Polisi Diogelu Data 2025

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

Data Protection Policy 2025

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

Rhif y fersiwn ***Version number***	**0.3**
Dyddiad Cyhoeddi ***Publication Date***	**11/2025**
Dyddiad cymeradwyo ***Date Adopted***	**Gorffennaf 2026**

~~F~~ersiwn cyfredol/ *Current Version*

Hanes Fersiwn/*Version History*

Fersiwn/Version	Dyddiad/Date	Awdur/Author	Arsylwadau/Observations
0.1	**05.2018**	**Mai Bere**	Polisi yn dilyn cyflwyniad y ddeddf GDPR *Policy following the introduction of the GDPR act*
0.2	**10.2019**	**Louise Jones**	Ychwanegu manylion am casgliad gwybodaeth COVID *Adding details about COVID information collection*
0.3	**09.2025**	**Louise Jones**	Newidiadau; – cyfnodau cadw Ychwanegu – 9.2-9.5 – DPIA – ROPA – Apendics 4 *Changes;* – *Retention periods* *Additions* – *9.2-9.5* – *DPIA* – *ROPA*

			– *Apendics 4*

Llofnodwyd ar ran Cadeirydd y Llywodraethwyr/*Signed by the Chairman of Governors*:

_____

06.07.26
Dyddiad/*Date*: _____

Cynnwys

Contents

Atodlenni'r Ddeddf	Appendix 1	Schedules of the Act
Yr hawl i gael mynediad at wybodaeth	Appendix 2	The right to access to information
Digwyddiad Torri Data	Appendix 3	Data Breach
Asesiad o'r Effaith ar Diogelu Data	Appendix 4	Data Protection Impact Assessment
Ffurflen ganiatâd ffotograffau	Appendix 5	Photographs consent form
Ffurflen ganiatâd gwybodaeth biometrig	Appendix 6	Biometric information consent form

Cyfnodau Cadw	Mewnrwyd Ysgolion Gwynedd - - - Rhestrau Gadw - All Documents	Rentention Periods

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 gweithwyr y dyfodol, 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 rwymedigaethau o dan y ddeddfwriaeth a bydd yn adolygu gweithdrefnau yn gyson er mwyn sicrhau ei fod yn gwneud hynny.

Diffiniadau

Data Personol	Gwybodaeth sydd yn ymwneud ag unigolyn byw y gellir ei adnabod sydd yn 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 sydd yn dweud rhywbeth wrthych am unigolyn byw y gellir ei adnabod. Mae'r egwyddorion hefyd yn ymestyn at yr holl wybodaeth mewn 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	Gwybodaeth sydd yn ymwneud â hil neu ethnigrwydd, barn wleidyddol, crefydd, 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.
DDD	Yn golygu Deddfwriaeth Diogelu Data yn unol â GDPR y DU a Deddf Diogelu Data 2018
Toriad data	Torri diogelwch sy'n arwain at ddifrodi, colli, newid neu ddatgelu data personol a drosglwyddir, sydd wedi'i storio neu ei brosesu fel arall, a hynny'n ddamweiniol neu'n anghyfreithlon.

Swyddfa'r Comisiynydd Gwybodaeth (ICO)	Yr ICO yw corff annibynnol y Deyrnas Unedig (awdurdod goruchwylio) a sefydlwyd i gynnal hawliau gwybodaeth. Rôl yr ICO yw cynnal hawliau gwybodaeth er budd y cyhoedd.
Rheolydd data	Y bobl, neu'r sefydliadau, sy'n pennu'r dibenion y caiff data personol eu prosesu ar eu cyfer, a'r ffordd y caiff unrhyw ddata personol ei brosesu. Mae gan y rheolydd data gyfrifoldeb i sefydlu arferion a pholisïau yn unol â deddfwriaeth. Mae'r ysgol yn rheolydd data.
Proseswyr data	Yn cynnwys unrhyw berson sy'n prosesu data personol ar ran rheolydd data (ac eithrio cyflogai'r rheolydd data). Gallai proseswyr data gynnwys cyflenwyr sy'n trin data personol ar ran yr ysgol.
Testun y data	Yr unigolyn y mae'r wybodaeth bersonol yn ymwneud ag ef. Gall hyn gynnwys, ond nid yw'n gyfyngedig i Staff, Disgyblion, Llywodraethwyr yr ysgol.
Swyddog Diogelu Data (DPO)	Mae DPO yn cynorthwyo i fonitro cydymffurfiaeth fewnol, hysbysu a chynghori ar rwymedigaethau diogelu data, gweithredu fel pwynt cyswllt ar gyfer testunau data a'r awdurdod goruchwylio.
Systemau TGCh	Cyfrifiaduron prosesu gwybodaeth neu systemau cyfathrebu data.
Gwybodaeth trydydd parti	Trydydd parti yw rhywun nad yw'n rheolydd data, y prosesydd data, neu'r gwrthrych data.
Cywirdeb	Cadw'r wybodaeth yn gyflawn, yn gywir ac yn ddilys.
Risg	Effaith ansicrwydd ar amcanion. Risgiau i unigolion: y potensial ar gyfer niwed neu ofid. Nodweddir risg yn aml drwy gyfeirio at "ddigwyddiadau" a "chanlyniadau", neu gyfuniad o'r rhain.
Anawdurdodedig	Heb hawl gyfreithlon.

