance number	☐		
Tax, benefit or pension Records	☐		
Criminal offences	☐		
Employment, school, Social Services, housing records	☐		
Data of a "higher" sensitivity (tick all that apply)			
Health condition information	☐	**Genetic**	☐
Mental Health	☐	**Adoption**	☐
Child Protection	☐	**Safeguarding Adults**	☐
Comments and Additional data types (if relevant):			

Section B – Privacy Impact Assessment Table [insert task name]

The **task lead** should complete the '*Response'* box for each question. The DPO will then complete the 'Risk Type' and 'Outcome' box

Guidance Notes:

Response - Please answer the questions as fully as possible. If you are unsure of how to answer the question, **please contact the Data Protection Officer (DPO).** If there is supporting information that relates to any of the questions, which you feel would be informative, indicate within the comments section and send this along with the completed assessment.

Additional guidance notes have been provided for some questions; once completed the guidance notes can be removed.

The assessment table is designed to be a 'working document' that can be added to at intervals throughout the process, for example bullet points or rough notes can be used. These notes can be used to highlight things that need to be followed up; noted requirements can be marked up ready for the requirement schedule, etc.

Risk Type – The DPO will use the guidance notes in Appendix 1 to identify the type of risk, this will help the organisation to judge the level of risk and either accept it or put in place appropriate measures to mitigate it.

Outcome – The DPO will use the information provided to decide if any potential IG risks are identified. If, following discussion with the task manager/lead it is agreed there is an IG risk that requires further action / management, the required actions will be noted on the DPIA. The risk will be scored and progress against the identified mitigations captured using a red/amber/green status. **If the DPIA identifies high risks and you are unable to take measures to reduce the risk, it is necessary to consult the Information Commissioner's Office before processing commences.**

1	Is there any data stored in the cloud?		
	Guidance Note: *Please complete*		
	Response (completed by task lead)	**Risk type (completed by DPO)**	**Outcome (completed by DPO)**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
2	Where will the information be held and who will have responsibility for it?		
	Guidance Note: *Detail which team or organisation has responsibility for the system that holds the data. Detail which team or organisation has responsibility for the storage of the data. Detail how the servers are configured and Resilient. Detail which team or organisation is responsible for the security of the server the data is located on. Where is the server located physically?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
3	What types of information will be held and/or shared?		
	Guidance Note*: For example a care plan, case correspondence, occupational health data.* *Will the records be electronic or paper?*		
	Response	**Risk type**	**Outcome**

	Type here	☐ Individual ☐ Organisational ☐ Compliance	

4	Will any of the following activities be involved (tick those that apply): ☐ Recording of demographic data ☐ Sharing of personal data ☐ Transfer of service user identifiable data: to other systems, to other third parties ☐ Other

5	What legal basis for processing will you be relying on? Please tick one for personal data and one for special category data (if processing). Please speak to your information governance team if unsure.			
	Personal Data		**Special Category Data (includes health data)**	
	Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☐	Provision of preventative or occupational medicine, health or social care or treatment, or the management of health or social care systems – Art 9(2)(h)	☐
	Protection of vital interests – Art 6(1)(d)	☐	Vital interests of the data subject or a third party where they are incapable of giving consent – Art 9(2)(c)	☐
	Necessary for compliance with a legal obligation – Art 6(1)(c)	☐	Necessary for reasons of substantial public interest - Art 9(2)(g)	☐
			Public health - Art 9(2)(i)	☐
	Consent – Art 6(1)(a)	☐	Explicit Consent – Art 9(2)(a)	☐
	Other (please detail)	☐	Research – Art 9(2)(j)	☐
			Other (please detail)	☐
	Outcome			

6	Will the planned use of personal data be covered by information already provided to individuals or is a new or revised communication planned or required?		
	Guidance Note: *'Fair Processing' i.e. informing individuals of what is happening to their information is a requirement under Data Protection Legislation. What are the existing communications? What are the planned communications?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
7	Will the development enable the sharing of records with other organisations? How will records be shared?		
	Guidance Note*: Will information be transferred to a central hub with a collated record made available to participating organisations? Will participating organisations be provided with a view of records created in another organisation?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
8	Will the development result in the handling of a significant amount of new data about each person, or significant change in existing data holdings? Please detail the new data handled.		
	Guidance Note*: i.e. Is more information held about the same population of service users?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
9	Will the development result in the handling of **new data** about a significant number of people, or a **significant change in the population coverage**?		
	Guidance Note*: Please complete.*		

	Response	Risk type	Outcome
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
10	Does the task involve **new linkage** of personal data with other data sets, or significant change in data linkages? Please list the linking systems		
	***Guidance Note**: Is the development dependent on, or does it link to other systems such as Welsh Demographic Service, NHS system? Will the NHS Number be used as the common identifier? How will records be matched / linked. What measures will be in place to correctly match/link records?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
11	What security controls will be in place to prevent unauthorised or unlawful processing of information?		
	***Guidance Note:** Describe any such measures (e.g. system controls such as role based access, audit notifications, etc.) and outline any possible implications?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
12	How is access to the system managed?		
	***Guidance Note**: Who authorises accounts, manages role based access and disables accounts? Please detail who is responsible for the business processes*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	

13	What additional controls will be in place to deal with information of a higher sensitivity?		
	Guidance Note: *Consideration must also be given to name changes through adoption, public protection or gender change and records relating to genetics, mental health, and occupational health.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
14	What are the retention periods for the personal information and how will this be implemented?		
	Guidance Note*: Within the record keeping system, there must be a method of deciding 'what is a record?' and therefore 'what needs to be kept?' This is described as 'declaring a record'. A declared record is then managed in a way that will hold it in an accessible format until it is appraised for further value or it is destroyed, according to retention policy that has been adopted.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
15	How will you action requests from individuals for access to their personal information (in accordance with their rights)?		
	Guidance Note*: Under relevant Data Protection legislation, individuals have a right to ask for a copy of information held about them. If this is a shared record it must be established who will be responsible for dealing with the request.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
16	Will there be any secondary use of personal information in an identifiable or non-identifiable form?		

	Guidance Note: *Will the information be used for anything other than the main stated purpose? What level of information is to be used for these purposes, how will it be managed and how it will be communicated to service users?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
17	How are users to be trained in their information governance responsibilities? Have any training needs been identified in addition to the mandatory Council data protection training? Please detail training in full.		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
18	Is the information you are using likely to be of good enough quality for the purpose it is used for?		
	Guidance Note*: Consider the flow process, and how often, the information is checked for accuracy and are there procedures to support this? Is there is a facility to deal with data inaccuracies? Is there a facility to record the source of the information?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
19	Will the task involve any data migration or transfer of records from other systems/new feeds? If so, will the system origin and whether they were digitally born be captured in the metadata as part of the transfer process?		
	Guidance Note: *If the task involves any data migration, new feeds? If so, what are the identifiers used? Will the data be maintained in an accessible format? Will the relevant metadata be captured such as whether the information is scanned in, the author, scanner, transcriber, system origin etc.*		
	Response	**Risk type**	**Outcome**

	Type here		
20	Does the system maintain a comprehensive audit trail of user activity and how will the audit log be accessed and analysed?		
	Guidance Note: *Who will be responsible for auditing? Will additional or new organisational processes be required to meet the requirement to audit all user access?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
21	Will the information be transferred (electronically, physically or by other portable means) to an organisation outside of the Council? Please list the organisations.		
	Guidance Note: *Where will it go and what security arrangements will apply (e.g. encryption)? Will removable media be used? How will the information be transported (e.g. telephone, post, secure file sharing portal, email)?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
22	Are there business continuity and disaster recovery plans in place to recover information which may be damaged or lost through human error, computer virus, network failure, theft, fire, flood or other disaster?		
	Guidance Note: *Has this been agreed as part of the Service Management arrangements?*		
	Response	**Risk type**	**Outcome**

	Type here	☐ Individual ☐ Organisational ☐ Compliance	
23	Are there any elements of the system or service that are provided by a third party?		
	Guidance Note: *Is there a contractor (and any sub-contractors?) If so please document who the contracting authority is, who the contractors are and the confidentiality provisions within the contract, please note whether the procurement has been subject to information governance input, and whether the organisation is registered with the information commissioner*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
24	Does the development involve the use of new or inherently privacy invasive technologies?		
	Guidance Note: *For example: smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies and intelligent transportation systems, visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
25	Is automated decision making involved?		
	Guidance Note: *Is there any profiling involved? Can there be any human intervention if required?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	

26	One of the principles of data protection is to process no more personal data than necessary. Is all information being processed by the task necessary?		
	Response	**Risk type**	**Outcome**
	☐Yes ☐No If no, please detail Type here ……	☐ Individual ☐ Organisational ☐ Compliance	
27	Has this task been detailed on the information asset register?		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
Name ……			Date: ……

Section C – IG Requirements Schedule [insert task name]

The requirements schedule forms part of the Data Protection Impact Assessment (DPIA) process. This document must be read in conjunction with the task description for [insert task name] (section A)

Following the review of the populated DPIA table (section B) the DPO and task lead/manager will agree the information governance / privacy requirements and record them on the IG requirements schedule. Each requirement will be scored against the risk matrix at Appendix 3. The requirements schedule will be used to capture progress against each requirement and note the final outcomes. It should be stated whether the risks identified have been eliminated, reduced or accepted.

The schedule is designed to be a living document which is updated regularly as the development progresses.

Using red, amber and green (RAG) as progress indicators within the schedule, by the time the task goes live all requirements should be green. However, dependent on the nature of the task and the issues raised it is possible that requirements may be amber or in an exceptional case even red; where this is the case the organisations involved must agree to accept any residual risk.

See Appendix 2 for further guidance on how to complete the requirements schedule.

Ref	Question No.	Identified Requirement	Risk Assessment					Time-scale	Lead	Completion (RAG)	Comments / Progress / Further Action / Final Outcome
			Risk History	Likelihood	Impact	Score	Status (low, moderate, high,				
RQ1			Initial								
			Residual								
RQ2			Initial								
			Residual								
RQ3			Initial								
			Residual								
RQ4			Initial								
			Residual								

Are any residual risks scored higher than 10?

☐Yes ☐No

If Yes, has the ICO been consulted on the processing? ☐Yes ☐No
If the ICO has not been consulted on the processing and a residual risk is scored higher than 10, please state the reasons for not consulting the ICO below.

4. Appendices

Appendix 1 – Risk Type

Risk Type – this is the 'classification' as noted on the DPIA table (risk to individuals, compliance risk, organisation/corporate risk) and is noted in Section B.

Risks to individuals	Compliance risk	Associated organisation/corporate risk
• Inadequate disclosure controls increase the likelihood of information being shared inappropriately. • The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge. • New surveillance methods may be an unjustified intrusion on their privacy. • Measures taken against individuals as a result of collecting information about them might be seen as intrusive. • The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect. • Identifiers might be collected and linked which prevent people from using a service anonymously. • Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. • Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised. • Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.	• Non-compliance with the common law duty of confidentiality • Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015 • Non-compliance with the relevant data protection legislation • Non-compliance with the Privacy and Electronic Communications Regulations (PECR). • Non-compliance with sector specific legislation or standards. • Non-compliance with human rights legislation.	• Non-compliance with the relevant data protection legislation or other legislation can lead to sanctions, fines and reputational damage. • Problems which are only identified after the task has launched are more likely to require expensive fixes. • The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation. • Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business. • Public distrust about how information is used can damage an organisation's reputation and lead to loss of business. • Data losses which damage individuals could lead to claims for compensation.

Risks to individuals	Compliance risk	Associated organisation/corporate risk
• If a retention period is not established information might be used for longer than necessary.		

Appendix 2 - Additional Guidance notes for completion of the Requirement Schedule

- **Ref -** Unique number allocated to each requirement (RQ) within the schedule, the reference number should be noted against the relevant question in the DPIA table.
- **Identified Requirement –** Details of the IG requirement identified and a brief description of the risk posed if the requirement is not addressed.
- **Risk History** – This is the status of the risk, whether it is the initial risk or the residual risk
- **Likelihood** – What is the likelihood of breaching relevant data protection legislation if no action is taken? This should be scored as per the table below.
- **Impact** – This is the severity of the impact of a breach of relevant data protection legislation if no action is taken. This should be scored as per the table below.
- **Score** – This is the *likelihood score* x *the impact score*.
- **Status** – This is whether the risk is **low**, **medium**, **high** or **extreme**. The score dictates the status as per the table below.
- **Timescale** – For each requirement to be addressed within, as aligned to the task timescales;
- **Lead** – Person responsible for taking each requirement forward;
- **Completion (RAG)** – The level of progress applicable to that action in red (for not begun), amber (in progress), green (complete)
- **Comments / Progress / Further Action / Final Outcome** describe the progress to date for each requirement (each entry should be dated), list any additional comments and further actions as appropriate. Ensure that it is noted if a risk has been eliminated, reduced or accepted. Any significant actions should be fed in as a further requirement.

Appendix 3 - Risk Scoring Tables

Likelihood score	1	2	3	4	5
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency How often might an IG breach occur	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it may not be a persisting issue	Will undoubtedly happen/recur,possibly frequently

Impact score (severity levels) and examples of descriptors	1	2	3	4	5
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on an individual's privacy and confidentiality	Minimal privacy impact requiring no/minimal intervention Other manual or electronic process in place to mitigate the IG risk	Minor impact on an individual's privacy Other manual or electronic process in place to mitigate the IG risk	Moderate privacy impact requiring professional intervention Aspects of reputational damage for the organization if IG requirement not adopted Could result in an event which impacts on a moderate (less than 100) number of individuals	Major breach leading to possible larger scale privacy breaches Mismanagement of patient/client privacy with long-term reputational issues Would impact on over 100 individuals – part system failure	Serious IG breach and non-compliance with the law if requirement not adhered to An event which impacts on a large number of individuals – full system breach because of no adherence to standards. Is likely to be 1000 of individuals

		Likelihood				
		1	**2**	**3**	**4**	**5**
		Rare	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Impact Score	**5 Catastrophic**	5	10	15	20	25
	4 Major	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	4	6	8	10
	1 Negligible	1	2	3	4	5

Status

1 - 3	Low risk
4 - 6	Moderate risk
8 - 12	High risk
15 - 25	Extreme risk

Atodiad 6

Defnydd Delweddau Digidol / Fideo

Enw'r Plentyn/Child's Name……

Bydd yr Ysgol yn cydymffurfio gyda Deddfwriaeth Diogelu Data ac yn gofyn caniatâd cyn cyhoeddi lluniau sydd wedi'i dynnu. Bydd delweddau yn cael eu defnyddio i ddathlu llwyddiannau wrth gyhoeddi hynny mewn cylchlythyrau, papurau newydd lleol, ar wefan Ysgol ac ar wefannau cymdeithasol megis 'Facebook', 'Twitter', 'Instagram'

Unwaith mae'r lluniau / delweddau yn mynd allan ar wefannau cymdeithasol, nid yw'n bosib dileu yn llwyr
Mae gennych yr hawl i dynnu eich caniatâd yn ôl ar unrhyw adeg.