1. 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, dyfeisiau llechen a 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.

2. Cyfrifoldebau

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

Y **Pennaeth** sy'n 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 ar gyfer yr holl staff.

Mae **pob aelod staff** neu gontractwyr sydd yn 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 fynegi eu bod wedi darllen, deall a derbyn y polisi hwn.

3. Gofynion

Mae Ddeddf Diogelu Data yn nodi bod 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;

1) dylid ei brosesu mewn **dull cyfreithiol, teg a thryloyw**
2) 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;
3) bydd y wybodaeth yn **ddigonol, yn berthnasol ac nid yn ormodol** o'i gymharu â diben neu ddibenion ei phrosesu;
4) bydd y **wybodaeth yn gywir** a, pan fo hynny'n briodol, yn hollol gyfredol;
5) ni ddylid cadw'r wybodaeth yn **hirach nag sydd rhaid** ar gyfer y diben neu'r dibenion hynny;
6) bydd y wybodaeth yn cael ei **chadw'n ddiogel**, h.y. ei gwarchod gan raddfa briodol o ddiogelwch.

Fel Rheolydd Data, mae'n ofynnol i'r Ysgol cadw cofnod mae gofyn i'r ysgol gadw **Cofnod o weithgareddau prosesu (ROPA)** sy'n ddogfen fyw sy'n ddisgrifio pob math o data personol mae'r Ysgol yn ei reoli a/neu ei brosesu. Dylai'r rhestr gynnwys;

- 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
- Y sail gyfreithiol sy'n cael ei dibynnu arno i brosesu'r data
- Y mesurau diogelwch ar waith i diogelu'r data

Mae gofyn i'r ysgol dalu ffi flynyddol i Swyddfa'r Comisiynydd Gwybodaeth (ICO).

Gallai methu â gwneud hynny arwain at gosb ariannol.

4. Datganiad Preifatrwydd

Pryd bynnag y casglir 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.

5. Amodau ar gyfer Prosesu

Gellir prosesu data personol dim ond pan fo un o amodau **Erthygl 6** y GDPR wedi cael eu bodloni.
Gellir prosesu data categori arbennig dim ond pan fo amod yn **Erthygl 9** GDPR y DU wedi cael ei fodloni yn ogystal ag un yn Erthygl 6.

Gweler **Atodiad 1** am restr o'r amodau.

6. Datgelu Data

Mae'n **drosedd** cael neu ddatgelu gwybodaeth am unigolyn yn fwriadol neu'n fyrbwyll heb achos cyfiawn.

- Ni ddylai'r ysgol ddatgelu unrhyw beth am gofnod y disgybl;

- a 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 dim ond rhoi **data perthnasol, cyfrinachol** i:

- aelodau staff eraill ar sail angen gwybod;

- 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.

7. Hawliau unigolion

7.1 Mynediad at wybodaeth amdanynt eu hunain

Mae gan bawb yr **hawl i gael mynediad** i wybodaeth a gedwir amdanynt. Fodd bynnag, o ran plant, mae hyn yn ddibynnol ar eu gallu i ddeall ac ar natur y cais. Gall yr unigolyn fod yn ddisgybl, yn rhiant neu'n aelod o staff.

Gweithredu cais

Gellir gwneud ceisiadau am wybodaeth yn ysgrifenedig, sy'n cynnwys e-bost, ar wefannau cyfryngau cymdeithasol ysgolion, neu ar lafar. Os nad yw'r cais cyntaf yn adnabod y wybodaeth sydd ei angen yn glir, yna gwneir ymholiadau pellach.

Mae'n rhaid **sefydlu hunaniaeth** y sawl sy'n gwneud y cais cyn datgelu unrhyw wybodaeth, a dylid cynnal gwiriadau ynghylch prawf y berthynas i'r plentyn.

Gellid sefydlu tystiolaeth o hunaniaeth gan ofyn am ddangos:

- Pasbort
- trwydded yrru
- biliau cyfleustodau gyda'r cyfeiriad presennol (a gyhoeddwyd o fewn y 3 mis diwethaf. Nid yw biliau ffôn symudol yn dderbyniol)
- Tystysgrif Geni / Priodas
- P45/P60
- Datganiad Morgais neu Gerdyn Credyd

Nid yw'r rhestr hon yn gyflawn.

Mae dau fath penodol o hawl i gael mynediad at wybodaeth a ddelir gan ysgolion am fyfyrwyr.

- O dan ddeddfwriaeth diogelu data, mae gan unigolion yr hawl i wneud cais i gael mynediad at gopi o'r **wybodaeth bersonol** a gedwir amdanynt y cyfeirir ato'n gyffredin fel Cais Gwrthrych y Data (SAR)
- Bydd hawl y rhai hynny sydd â hawl i gael mynediad at **gofnodion addysgol** fel y'i diffinnir o fewn Rheoliadau Gwybodaeth am Ddisgyblion (Cymru) 2011.

ii. Darparu data i blant

Mewn perthynas â gallu plentyn i wneud cais am ei **ddata personol,** 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 yn gynt; **dylid ystyried aeddfedrwydd pob plentyn ar sail bob achos unigol.**

iii. Hawliau rhieni

Mae gan rieni eu hawl annibynnol eu hunain dan Reoliadau Gwybodaeth am Ddisgyblion (Cymru) 2011 i gael mynediad at **gofnodion addysgol** swyddogol eu plant.