The school will comply with Data Protection legislation and ask for permission before publishing images taken. Images will be used to celebrate successes and will be announced in newsletters, local newspapaers, on the school website and, at times, on social media – 'Facebook', 'Twitter', and 'Instagram'

Once the pictures / images go out on social websites, it is not possible to delete totally

You have the right to withdraw your consent at any time.

Rwy'n rhoi caniatâd i'r ysgol cyhoeddi lluniau / fideos o'm plentyn i gael eu defnyddio. Rwyf yn deall mai dim ond i gefnogi gweithgareddau dysgu neu mewn cyhoeddusrwydd sydd yn dathlu llwyddiant ac yn hyrwyddo gwaith yr ysgol yn rhesymol defnyddir y delweddau yma:

I give permission for the school to publish pictures/videos of my child, I understand that these images will only be used to support learning activities or for publicity to celebrate successes and to reasonably to promote the schools work:

a. tu fewn i'r ysgol, cylchlythyrau / within the school, newsletters ☐

b. gwefan yr ysgol / the school website ☐

c. Facebook/Twitter/Instagram ☐

d. Papur newydd lleol/Local newspaper ☐

Nid wyf yn rhoi caniatâd o gwbl / I do not give permission at all ☐

Enw/Name……..

Perthynas/Relationship……..

Arwyddo/Signed……

Dyddiad/Date……

Atodiad 7

Defnyddio Systemau Biometrig

Mae'r ysgol yn defnyddio systemau biometrig i adnabod plant unigol trwy'r dulliau canlynol *(dylai'r ysgol ddisgrifio yma sut mae'n defnyddio'r system fiometrig).*

Mae gan dechnolegau biometrig fanteision penodol dros systemau adnabod awtomatig eraill, oherwydd nid oes angen i ddisgyblion ddod ag unrhyw beth *(i'r ffreutur neu lyfrgell yr ysgol)* felly ni ellir colli dim byd, megis cerdyn allwedd.

Mae'r ysgol wedi cwblhau asesiad o'r effaith ar breifatrwydd ac mae'n hyderus fod y defnydd o dechnolegau o'r fath yn effeithiol ac wedi'i gyfiawnhau yng nghyd-destun yr ysgol.

Ni chaiff delweddau cyflawn o olion *bysedd / cledrau* dwylo eu storio, ac ni ellir ail-greu'r ddelwedd wreiddiol o'r data. Hynny yw, ni ellir ail-greu ôl bys disgybl neu hyd yn oed darlun o ôl bys gan ddefnyddio'r hyn sydd yn ei hanfod yn rhes o rifau.

Gofynnir i rieni / gofalwyr am ganiatâd i'w plentyn ddefnyddio technoleg biometreg.

Enw Rhiant / Gofalwr	
Enw Myfyriwr / Disgybl	

Fel rhiant / gofalwr y disgybl / myfyriwr uchod, rwy'n cytuno y gall yr ysgol ddefnyddio'r systemau adnabod biometrig a ddisgrifir uchod. Deallaf na ellir defnyddio'r delweddau hyn i greu print ôl bys / cledr llaw cyflawn fy mhlentyn ni chaiff y delweddau hyn eu rhannu ag unrhyw un y tu allan i'r ysgol.

Ydw / Nac ydw

Llofnod	
Dyddiad	

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

Ysgol

Dyddiad Cymeradwyo/Date Adopted:
Dyddiad Adolygu/Review Date:

Llofnodwyd ar ran Cadeirydd y Llywodraethwyr:
_____

Dyddiad: _____

Contents:

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.

See Appendix 1 for a list of the conditions.

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.

See Appendix 2 for further details on how to deal with these requests.

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 using the relevant document in Attachment 3
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.

Appendix 4 sets out the relevant retention periods for school records.

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. An example of permission form is provided in Appendix 6.

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. CCTV

Capturing and/or recording images of identifiable individuals is an example of processing personal information and therefore needs to comply with DPL.

The school will notify staff, pupils and visitors why it is collecting personal information in the form of CCTV images.
The school will ensure that it has a set retention period based on the possible need to review the footage and will consider who is allowed access to this footage and why.

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

See the Information Commissioner's Office's guide on CCTV here:

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

16. Biometric Information (fingerprinting) - OPTIONAL

The Protection of Freedoms Act 2012 includes measures relating to the use of biometric identification systems, i.e. fingerprinting and facial recognition systems.
Under the GDPR, it is recognised that this type of data is special category data

- For every school pupil under the age of 18, the school will obtain the written consent of parents before recording and processing their child's biometric details.
- All such data must be handled appropriately and in accordance with DPL principles.
- Alternative methods of service provision must be identified if a parent or pupil refuses to provide consent.

A consent form for biometric information is provided in Appendix 7.

17. 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.

18. 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.

19. 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

20. 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

Appendix 1

Article 6 Conditions (summary)

6(1)(a) – Individual's consent;
6(1)(b) – Processing is necessary for a contract;
6(1)(c) – Processing is necessary to comply with a legal duty;
6(1)(d) – Processing is necessary for the individual's vital interests;
6(1)(e) - Processing is necessary as it undertakes a task in the public's interest
6(1)(f) – Processing is necessary for the purposes of legitimate interests of the data controller or third party

Article 9 Conditions (summary)

9(2)(a) – Processing with the specific consent of the individual;
9(2)(b) – Processing is necessary under employment law;
9(2)(c) – Processing is necessary to protect the individual's vital interests;
9(2)(d) – Processing for the use of a special category group (Not-for-profit organisation with a political or religious aim or a 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;
9(2)(g) – Processing is necessary for reasons of substantial public interests based on law;
9(2)(h) – Processing is necessary to respond to the needs of Occupational Health and Social Care;
9(2)(i) – Processing is necessary for Public Health reasons;
9(2)(j) – Processing is necessary for archiving purposes in the public interest; or for scientific or historical research purposes; or for statistical purposes.

Further Special Category conditions are included in Schedule 1 of the Data Protection Act 2018.

Appendix 2

The right to have access to information

There are two distinct rights of access to information held by schools about students.
1. Under data protection legislation, any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records as defined within The Pupil Information (Wales) Regulations 2011.

Actioning a request

1) Requests for information can be made in writing; which includes email or verbally. If the initial request does not clearly identify the information required, then further enquiries will be made.

2) The identity of the person making the request must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child.

Evidence of identity can be established by requesting production of:

- Passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3) Everyone has the right of access to information held about them. However, for children, this depends on their ability to understand and the nature of the request (usually 12 and over). The Head of School should discuss the application with the child and consider his / her views when making a decision. A child with the ability to understand may refuse to agree to the request for their records. If it is decided that the child lacks capacity, a person with parental responsibility for the child, or guardian, will make the decision on behalf of the child.

4) The school may charge for providing the information, subject to the following:

   • If the information requested contains the educational record, the fee charged will depend on the number of pages provided.
   • If the information requested is personal, does not include any information contained in educational records, there is no charge.
   • if anyone only requests the educational record, it will be free to see, but the Head of School will charge a fee to cover the cost of photocopying the information.

5) The time allowed to respond to a request, once formally accepted, is one month (not working days or school days, but calendar days, regardless of school holiday period). However, the month does not start until the fees are received or clarification requested.

   If the application is thought to be complex or there are multiple applications, the school will inform the applicant within one month that the application period is to be extended and the reason why. Up to a further two months will be allowed to meet the request in such circumstances.

   If applications are clearly unfounded or excessive (especially if they are repeatable), the school will charge a reasonable fee for the administration costs or refuse to deal with the request.

6) DDD allows for exceptions to the provision of certain information; therefore all information will be reviewed prior to disclosure.

7) Third party information is information that has been provided by others, such as the Police, Local Authority, Healthcare professional or other school. Permission to disclose information from third parties is usually required. The timesheet needs to be kept the same.

8) No information should be disclosed that could significantly harm the physical or mental health or emotional state of the pupil or any other person. Neither should information disclosed that the child is at risk of abuse, or any information relating to court proceedings.

9) Further advice should be sought if there is any concern about disclosure of information.

10) Where information has been edited (blackened or deleted), a complete copy of the information provided should be kept to establish what was edited and why, in case someone made a complaint.

11) The information disclosed should be clear, so any technical codes or terms will need to be clarified. If the information contained is difficult to read or understand, it should be typed again.

12) Information can be provided in school with a member of staff available to help and clarify issues if required, or it could be provided on a face to face basis. The applicant's views should be taken into account when deciding how to provide the information. If postal systems have to be used then registered mail must be used.

Complaints

Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate to deal with the complaint in accordance with the school's complaints procedure. The Information Commissioner will deal with complaints that are not appropriate for consideration under the school's complaints procedure. Contact details for both will be included with the information disclosed.

Contacts

If you have any queries or concerns about these policies / procedures, please contact the Head of School or School Data Protection Officer.

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

The response time for subject access requests, once officially received, is one month **(not working or school days but calendar days, irrespective of school holiday periods)**. However, the one month will not commence until after identification of the requester has been clarified and clarification of information sought received.

Investigation Form for cases of Breaching Data Protection Regulations

1. This form must be completed whenever the protection of personal data has been jeopardized, so that the school has evidence of the steps it has taken to rectify things. Steps taken by the school can include a self-referral to the Information Commissioner. As a result, it is important to complete this form correctly so that it is possible to address all facts and circumstances of the case and to take positive steps to mitigate and reduce risks for individuals and the school.

2. This form should be completed alongside the guidance for investigating cases of data protection breaches which is intended to assist the investigating officer.

3. Please note that the form has three sections.

Section A	to be completed and signed by the **investigating officer**.
Section B	to be completed by a member of the **senior management team/Headteacher**
Section C	to completed by the **Data Protection Officer**

Section A
The investigating officer should complete and sign this section.

About you	
• Name	
• E-mail Address	
• Contact Telephone Number	
Details about the case of breaching Data Protection regulations	
• When did the incident occur?	
• When was the case discovered?	
• Please provide a brief summary of the case.	
• Please outline the personal data involved.	
• In your opinion, has the personal data of any individual been jeopardized as a result of the case? ○ How serious is the risk to individuals?	

• Approximately how many people have been affected?	

• Have these individuals been informed about the case?
  ○ If yes, when and by whom?
  ○ If not, please explain why.	

• Have any steps been taken to reduce/alleviate the impact on those affected? ○ Please provide details.	
• In your opinion, which steps could be introduced to ensure that the same thing never happens again?	
• Do you have any additional comments about the case?	
Please sign and date this section. Signature:	Date:

Section B

A member of the senior management team (or amend where relevant) should complete this section.

About you	
• Name	
• E-mail Address	
• Contact Telephone Number	
Details about the case of breaching Data Protection regulations	
• What steps can be taken to prevent similar cases in the future? ○ If relevant, when do you intend to introduce the necessary changes to your work practice?	
• Do you consider that there is a need to train and develop any staff member associated with the case?	
• Do you consider that disciplinary action needs to be taken?	
Please sign and date this section. Signature:	Date:

Section C

The Data Protection Officer should complete this section.

Note whether or not the case should be referred to the Information Commissioner's Office and whether or not the response to the case noted in Section B is commensurable and sufficient.
Outcome review date (usually 3 months after completing the investigation).

1. School Management

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body					
	Basic File Description	**Data Protection Issues**	**Legal Requirements**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of. PERMANENT	SECURE DISPOSAL[7]
1.1.2	Minutes of Governing Body meetings:	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		PERMANENT	
	Principal Set (signed)			PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
	Inspection Copies[8]			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports	SECURE DISPOSAL or retain with the signed set of the minutes

7 In this context, SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a cross cut shredder.

8 These are the copies which the Clerk of Governors may wish to retain so that persons making a request can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

				should be kept permanently.	
1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL
1.1.5	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.6	Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.7	Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8	Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
1.1.9	Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.1.10	Annual Reports created under the requirements of the Education Act 2002	No	Education Act 2002	Date of report + 10 years	SECURE DISPOSAL
1.1.11	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

Please note that all information about the retention of records concerning the recruitment of Headteachers can be found in the Human Resources section below.

1.2 Headteacher and Senior Management Team					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
1.2.1	Log books of activity in the school maintained by the Headteacher (if relevant)	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Headteacher or the Senior Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
1.2.4	Minutes created by headteachers, deputy headteachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the minutes refers to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5	Correspondence created by headteachers, deputy headteachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL
1.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
1.2.7	School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

1.3 Admissions Process					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	*School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeal panels* December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL
1.3.2	Admissions – if the admission is successful	Yes	*School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeal panels* December 2014	Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions – if the appeal is unsuccessful	Yes	*School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeal panels* December 2014	Resolution of case + 1 year	SECURE DISPOSAL
1.3.4	Register of Admissions	Yes	*School Attendance: Departmental advice for maintained schools, academies, independent schools and local authorities* October 2014	Every entry in the admission register must be retained for a period of three years after the date on which the entry was made[9]	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from former pupils to confirm the dates they attended the school.

9 School Attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014

1.3.5	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	*School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeal panels* December 2014	Current year + 1 year	SECURE DISPOSAL
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc. (e.g. SIMS Pupil Information Collection Form	Yes		See below	
	For successful admissions			This information should be added to the pupil file (e.g. SIMS / file)	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL

1.4 Operational Administration					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
1.4.1	General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
1.4.2	Records relating to the creation and publication of the school brochure or prospectus (if relevant)	No		Current year + 3 years	STANDARD DISPOSAL
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils (if relevant)	No		Current year + 1 year	STANDARD DISPOSAL
1.4.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
1.4.5	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Former Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

2. Human Resources

This section deals with all matters of Human Resources management within the school.

2.1 Recruitment					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
2.1.1	All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years (To be kept in Area Education Office – not be kept in the schools)	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months (Area Education Office to keep a copy – school to dispose the information securely)	SECURE DISPOSAL
2.1.3	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months.	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks (Employment audit information)	Yes	*DBS Update Service Employer Guide June 2012: Keeping children safe in education*. July 2015 (Statutory Guidance from the Department of Education) Sections 73, 74	Copies of DBS certificates should not be kept.	
2.1.5	Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Yes		Copies of identification test documents should not be kept as part of the advanced "portable" DBS disclosure check.	