Gall oedolyn sydd â **chyfrifoldeb rhiant** gael mynediad at y wybodaeth am eu plentyn, ar yr amod nad yw'r plentyn yn cael ei ystyried yn ddigon aeddfed.

- Rhaid iddynt allu profi eu cyfrifoldeb fel rhiant ac mae gan yr ysgol hawl i ofyn am y ddogfennaeth berthnasol i brofi hyn yn ogystal â phrawf o bwy yw'r sawl sy'n gwneud y cais.

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.

Gall plentyn sydd â'r gallu i ddeall wrthod cytuno i gais y rhieni am ei gofnodion (SAR).

Nid oes gan fyfyrwyr hawl i atal eu rhieni rhag cael copi o'u cofnodion addysgol oni bai bod amgylchiadau lliniarol.

Gwybodaeth Ychwanegol

Yr amser a ganiateir i ymateb i **Gais Gwrthrych y Data (SAR)**, ar ôl cael 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 yr un mis yn dechrau hyd nes y bydd hunaniaeth y sawl sy'n gwneud y cais wedi'i gadarnhau a bod eglurhad o'r wybodaeth a geisir wedi'i dderbyn.

Gellir ymestyn y cyfnod o hyd at ddeufis, os yw'r cais yn gymhleth neu'n niferus neu'n cael ei ystyried yn afresymol ar y sail ei fod yn amlwg yn ormodol ac yn ddi-sail. Bydd yr ysgol yn hysbysu'r ymgeisydd o fewn mis bod y cyfnod ymgeisio i'w ymestyn a'r rheswm pam. Caniateir hyd at ddeufis arall i fodloni'r cais mewn amgylchiadau o'r fath.

Mae'r term **'amlwg ddi-sail'** yn cael ei ddiffinio fel un sydd ddim yn ddidwyll ac sydd heb unrhyw wir ddiben.
Mae'r term **'gormodol'** 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 allu arddangos pam fod y cais yn ddi-sail neu'n ormodol.
Mae Deddf Diogelu Data 2018 yn caniatáu ar gyfer eithriadau i ddarparu gwybodaeth benodol; felly, bydd **yr holl wybodaeth yn cael ei hadolygu cyn ei datgelu.**
Ni ddylid datgelu unrhyw wybodaeth a allai niweidio iechyd corfforol neu feddyliol neu gyflwr emosiynol y disgybl neu unrhyw berson arall yn sylweddol. Ni ddylid datgelu gwybodaeth bod y plentyn mewn perygl o gamdriniaeth, nac unrhyw wybodaeth sy'n ymwneud ag achos llys.

Mae gwybodaeth trydydd parti yn wybodaeth sydd wedi'i darparu gan eraill, megis yr Heddlu, yr Awdurdod Lleol, gweithiwr gofal iechyd proffesiynol neu ysgol arall. Fel arfer, mae angen caniatâd i ddatgelu gwybodaeth gan drydydd partïon. Mae angen cadw'r amserlen yr un fath.
Dylid gofyn am gyngor pellach os oes unrhyw bryder ynglŷn â datgelu gwybodaeth.

Dylai'r wybodaeth a ddatgelir fod yn glir, felly bydd angen egluro unrhyw godau neu dermau technegol. Os yw'r wybodaeth a gynhwysir yn anodd ei darllen neu ei deall, dylid ei theipio eto.

Pan fo gwybodaeth wedi'i golygu, dylid cadw copi cyflawn o'r wybodaeth a ddarperir i sefydlu beth gafodd ei olygu a pha resymau dros olygu a ddefnyddiwyd yn achos cwyn.

Rhaid i geisiadau am **Gofnodion Addysgol** gael eu hateb o fewn **15 diwrnod ysgol** o dderbyn cais ysgrifenedig gan riant. Rhaid i'r Pennaeth sicrhau bod y cofnodion ar gael i'w harchwilio, yn rhad ac am ddim, i'r rhiant.

Rhaid i geisiadau am gopi o **gofnod addysgol disgybl** gael eu hateb pan delir ffi o'r fath (heb fod yn fwy na chost y cyflenwad), os o gwbl, **fel y pennir gan y Corff Llywodraethu**. 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 sydd wedi'u darparu mewn hysbysiad preifatrwydd.

Gellir darparu gwybodaeth yn yr ysgol gydag aelod o staff ar gael i helpu ac egluro materion os oes angen, neu gellid ei darparu 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.

7.2 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**. Gweler Atodlen 2.

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.

7.3 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** amdanynt eu hunain. Bydd yr ysgol yn ystyried pob cais ar sail unigol.

7.4 Yr hawl i wrthwynebu neu i gyfyngu ar y prosesu

Mae gan bob unigolyn yr hawl i **wrthwynebu** i'w gwybodaeth gael ei phrosesu o 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.
- mae unigolion wedi gwrthwynebu.
- mae prosesu yn anghyfreithlon, a
- lle nad yw'r ysgol angen y data ond mae ar 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 o bwy yw'r trydydd partïon hyn.