2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[10]	Yes	*An employer's guide to right to work checks* [The Home Office, May 2015]	Send the information to the authority	

2.2 Operational Staff Management

	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of employment +25 (For information: Although the IRMS Toolkit notes: Termination of employment + 6 years, Gwynedd Council has undertaken a risk assessment and has decided to retain the personal files of any staff member who requires a DBS for 25 years following termination of employment)	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal / assessment records	Yes		Current year + 5 years	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes

	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[11]	Yes	*"Keeping children safe in education: Statutory guidance for schools and colleges, March 2015"; "Working together to safeguard children. A guide to inter-agency working to*	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from	SECURE DISPOSAL These records must be shredded.

10 Employers need to make a "clear copy" of the documents shown to them as part of this process.

11 This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention.

			safeguard and promote the welfare of children, March 2015"	personnel files. If found they are to be kept on the file and a copy provided to the person concerned.	
2.3.2	Disciplinary Proceedings	Yes			
	Verbal Warning			Date of warning[12] + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
	Written Warning – level 1			Date of warning + 6 months	
	Written Warning – level 2			Date of warning + 12 months	
	Final Warning			Date of warning + 18 months	
	Case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

12 Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter please contact your Safeguarding Children Officer for further advice.

2.4 Health and Safety					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
2.4.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety Risk Assessments	No		Life of risk assessment + 3 years (Details below in regards to risk assessment that are sent with HS11)	SECURE DISPOSAL
2.4.3	Records relating to accident / injury at work	Yes		Date of incident + 12 years. In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
2.4.4	Accident Reporting (e.g. HS11)	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	Adults			Date of the incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years ADYaCH: Date Of Birth +35 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18(2)	Current year + 40 years	SECURE DISPOSAL
2.4.6	Process of monitoring of areas where employees and persons are likely to have	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL

	become in contact with asbestos				
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire Precautions Log Books	No		Current year + 6 years	SECURE DISPOSAL
2.5 Payroll and Pensions					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
2.5.1	Maternity Pay Records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

3 Financial Management of the School

This section deals with all aspects of the financial management of the school including the administration of school meals.

3.1 Risk Management and Insurance					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL
3.2 Asset Management					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL
3.3 Accounts and Statements including Budget Management					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years and then REVIEW	SECURE DISPOSAL
3.3.3	Student Grant Applications	Yes		Current year + 3 years	SECURE DISPOSAL
3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 6 years (For information: Although the IRMS Toolkit notes: Life of the budget + 3 years, Gwynedd Council recommends retaining them for 6 years to correspond with the retention periods of other budgetary material)	SECURE DISPOSAL

3.3.5	Invoices, receipts, order books, delivery notes	No		The current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of money	No		The current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debts	No		The current financial year + 6 years	SECURE DISPOSAL

3.4 Contracts Management

	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.4.1	All records relating to management of contracts under seal	No	Limitation Act 1980	Final payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to management of contracts under hand	No	Limitation Act 1980	Final payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	All records relating to management of contracts	No		Current year + 2 years	SECURE DISPOSAL

3.5 School Fund

	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.5.1	School Fund - Cheque Books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund - Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund - Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund - Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank Statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – School Trips	No		Current year + 6 years	SECURE DISPOSAL

3.6 School Meals Management

	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.6.1	Free School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL
3.6.2	School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL

4. Property Management

This section covers the management of buildings and property.

4.1 Property Management					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
4.1.1	Title deeds of properties belonging to the school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
4.1.2	Plans of property belonging to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No		The current financial year + 6 years	SECURE DISPOSAL

4.2 Maintenance					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL

5. Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above.

5.1 Pupil's Educational Record					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Nursery			Retain whilst the child remains at the nursery	The file should follow the pupil when he/she leaves the nursery to the primary / relevant school
	Primary			Retain whilst the child remains at the primary school (E.g. Results, Parent Reports, Targets, National / Internal Assessments / Tests, Foundation assessment)	The file should follow the pupil when he/she leaves the primary school. This will include: • moving to another primary school • moving to a secondary school • moving to a pupil referral unit • if the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It

					makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority.
	Secondary		Limitation Act 1980 (Section 2)	DOB of the pupil + 25 years (ADYach / Child Protection details below)	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes			
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
	Internal			This information should be added to the pupil file	
This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention.					
5.1.3	Child Protection information held on pupil file	Yes	*"Keeping children safe in education: Statutory guidance for schools and colleges, March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children, March 2015"*	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file. (There is a need to transfer the file to the new / secondary school)	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child Protection information held in separate files	Yes	*"Keeping children safe in education: Statutory guidance for schools and colleges, March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of*	DOB of the child + 25 years. This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the master copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded

			children, March 2015"		

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.

5.2 Attendance					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
5.2.1	Attendance Registers	Yes	*School Attendance: Departmental advice for maintained schools, academies, independent schools and local authorities* October 2014	End of the current academic year + 3 years. (For information, the toolkit notes: Every entry in the admission register must be retained for a period of three years after the date on which the entry was made)	SECURE DISPOSAL
5.2.2	Correspondence relating to authorized absence		Education Act 1996 Section 7	The current financial year + 2 years	SECURE DISPOSAL
5.3 Special Educational Needs / ADyaCh					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil +35 (For information: Although the IRMS Toolkit notes: DOB of the pupil + 25 years, a decision has been made by the Integrated ADYaCh Service that it should be retained for 35 years from the pupil's date of birth)	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk

				The information needs to be transferred from primary school to secondary school.	analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	DOB of the pupil + 35 years [This would normally be retained on the pupil file] (For information: Although the IRMS Toolkit notes: DOB of the pupil + 25 years, a decision has been made by the Integrated ADYaCh Service that it should be retained for 35 years from the pupil's date of birth)	SECURE DISPOSAL unless the document is subject to a *"legal hold".*
5.3.3	Advice and information provided to parents regarding educational needs (e.g. Specialist health and safety reports)	Yes	Special Educational Needs and Disability Act 2001 Section 2	DOB of the pupil + 35 years [This would normally be retained on the pupil file] (For information: Although the IRMS Toolkit notes: DOB of the pupil + 25 years, a decision has been made by the Integrated ADYaCh Service that it should be retained for 35 years from the pupil's date of birth)	SECURE DISPOSAL unless the document is subject to a *"legal hold".*
5.3.4	Individual Accessibility Strategy (e. g Risk Assessments / Medical plans / PEEP)	Yes	Special Educational Needs and Disability Act 2001 Section 14	DOB of the pupil + 35 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a *"legal hold".*

				(For information: Although the IRMS Toolkit notes: DOB of the pupil + 25 years, a decision has been made by the Integrated ADYaCh Service that it should be retained for 35 years from the pupil's date of birth)	

6. Curriculum Management

6.1 Statistical and Management Information					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
6.1.1	Curriculum Returns (E.g. End year results sheets)	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	National Tests records	Yes			
	Results			The National Tests results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year National Tests results. These could be kept for current year + 6 years to allow suitable comparison.	SECURE DISPOSAL
	Examination Papers/ National Tests			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) Reports *(Access)*	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data (E.g. . Assessments forms / monitoring progress)	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL
6.2 Implementation of Curriculum					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
6.2.1	Schemes of Work	No		Current year + 1 year	
6.2.2	Timetable	No		Current year + 1 year	It may be appropriate to review these

6.2.3	Class Record Books	No		Current year + 1 year	records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.4	Mark Books	No		Current year + 1 year	
6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' Work	No		The pupil's work should be returned to the pupil at the end of the academic year. Work completed for examination purposes should be kept in accordance with the requirements of the specific examination board / qualification. The headteacher will be responsible for ensuring that such work is marked in accordance with school policy, and audits it to ensure that it cannot be used as evidence in any future legal action. If this is not the school's policy then remove it after current year + year	SECURE DISPOSAL

7. Extra Curricular Activities

7.1 Educational Visits outside the Classroom					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 – *"Legal Framework and Employer Systems"* and Section 4 – *"Good Practice"*	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 – *"Legal Framework and Employer Systems"* and Section 4 – *"Good Practice"*	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental Consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.
7.1.4	Parental Consent forms for school trips where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years. The consent forms for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

7.2 Walking Bus					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
7.2.1	Walking Bus Registers	Yes		Date of register + 3 years.	SECURE DISPOSAL [If these records are retained electronically

				This takes into account the fact that if there is an incident requiring an accident report, the register will be submitted with the accident report and kept for the period of time required for accident reporting	any back up copies should be destroyed at the same time]

7.3 Family Liaison Officers and Home School Liaison Assistants

	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.3.1	Day Books	Yes		Current year + 2 years then review	
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	
7.3.3	Referral forms	Yes		While the referral is current	
7.3.4	Contact Data Sheets	Yes		Current year then review, if contact is no longer active then destroy	
7.3.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
7.3.6	Group Registers	Yes		Current year + 2 years	

7.4 TRAC

	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.4.1	Day Books	Yes	European Funding	2024	SECURE DISPOSAL
7.4.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		once the pupil leaves the project	SECURE DISPOSAL
7.4.3	Referral forms	Yes	European Funding	2024	SECURE DISPOSAL
7.4.4	Contact Data Sheets	Yes	European Funding	2024	SECURE DISPOSAL
7.4.5	Contact database entries	Yes	European Funding	2024	SECURE DISPOSAL
7.4.6	Group Registers	Yes	European Funding	2024	SECURE DISPOSAL

8. Central Government and Local Authority

This section covers records created in the course of interaction between the school and the local authority.

8.1 Local Authority					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
8.1.1	Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
8.1.2	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3	School Census Returns	No		Current year + 5 years	SECURE DISPOSAL
8.1.4	Circulars and any other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL
8.2 Central Government					
	Basic File Description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
8.2.1	ESTYN reports and papers	No		Life of the report and then REVIEW	SECURE DISPOSAL
8.2.2	Returns to central government	No		Current year + 6 years	SECURE DISPOSAL
8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL

Appendix 5

Data Protection Impact Assessment

[]

Version Number: (0.1 etc. for DRAFT; 1.0 for FINAL)	
Status: (DRAFT or FINAL)	
Author(s):	
Telephone and email address of author(s) :	
Date of current version:	
Information Asset Owner:	
Date Approved by Information Asset Owner:	

5. Document history

5.1 Revision history

Date	Version	Author	Revision Summary

5.2 Review by Data Protection Officer (DPO)

This DPIA has been reviewed by the DPO on these dates:

Date	Version Number of DPIA	DPO Comments

5.3 Approval

This document requires approval from **Information Asset Owner** named below:

Date	Version	Name

6. Screening Questions

To be completed by the task lead

Please complete the table below. **Answering "Yes" to any of the screening questions below represents a potential IG risk factor** that will have to be further analysed to ensure those risks are *identified*, *assessed* and *mitigated* wherever possible by working through **sections A**, **B** and **C** of this document.

Category	Screening question	Yes/No
Identity	Will the task involve the collection of new information identifiable about individuals?	
Identity	Will the task compel individuals to provide personal information about themselves?	
Multiple organisations	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Data	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
Data	Does the task involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?	
Data	Will the task result in you making decisions or taking action around individuals in ways which could have a significant impact on them?	
Data	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example health records, criminal records, or other information that people are likely to consider as private? Also vulnerable individuals eg children	
Data	Will the task require you to contact individuals in ways which they may find intrusive?	
Storage	Will the information/task be stored in the cloud? (I*f answer is yes please complete the questions on cloud (page 9 onwards)*	
Systems	Have you discussed technical requirements (*if applicable*) with IT?	
Systems	Has an *IT Technical Specification* been completed by the supplier / provider?	

7. Privacy Impact Assessment

Section A - Task Description

To be completed by the task lead

Please complete with as much information as possible as this will assist the DPO in assessing whether further action is required.

Task Name:	
Directorate/Department:	
Is this a change to an existing process?	
Assessment Completed by:	
Job Title:	
Date completed:	
Phone:	
E-mail:	
Information Asset Owner:	
Task/Change Outline - *What* is it that is being planned?	
Purpose / Objectives - *Why* is it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the task.	
What is the purpose of collecting the information within the system? For example research, audit, reporting, staff administration etc.	
Provide a description of the information flows. Even if detailed information is not available some indication must be provided; this may already be available through requirements gathering. Broadly speaking the aim is to establish: **who** the information will be made available to, **what** type of information, **why** the information is required, **how** it will be shared and **how often**.	

Provide details of how the proposal will have the potential to impact on the confidence service users have in the Council maintaining the confidentiality of their personal data. For example, it could be that specific information is being gathered or used that hasn't been used or gathered previously; the level of information held about an individual is increasing or information is being shared with another organisation through a shared system or database where it wasn't previously.
Provide details of any previous Data Protection Privacy Impact Assessment or other form of personal data compliance assessment done on this initiative. If this is a change to an existing system, a DPIA may have been undertaken during the task implementation.
Stakeholders - who is involved in this task/change? Please list stakeholders, including internal, external, organisations (public/private/third) and groups that may be affected by this system/change in the table below and detail any stakeholder activity taken.

Organisation	Engagement / Stakeholder Activity

Stakeholders - Has there been any consultation with data subjects (the individuals that the system or proposed change will affect or impact)?
☐**Yes** **How was this done?** …… ☐**No**

Data Types

In order to understand the potential risks to individual's privacy, it is important to know the types of data that will be held and/or shared. Even if exact detail is not known and initial indication will assist in the privacy impact assessment.

Personal	Tick (All that Apply)	Special Category	Tick (All that Apply)
Name	☐	**Racial / ethnic origin**	☐
Address (home or business)	☐	**Political opinions**	☐
Postcode	☐	**Religious beliefs**	☐
NHS No.	☐	**Trade union membership**	☐
Email address	☐	**Physical or mental health**	☐
Date of birth	☐	**Sexual life**	☐
Reference number If ticked, please detail:	☐	**Genetic data / Biometrics; DNA profile, fingerprints**	☐
Driving Licence [shows date of birth and first part of surname]	☐		
Bank, financial or credit card details	☐		
Mother's maiden name	☐		
National Insurance number	☐		
Tax, benefit or pension Records	☐		
Criminal offences	☐		
Employment, school, Social Services, housing records	☐		
Data of a "higher" sensitivity (tick all that apply)			
Health condition information	☐	**Genetic**	☐
Mental Health	☐	**Adoption**	☐
Child Protection	☐	**Safeguarding Adults**	☐
Comments and Additional data types (if relevant):			

Section B – Privacy Impact Assessment Table [insert task name]

The **task lead** should complete the '*Response'* box for each question. The DPO will then complete the 'Risk Type' and 'Outcome' box

Guidance Notes:

Response - Please answer the questions as fully as possible. If you are unsure of how to answer the question, **please contact the Data Protection Officer (DPO).** If there is supporting information that relates to any of the questions, which you feel would be informative, indicate within the comments section and send this along with the completed assessment.