8. Diogelwch

8.1 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 yn rhaid mynd â'r dogfennau o'r ysgol.

8.2 Dyfeisiau Electronig

Dylai'r ysgol gadw **cofnod cyfredol o ddyfeisiau electronig** sy'n gysylltiedig â myfyrwyr yn ogystal ag aelodau staff unigol.

Dylid cadw pob dyfais gludadwy electronig mor ddiogel â phosib ac o dan glo pan nad yw'n cael ei defnyddio. Rhaid i bob dyfais gael ei diogelu gan gyfrinair.

Ni anogir y defnydd o gyfryngau symudadwy (**Dyfeisiau USB/cofbinnau** neu ffurf arall o gadw gwybodaeth nad yw'n rhan o'r cyfrifiadur ei hun) sy'n cadw gwybodaeth bersonol a chyfrinachol.
Dylid defnyddio meddalwedd amgryptio i amddiffyn pob dyfais gludadwy a chyfryngau symudadwy, megis gliniaduron a dyfeisiadau USB.

Os defnyddir cyfryngau symudadwy a/neu ddyfeisiau USB, rhaid trosglwyddo data i safle SharePoint yr ysgol ac yna ei waredu'n ddiogel.

Dylid annog **cyfrineiriau cryf**, h.y. o leiaf wyth nod a chynnwys symbolau arbennig os yw unrhyw gyfarpar electroneg yn dal gwybodaeth bersonol gyfrinachol.

- **Ni ddylid rhannu cyfrineiriau o gwbl**.
- Dylid defnyddio gwahanol gyfrineiriau ar gyfer gwahanol systemau a dyfeisiadau.

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

8.3 E-bost

Rhaid i **Fusnes Swyddogol yr Ysgol,** gan gynnwys corff Llywodraethu'r ysgol, gael ei anfon yn defnyddio 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. Mae gwirio pwy yw'r derbynyddion a defnyddio BCC yn hanfodol i leihau'r risg o dorri diogelwch data.

8.4 Dyfeisiau Symudol

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.

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.

8.5 Cyfrifon Hwb a One Drive

Dim ond **gwybodaeth am ddatblygiad proffesiynol** ddylid ei storio o fewn cyfrifon *One Drive* a HwB unigol.
Dylid trosglwyddo busnes/dogfennaeth swyddogol yr ysgol i system ffeilio *SharePoint* swyddogol yr ysgol.

9. Prosesu Data

Dylai staff yr ysgol gymryd gofal wrth gofrestru i ddefnyddio unrhyw systemau, rhaglenni neu apiau addysgol a ddarperir gan sefydliad/darparwr allanol.
Dylai fod yn glir sut mae gwybodaeth bersonol yn cael ei defnyddio a'i phrosesu.
Yr ysgol, fel y rheolydd data, sydd â'r cyfrifoldeb terfynol am y data personol.

Mae'r ysgol yn gyfrifol am asesu **cymhwysedd proseswyr** data gyda *gofynion GDPR y DU* .

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

Mae angen i'r ysgol, fel rheolydd data, sicrhau bod **cytundebau prosesu angenrheidiol** yn eu lle cyn i unrhyw wybodaeth gael ei rhannu.

Dylid cymryd gofal pan fydd systemau, rhaglenni neu apiau eisiau cael mynediad at, neu eisiau tynnu data o, systemau ysgol eraill h.y. system MIS yr ysgol
Rhaid i unrhyw **risgiau a mesurau lliniaru** gael eu hystyried **cyn comisiynu'r darparwr**.

Rhaid cwblhau **DPIA (Asesiad Effaith Diogelu Data)** 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 Swyddog Diogelu Data yr Ysgol i'w adolygu a'i awdurdodi. Gweler **Atodiad 4**

10. 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) mewn lle 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/rhannu data**.
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 derbynnir cais am wybodaeth gan yr Heddlu, dylid hefyd gynnwys ffurflen SA3 wedi'i chwblhau yn llawn sy'n cynnwys yr holl wybodaeth berthnasol. Dylai'r holl wybodaeth berthnasol, ofynnol fod yn bresennol cyn datgelu gwybodaeth.

Dylai'r Ysgol ddilyn y **Gweithdrefn Rhannu Gwybodaeth gyda'r Awdurdodau Heddlu'r Deyrnas Unedig**

Dylid anfon y cais ymlaen at y Swyddog Diogelu Data Ysgolion er mwyn ei awdurdodi.

11. Toriad/Digwyddiad Data

Mae toriad/digwyddiad data yn golygu bod gwybodaeth bersonol wedi cael ei **chyfaddawdu neu cholli**, a allai fod wedi digwydd o ganlyniad i ddigwyddiad seiber; data wedi'i adael mewn lleoliad anniogel; data wedi'i bostio at y derbynnydd anghywir; colli neu ddwyn gwaith papur neu ddyfais anniogel, ac ati.

Rhaid i'r ysgol adrodd am unrhyw doriadau data i'r Swyddog Diogelu Data Ysgolion (SDD) ar unwaith, gan ddefnyddio'r dogfennau perthnasol yn **Atodiad 3**
Bydd y SDD yn ymchwilio ac yn cymryd camau adfer priodol.