Additional guidance notes have been provided for some questions; once completed the guidance notes can be removed.

The assessment table is designed to be a 'working document' that can be added to at intervals throughout the process, for example bullet points or rough notes can be used. These notes can be used to highlight things that need to be followed up; noted requirements can be marked up ready for the requirement schedule, etc.

Risk Type – The DPO will use the guidance notes in Appendix 1 to identify the type of risk, this will help the organisation to judge the level of risk and either accept it or put in place appropriate measures to mitigate it.

Outcome – The DPO will use the information provided to decide if any potential IG risks are identified. If, following discussion with the task manager/lead it is agreed there is an IG risk that requires further action / management, the required actions will be noted on the DPIA. The risk will be scored and progress against the identified mitigations captured using a red/amber/green status. **If the DPIA identifies high risks and you are unable to take measures to reduce the risk, it is necessary to consult the Information Commissioner's Office before processing commences**

1	Is there any data stored in the cloud?		
	Guidance Note: *Please complete*		
	Response (completed by task lead)	**Risk type (completed by DPO)**	**Outcome (completed by DPO)**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
2	Where will the information be held and who will have responsibility for it?		
	Guidance Note: *Detail which team or organisation has responsibility for the system that holds the data. Detail which team or organisation has responsibility for the storage of the data. Detail how the servers are configured and Resilient. Detail which team or organisation is responsible for the security of the server the data is located on. Where is the server located physically?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
3	What types of information will be held and/or shared?		
	Guidance Note*: For example a care plan, case correspondence, occupational health data.* *Will the records be electronic or paper?*		
	Response	**Risk type**	**Outcome**

	Type here	☐ Individual ☐ Organisational ☐ Compliance	

4	Will any of the following activities be involved (tick those that apply): ☐ Recording of demographic data ☐ Sharing of personal data ☐ Transfer of service user identifiable data: to other systems, to other third parties ☐ Other

5	What legal basis for processing will you be relying on? Please tick one for personal data and one for special category data (if processing). Please speak to your information governance team if unsure.			
	Personal Data		**Special Category Data (includes health data)**	
	Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☐	Provision of preventative or occupational medicine, health or social care or treatment, or the management of health or social care systems – Art 9(2)(h)	☐
	Protection of vital interests – Art 6(1)(d)	☐	Vital interests of the data subject or a third party where they are incapable of giving consent – Art 9(2)(c)	☐
	Necessary for compliance with a legal obligation – Art 6(1)(c)	☐	Necessary for reasons of substantial public interest - Art 9(2)(g)	☐
			Public health - Art 9(2)(i)	☐
	Consent – Art 6(1)(a)	☐	Explicit Consent – Art 9(2)(a)	☐
	Other (please detail)	☐	Research – Art 9(2)(j)	☐
			Other (please detail)	☐
	Outcome			

6	Will the planned use of personal data be covered by information already provided to individuals or is a new or revised communication planned or required?		
	Guidance Note: *'Fair Processing' i.e. informing individuals of what is happening to their information is a requirement under Data Protection Legislation. What are the existing communications? What are the planned communications?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
7	Will the development enable the sharing of records with other organisations? How will records be shared?		
	Guidance Note*: Will information be transferred to a central hub with a collated record made available to participating organisations? Will participating organisations be provided with a view of records created in another organisation?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
8	Will the development result in the handling of a significant amount of new data about each person, or significant change in existing data holdings? Please detail the new data handled.		
	Guidance Note*: i.e. Is more information held about the same population of service users?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
9	Will the development result in the handling of **new data** about a significant number of people, or a **significant change in the population coverage**?		
	Guidance Note*: Please complete.*		

Response	Risk type	Outcome
Type here	☐ Individual ☐ Organisational ☐ Compliance	
Does the task involve **new linkage** of personal data with other data sets, or significant change in data linkages? Please list the linking systems		
***Guidance Note**: Is the development dependent on, or does it link to other systems such as Welsh Demographic Service, NHS system? Will the NHS Number be used as the common identifier? How will records be matched / linked. What measures will be in place to correctly match/link records?*		
Response	**Risk type**	**Outcome**
Type here	☐ Individual ☐ Organisational ☐ Compliance	
What security controls will be in place to prevent unauthorised or unlawful processing of information?		
***Guidance Note:** Describe any such measures (e.g. system controls such as role based access, audit notifications, etc.) and outline any possible implications?*		
Response	**Risk type**	**Outcome**
Type here	☐ Individual ☐ Organisational ☐ Compliance	
How is access to the system managed?		
***Guidance Note**: Who authorises accounts, manages role based access and disables accounts? Please detail who is responsible for the business processes*		
Response	**Risk type**	**Outcome**

Type here	☐ Individual ☐ Organisational ☐ Compliance	

13	What additional controls will be in place to deal with information of a higher sensitivity?		
	Guidance Note: *Consideration must also be given to name changes through adoption, public protection or gender change and records relating to genetics, mental health, and occupational health.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
14	What are the retention periods for the personal information and how will this be implemented?		
	Guidance Note*: Within the record keeping system, there must be a method of deciding 'what is a record?' and therefore 'what needs to be kept?' This is described as 'declaring a record'. A declared record is then managed in a way that will hold it in an accessible format until it is appraised for further value or it is destroyed, according to retention policy that has been adopted.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
15	How will you action requests from individuals for access to their personal information (in accordance with their rights)?		
	Guidance Note*: Under relevant Data Protection legislation, individuals have a right to ask for a copy of information held about them. If this is a shared record it must be established who will be responsible for dealing with the request.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
16	Will there be any secondary use of personal information in an identifiable or non-identifiable form?		

	Guidance Note: *Will the information be used for anything other than the main stated purpose? What level of information is to be used for these purposes, how will it be managed and how it will be communicated to service users?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
17	How are users to be trained in their information governance responsibilities? Have any training needs been identified in addition to the mandatory Council data protection training? Please detail training in full.		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
18	Is the information you are using likely to be of good enough quality for the purpose it is used for?		
	Guidance Note*: Consider the flow process, and how often, the information is checked for accuracy and are there procedures to support this? Is there is a facility to deal with data inaccuracies? Is there a facility to record the source of the information?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
19	Will the task involve any data migration or transfer of records from other systems/new feeds? If so, will the system origin and whether they were digitally born be captured in the metadata as part of the transfer process?		
	Guidance Note: *If the task involves any data migration, new feeds? If so, what are the identifiers used? Will the data be maintained in an accessible format? Will the relevant metadata be captured such as whether the information is scanned in, the author, scanner, transcriber, system origin etc.*		
	Response	**Risk type**	**Outcome**

	Type here		
20	Does the system maintain a comprehensive audit trail of user activity and how will the audit log be accessed and analysed?		
	Guidance Note: *Who will be responsible for auditing? Will additional or new organisational processes be required to meet the requirement to audit all user access?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
21	Will the information be transferred (electronically, physically or by other portable means) to an organisation outside of the Council? Please list the organisations.		
	Guidance Note: *Where will it go and what security arrangements will apply (e.g. encryption)? Will removable media be used? How will the information be transported (e.g. telephone, post, secure file sharing portal, email)?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
22	Are there business continuity and disaster recovery plans in place to recover information which may be damaged or lost through human error, computer virus, network failure, theft, fire, flood or other disaster?		
	Guidance Note: *Has this been agreed as part of the Service Management arrangements?*		
	Response	**Risk type**	**Outcome**

	Type here	☐ Individual ☐ Organisational ☐ Compliance	
23	Are there any elements of the system or service that are provided by a third party?		
	Guidance Note: *Is there a contractor (and any sub-contractors?) If so please document who the contracting authority is, who the contractors are and the confidentiality provisions within the contract, please note whether the procurement has been subject to information governance input, and whether the organisation is registered with the information commissioner*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
24	Does the development involve the use of new or inherently privacy invasive technologies?		
	Guidance Note: *For example: smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies and intelligent transportation systems, visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
25	Is automated decision making involved?		
	Guidance Note: *Is there any profiling involved? Can there be any human intervention if required?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	

26	One of the principles of data protection is to process no more personal data than necessary. Is all information being processed by the task necessary?		
	Response	**Risk type**	**Outcome**
	☐Yes ☐No If no, please detail Type here ……	☐ Individual ☐ Organisational ☐ Compliance	
27	Has this task been detailed on the information asset register?		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
Name ……			Date: ……

Risk Type – this is the 'classification' as noted on the DPIA table (risk to individuals, compliance risk, organisation/corporate risk) and is noted in Section B.

Risks to individuals	Compliance risk	Associated organisation/corporate risk
• Inadequate disclosure controls increase the likelihood of information being shared inappropriately. • The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge. • New surveillance methods may be an unjustified intrusion on their privacy. • Measures taken against individuals as a result of collecting information about them might be seen as intrusive. • The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect. • Identifiers might be collected and linked which prevent people from using a service anonymously. • Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. • Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised. • Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk. • If a retention period is not established information might be used for longer than necessary.	• Non-compliance with the common law duty of confidentiality • Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015 • Non-compliance with the relevant data protection legislation • Non-compliance with the Privacy and Electronic Communications Regulations (PECR). • Non-compliance with sector specific legislation or standards. • Non-compliance with human rights legislation.	• Non-compliance with the relevant data protection legislation or other legislation can lead to sanctions, fines and reputational damage. • Problems which are only identified after the task has launched are more likely to require expensive fixes. • The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation. • Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business. • Public distrust about how information is used can damage an organisation's reputation and lead to loss of business. • Data losses which damage individuals could lead to claims for compensation.

Risk Scoring Tables

Likelihood score	1	2	3	4	5
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency How often might an IG breach occur	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it may not be a persisting issue	Will undoubtedly happen/recur,possibly frequently

Impact score (severity levels) and examples of descriptors	**1**	**2**	**3**	**4**	**5**
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on an individual's privacy and confidentiality	Minimal privacy impact requiring no/minimal intervention Other manual or electronic process in place to mitigate the IG risk	Minor impact on an individual's privacy Other manual or electronic process in place to mitigate the IG risk	Moderate privacy impact requiring professional intervention Aspects of reputational damage for the organization if IG requirement not adopted Could result in an event which impacts on a moderate (less than 100) number of individuals	Major breach leading to possible larger scale privacy breaches Mismanagement of patient/client privacy with long-term reputational issues Would impact on over 100 individuals – part system failure	Serious IG breach and non-compliance with the law if requirement not adhered to An event which impacts on a large number of individuals – full system breach because of no adherence to standards. Is likely to be 1000 of individuals

		Likelihood				
		1	**2**	**3**	**4**	**5**
		Rare	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Impact Score	**5 Catastrophic**	5	10	15	20	25
	4 Major	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	4	6	8	10
	1 Negligible	1	2	3	4	5

Status

1 - 3	Low risk
4 - 6	Moderate risk
8 - 12	High risk
15 - 25	Extreme risk

Appendix 6

Use of Digital images/video

Enw'r Plentyn/Child's Name……

Bydd yr Ysgol yn cydymffurfio gyda Deddfwriaeth Diogelu Data ac yn gofyn caniatâd cyn cyhoedddi lluniau sydd wedi'i dynnu. Bydd delweddau yn cael eu defnyddio i ddathlu llwyddiannau wrth gyhoeddi hynny mewn cylchlythyrau, papurau newydd lleol, ar wefan Ysgol ac ar wefannau cymdeithasol megis 'Facebook', 'Twitter', 'Instagram'

Unwaith mae'r lluniau / delweddau yn mynd allan ar wefannau cymdeithasol, nid yw'n bosib dileu yn llwyr
Mae gennych yr hawl i dynnu eich caniatâd yn ôl ar unrhyw adeg.

The school will comply with Data Protection legislation and ask for permission before publishing images taken. Images will be used to celebrate successes and will be announced in newsletters, local newspapaers, on the school website and, at times, on social media – 'Facebook', 'Twitter', and 'Instagram'

Once the pictures / images go out on social websites, it is not possible to delete totally

You have the right to withdraw your consent at any time.

Rwy'n rhoi caniatâd i'r ysgol cyhoeddi lluniau / fideos o'm plentyn i gael eu defnyddio. Rwyf yn deall mai dim ond i gefnogi gweithgareddau dysgu neu mewn cyhoeddusrwydd sydd yn dathlu llwyddiant ac yn hyrwyddo gwaith yr ysgol yn rhesymol defnyddir y delweddau yma:

I give permission for the school to publish pictures/videos of my child, I understand that these images will only be used to support learning activities or for publicity to celebrate successes and to reasonably to promote the schools work:

e. tu fewn i'r ysgol, cylchlythyrau / within the school, newsletters ☐

f. gwefan yr ysgol / the school website ☐

g. Facebook/Twitter/Instagram ☐

h. Papur newydd lleol/Local newspaper ☐

Nid wyf yn rhoi caniatâd o gwbl / I do not give permission at all ☐

Enw/Name……..

Perthynas/Relationship……..

Arwyddo/Signed……

Dyddiad/Date……

Appendix 7

Use of Biometric Systems

The school uses biometric systems to identify individual children by means of the following methods *(the school should describe how it uses the biometric system here).*

Biometric technologies have specific advantages over other automatic identification systems, as there is no need for the pupils to bring anything *(to the school canteen or library)* , therefore, nothing can be lost, such as a key card.

The school has completed a privacy impact assessment and is confident that using such technologies is effective and has been justified in the school context.

Full images of *fingerprints / palm prints* will not be stored, and the original image cannot be re-created from the data. That is, a pupil's fingerprint or even an image of a fingerprint cannot be re-created using, what is in essence, a row of numbers.

Parents / guardians will be asked for their consent for their child to use biometric technology.

Name of Parent / Guardian	
Name of Student / Pupil	

As the parent / guardian of the above pupil / student, I agree that the school can use the biometric identification systems described above. I understand that these images cannot be used to create my child's full fingerprint / palm print, and that these images will not be shared with anyone outside the school.

Yes / No

Signature	
Date	