Rhaid adrodd am doriadau data difrifol i Swyddfa'r Comisiynydd Gwybodaeth o fewn 72 awr o ganfod y tor-rheol.

12. Rheoli Asedau

Mae'r ysgol yn berchen ar lawer o asedau gan gynnwys dyfeisiau ac offer a roddir i staff i ymgymryd â'u gwaith. Mae'r asedau hyn yn cynnwys, ond heb fod yn gyfyngedig i;

- Cyfrifiadur Personol/Gliniadur
- Ffonau symudol a dyfeisiau data symudol, sef dyfeisiau llechen (*Ipad*).
- Camerâu

Dylid cymryd pob gofal rhesymol i **ddiogelu asedau** rhag difrod a cholled neu ladrad. Mae aelodau staff yn gyfrifol am ofalu am asedau a roddir iddynt bob amser p'un a ydynt yn cael eu defnyddio, eu storio neu eu cludo o un lle i'r llall.
Os bydd yr ased yn cael ei golli neu ei ddwyn, rhaid rhoi gwybod am hyn ar unwaith i'r rheolwr llinell.

Mae'n gyfrifoldeb ar yr ysgol i gynnal **cofrestr asedau** a fydd yn galluogi adnabod perchnogaeth ar unrhyw adeg. Dylai'r gofrestr hon **gael ei chadw'n gyfredol** bob amser ac yn gynnwys;

- **Disgrifiad o'r ased** - e.e. gliniadur, ffôn symudol, camera, IPad
- **Rhif Adnabod unigryw** – neilltuo rhif unigryw i bob ased er mwyn cyfeirio'n hawdd ac i atal dyblygu
- **Perchennog Asedau Gwybodaeth** – Nodi'r unigolyn sy'n gyfrifol am bob ased

13. Cadw Data a Rheoli Cofnodion

Dylid cadw cofnodion mewn modd fel y gallai'r unigolyn dan sylw eu hymchwilio. Dylid hefyd cofio 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, yn ddiduedd, yn ddiamwys** ac yn hawdd i'w ddehongli/darllen.

Pan ceir 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 ac yn unol â chyfnodau cadw'r ysgol (sydd ar gael yn yr ysgol).

Mae'r cyfnodau cadw ar gael Mewnrwyd Ysgolion Gwynedd - - - Rhestrau Gadw - All Documents

14. Gwaredu

Unwaith y bydd y cyfnod cadw wedi dod i ben, rhaid adolygu'r cofnod a'i **waredu'n ddiogel** a chywir **yn unol â chyfarwyddiadau gwaredu**.

Os cedwir unrhyw wybodaeth gyfrinachol ar **gofnodion papur**, dylid cael gwared arnynt yn ddiogel trwy dorri neu drwy ddefnyddio gwasanaethau gwastraff cyfrinachol.
Dylid dileu neu ddinistrio **Cofnodion Electronig**, a chadw tystysgrif dinistrio.

15. 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**.

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 yr ysgol yn cydymffurfio â'u **polisi gwefan/cyfryngau cymdeithasol mabwysiedig** lle bo hynny'n berthnasol.

Rhaid i unigolion gael gwybod am ganlyniadau eu data yn cael ei ledaenu ledled y byd ar y ffurflen ganiatâd fel y gallant wneud dewis gwybodus.

16. Ffotograffau

Mae'n bosib y bydd ffotograffau a dynnir ar gyfer **defnydd swyddogol yr ysgol** wedi'u cynnwys gan y Ddeddf Diogelu Data (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.

Mae **enghraifft** o ffurflen ganiatâd yn cael ei ddarparu yn **Atodiad 5**

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 yr ysgol yn anfon neges at bob rhiant ar ddechrau pob blwyddyn academaidd i **adolygu unrhyw ganiatâd** a roddir a bydd caniatâd yn cael ei adolygu cyn i unrhyw ffotograffau gael eu tynnu a/neu eu postio ar dudalennau cyfryngau cymdeithasol yr ysgol/gwefan/llawlyfr yr ysgol.

17. TELEDU CYLCH CYFYNG

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 cydymffurfio â'u **polisi TCC sydd wedi'i fabwysiadu** lle bo hynny'n berthnasol.

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.

18. Gwybodaeth Biometrig (lle bo hynny'n berthnasol)

Mae gwybodaeth biometrig yn golygu nodweddion mesuradwy, biolegol sy'n gallu adnabod unigolyn yn unigryw fel olion bysedd neu adnabod wynebau.
Mae **Deddf Diogelu Rhyddidau 2012** yn cynnwys mesurau sy'n ymwneud â defnyddio systemau adnabod biometrig.

O dan GDPR y DU, cydnabyddir bod y math hwn o ddata yn **ddata categori arbennig.**

Bydd yr Ysgol yn adfer **caniatâd ysgrifenedig** gan unigolion **cyn prosesu** eu data biometrig.

Ar gyfer pob disgybl ysgol o dan 18 oed, bydd yr ysgol yn cael **caniatâd ysgrifenedig** rhieni **cyn** cofnodi a phrosesu manylion biometrig eu plentyn.

Bydd **dulliau amgen** o ddarpariaeth gwasanaeth ar gael os bydd unigolyn yn gwrthod rhoi caniatâd.

Darperir ffurflen ganiatâd ar gyfer gwybodaeth biometrig yn **Atodiad 6**

19. Hyfforddiant Staff

Bydd pob gweithiwr yn derbyn **Hyfforddiant Diogelu Data** priodol a fydd yn cynnwys cyrsiau **gloywi blynyddol**.

Bydd yr hyfforddiant yn berthnasol, yn gywir ac yn cael ei ddiweddaru i'r holl staff. Bydd yn canolbwyntio ar feysydd allweddol o ddiogelu data megis trin ceisiadau, rhannu data, diogelwch gwybodaeth, toriad data personol a rheoli cofnodion.

Bydd yr ysgol yn cadw **cofnod o ddyddiadau hyfforddiant staff** a phresenoldeb yn ogystal â chofnod o staff sydd wedi darllen, deall a derbyn y polisi hwn.

20. Hawliau mynediad - staff newydd/newid rôl/staff sy'n gadael

Rhaid i'r ysgol gael rheolaethau ar waith i sicrhau **cyfrinachedd, cywirdeb** ac **argaeledd** y data maent yn eu prosesu er mwyn cydymffurfio â'r polisi Diogelu Data a rheoliadau GDPR y DU.

Dylid cadw ac adolygu'r lefel mynediad a roddir i bob defnyddiwr (staff/disgyblion/Llywodraethwyr) fel rhan o gofnodion 'staff newydd/newid rôl/staff sy'n gadael' gan ganiatáu i fynediad gael ei ddiweddaru'n gywir pan fo angen.

Bydd pob **aelod o staff newydd** yn derbyn hyfforddiant diogelu data fel rhan o'u pecyn anwytho. Dylid ychwanegu manylion am hyn at gofnod hyfforddi staff.

Dylai unrhyw un **sy'n gadael yr ysgol** gael eu cynghori i lawrlwytho eu dogfennau personol o'u cyfrif HwB ac One Drive.
Dylai hawliau mynediad, ar bob system, i bawb sy'n gadael gael eu **dirymu ar eu diwrnod olaf** yn yr ysgol.

21. Torri'r polisi

Gall methiant aelodau staff i gydymffurfio â gofynion y DDD arwain at drydydd partïon yn cymryd camau difrifol yn erbyn yr 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.

22. Cwynion

Dylid gwneud cwynion am y gweithdrefnau uchod i **Gadeirydd y Corff Llywodraethol** fydd yn penderfynu a yw hi'n briodol ymdrin â'r gŵyn yn unol â threfn gwyno'r ysgol ai peidio. Gellir ymdrin â chwynion nad yw'n briodol ymdrin â hwy drwy drefn gwyno'r ysgol gan swyddog Diogelu Data'r Ysgol yn y lle cyntaf a'u cyfeirio at y

Comisiynydd Gwybodaeth os oes angen. Bydd manylion cyswllt pawb yn cael eu darparu gyda'r wybodaeth sy'n cael ei datgelu.

23. Cysylltiadau

Os oes gennych unrhyw ymholiadau neu bryderon ynghylch y polisïau / gweithdrefnau hyn, cysylltwch â'r **Pennaeth** yn y lle cyntaf neu'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

24. Adnoddau Defnyddiol

Pecyn penodol ar gyfer ysgolion gan Swyddfa'r Comisiynydd Gwybodaeth:
Ysgolion, prifysgolion a cholegau | ICO

HwB
Adnoddau cenedlaethol ar ddiogelwch ar-lein:
https://hwb.gov.wales/resources/resource/def9bffd-1fba-4902-9834-3ecca60bb7e7/cy

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 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	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	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.
DPL	Means Data protection Legislation in line with the UK GDPR and the Data Protection Act 2018
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed information.
Information Commissioner's Office (ICO)	The ICO is the UK's independent body (supervisory authority) set up to uphold information rights. The ICO's role is to uphold information rights in the public interest.
Data controller	The people, or organisations, which determine the purposes for which, and the way any personal data is processed. The data controller has a responsibility to establish practices and policies in line with legislation. The school is a data controller.

Data processors	Includes any person who processes personal data on behalf of a data controller (other than the employee of the data controller). Data processors could include suppliers which handle personal data on behalf of the school.
Data subject	The individual to whom the personal information relates. This can include, but is not limited to Staff, Pupils, Governors of the school.
Data Protection Officer (DPO)	A DPO assists to monitor internal compliance, inform, and advise on data protection obligations, act as a contact point for data subjects and the supervisory authority.
ICT Systems	Information processing computers or data communication systems.
Third-party information	A third party is somebody who is not the data controller, the data processor or the data subject.
Integrity	The preservation of the complete, accurate and validated state of information.
Risk	Effect of uncertainty on objectives. Risks to individuals: the potential for damage or distress. Risk is often characterised by reference to potential “events” and “consequences”, or a combination of these.
Unauthorised	Without a legitimate right.

1. 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, tablets and CCTV).

Any information created by the school and its staff becomes the property of the school.

Data Protection Legislation (DPL) does not apply to access to information about deceased individuals.

2. 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 staff members should express that they have read, understood and accepted this policy.

3. 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** (ROPA) which is a living document that describes all types of personal data the School controls and/or processes. The list should contain;

- 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 lawful basis being relied upon to process such data
- The security safeguards in place

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.

4. 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;

- 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.

5. 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** UK GDPR is met as well as one in Article 6.

See **Appendix 1** for a list of the conditions.

6. 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

7. Individuals' rights

7.1 Access to information about themselves

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. The individual may be a pupil, a parent, or a staff member.

Actioning a request

Requests for information can be made in writing, which includes email, on school social media sites, or verbally. Please see **Appendix 2**

If the initial request does not clearly identify the information required, then further enquiries will be made.

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.

There are two distinct rights of access to information held by schools about students.

- Under data protection legislation, individuals have the right to make a request to access a copy of the personal information held about them commonly referred to as a Subject Access Request (SAR)
- The right of those entitled, will have access to curricular and educational records as defined within The Pupil Information (Wales) Regulations 2011.

(ii) Provision of data to children

In relation to the capacity of a child to make a request for his/her **personal data,** 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.

(iii) Parents' rights

Parents have their own independent right under The Pupil Information (Wales) Regulations 2011 to inspect the official **curricular and educational records** of their children.

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.

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.

A child with competency to understand can refuse to consent to the parents request for their records (SAR).

Students do not have a right to prevent their parents from obtaining a copy of their educational records.

Additional Information

The time allowed to respond to a **Subject Access Request (SAR)**, once formally accepted, is **one month (not working days or school days, but calendar days, regardless of school holiday period).** However, the one month will not commence until after identification of the requester has been clarified and clarification of information sought received.

The period can be extended by up to two months if a request is complex or numerous or deemed unreasonable on the grounds it is 'manifestly excessive and unfounded. 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.

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.
The Data protection Act 2018 allows for **exceptions to the provision of certain information**; therefore, all information will be reviewed prior to disclosure.
No information that could significantly harm the physical or mental health or emotional state of the pupil or any other person should be disclosed. Neither should Information that the child is at risk of abuse, or any information relating to court proceedings be disclosed.

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 timescale needs to be kept the same.
Further advice should be sought if there is any concern about disclosure of information.

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.

Where information has been redacted, a complete copy of the information provided should be kept establishing what was edited and what reasons for redaction were used in the event of a complaint.

Requests for **Educational Records** must be answered within **15 school days** of receiving a written request by a parent. The Headteacher must make the records available for inspection, free of charge, to the parent.

Requests for a copy of a **pupil's educational record** must be answered on the payment of such fee (not exceeding the cost of supply) if any, as the **Governing body may prescribe**. 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.

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 considered** when deciding how to provide the information. If postal systems have to be used, then registered mail must be used.

7.2 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.

7.3 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.

7.4 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 based on 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.

8. Security

8.1 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.

8.2 Electronic Devices

The school should keep an **up-to-date record of electronic devices** connected to students as well as individual staff members.

All portable electronic devices should be kept as securely as possible and under lock and key when not in use. All devices must be password protected.

The use of removable media (**USB devices/memory sticks** or another form of memory storage not part of the computer itself) which hold confidential personal information, is discouraged.
Encryption software should be used to protect all portable devices and removable media, such as laptops and USB devices.

If removable media and/or USB devices are used, data must be transferred to the school SharePoint site then disposed of securely.

Strong passwords, i.e. at least eight characters long and containing special symbols, should be encouraged if any electronic equipment holds personal information.

- Passwords should never be shared.
- 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.

8.3 E-Mail

Official School business, including the school Governing body, 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. Checks made of recipients and the use of BCC is essential to reduce the risk of a data security breach.

8.4 Mobile Devices

Personal Mobile devices should **not be used** unless deemed completely necessary. Any personal information recorded on said device should be shared with the school immediately and deletion confirmed with a senior member of staff.

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

8.5 Hwb Accounts and One Drive

Only **professional development information** should be stored within individual One Drive and HwB accounts. Official school business/documentation should be transferred to the official school SharePoint filing system.

9. Data Processing

Care should be taken by school staff when signing up to using any educational systems, programmes or apps supplied by an external organisation/provider.
It should be clear how personal information is used and processed.

The school, as the data controller has the ultimate responsibility for the personal data.

The school is responsible for assessing the data processors competency line with *UK GDPR's* requirements.

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

The school, as data controller, needs to ensure that **necessary agreements** are in place prior to any information being shared.

Care should be given when systems, programmes or apps want access to, or want to extract data from, other school systems i.e the school MIS system
Any **risks and mitigation** must be considered before commissioning the provider.

DPIA (Data Protection Impact Assessment) must 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 review and authorisation. See **Appendix 4**

10. 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) must be covered by a **data processing agreement**.

The UK GDPR does not prevent the School from 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 fully completed SA3 form containing all relevant information. All relevant, required information should be present prior to disclosure of information

The School should follow the **Information sharing procedure with United Kingdom Police Authorities**

The request should be forwarded to the School Data Protection Officer for authorisation.

11. Data Breach

A data breach means that personal information has been compromised or lost which could be because 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 and take appropriate remedial action.
Serious data breaches must be reported to the Information Commissioner's Office within 72 hours of identifying the breach.

12. Asset Management

The school own many assets including devices and equipment given to staff to undertake their jobs.
These assets include, but is not limited to;

- Personal Computer/Laptop
- Mobile phones and mobile data devices, namely tablets(Ipad).
- Cameras

Every reasonable care should be taken to **protect assets** from damage and loss or theft. Staff members are responsible to always look after assets issued to them whether it's being used, stored, or transported from one place to another.
Should the asset be lost or stolen, this must be reported immediately to the line manager.

It is the responsibility of the school to maintain an **asset register** which will enable identification of ownership at any given time. This register should be always **kept up to date**. The register should include the following:

- **Asset description** – a description of the asset e.g laptop, desktop,phone, ipad

- **Unique Identification Number** – assign a unique ID to each asset for easy reference and to prevent duplication
- **Information Asset Owner** – Identify the individual responsible for each asset.

13. 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 and in line with the school retention periods (available at the school).

The retention periods for documents can be found Mewnrwyd Ysgolion Gwynedd - - - Rhestrau Gadw - All Documents

14. Disposal

Once the retention period has expired, the record must be reviewed and **disposed of securely** and correctly **in line with disposal instructions**.

If any confidential information is held on **paper records**, they should be disposed of securely by shredding or by using confidential waste services.
Electronic records should be erased or destroyed, and a certificate of destruction kept.

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

The school will comply with their adopted **website/social media policy** where applicable.

Individuals must be informed about the consequences of their data being disseminated worldwide on the consent form so they can make an informed choice.

16. 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 school admissions paperwork.

An **example** of permission form is provided in **Appendix 5**

The consent will be recorded appropriately including date given and name of consent giver using the schools MIS system.
The school will message all parents at the beginning of each academic year to **review any consent** given and permission will be reviewed prior to any photographs being taken and/or posted on school social media pages/website/School handbook.

17. 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 comply with their **adopted CCTV policy** where applicable.

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.

18. Biometric Information (where applicable)

Biometric information means measurable, biological characteristics that can uniquely identify an individual such as fingerprints or facial recognition.
The **Protection of Freedoms Act 2012** includes measures relating to the use of biometric identification systems.

Under UKGDPR, it is recognised that this type of data is **special category data.**

The School will retrieve **written consent** from individuals **prior to processing** their biometric 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.

Alternative methods of service provision will be available in the event of an individual refusing to provide consent.
A consent form for biometric information is provided in **Appendix 6**

19. Staff Training

All employees will receive appropriate **Data Protection Training** which will include **annual refresher** courses.

The training will be relevant, accurate and kept up to date for all staff. It will focus on key areas of data protection such as handling requests, data sharing, information security, personal data breaches and records management.

The school will keep a **record of staff training** dates and attendance as well as a record of staff who have read, understood, and accepted this policy.

20. Access rights - new starters/change of role/leavers

The school must have controls in place to ensure the **confidentiality, integrity** and **availability** of the data they process in order to comply with the Data Protection policy and UKGDPR regulations.

The level of access granted for each user (staff/pupils/Governors) should be retained and reviewed as part of 'new starter/change of role/leaver' records allowing access to be correctly updated when required.

All **new starters** will receive data protection training as part of their induction package. Details of this should be added to the staff training record.

Anyone **leaving the school** should be advised to download their personal documents from their HwB and One Drive account.
Access rights, on all systems, for all leavers should be **revoked on their last day** at the school.

21. 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.

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.

22. 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 Schools Data Protection officer in the first instance and directed to the Information Commissioner if required. Contact details of all will be provided with the disclosure information.

23. 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

24. Useful Resources

A pack specifically for schools from the Information Commissioner's Office:
Schools, universities and colleges | ICO

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

Cais i dderbyn Gwybodaeth Bersonol– Cais Gwrthrych am Wybodaeth (SAR)

Defnyddir y ffurflen gais hon i ganiatáu i unigolion gael mynediad at wybodaeth a gedwir amdanynt

Rhan 1 – Y Cais

Amdanaf i fel unigolyn y mae'r wybodaeth ☐
Os mai ie yw'r ateb, ticiwch ac yna cwblhewch 3,4,5 a 6

Neu

Rwy'n gweithredu ar ran rhywun arall ☐
Os mai ie yw'r ateb, ticiwch ac yna cwblhewch 2,3,4,5 a 6

Rhan 2 – Gwybodaeth rhywun arall

Fi yw rhiant y plentyn Amgaeaf brawf o gyfrifoldeb rhiant

Mae'r plentyn dros 12 oed Amgaeaf ganiatâd i rannu gan y plentyn

NEU

Rwyf yn gwneud cais am yr wybodaeth ar

Amgaeaf llythyr caniatâd i rannu ar ran rhwyun arall.

Rhan 3 – 'Gwrthrych Data' (Yr unigolyn y mae'r wybodaeth yn ymwneud ag ef)

Teitl ..... Cyfenw……Enw Cyntaf……

Enw cyn priodi, blaenorol neu enwau eraill……

Dyddiad Geni……

Cyfeiriad Presennol…….

Rhif Ffôn……..

Email Address (optional)……

Dogfennau Adnabod – Dewiswch un o bob adran

Adran 1 – **prawf o gyfeiriad** Cyfriflen Banc ☐ Bil cyfleustodau ☐

Arall, nodwch os gwelwch yn dda…….

Section 2 – **prawf adnabod ffotograffig**

Pasbort ☐ Trwydded Yrru ☐

Arall, nodwch os gwelwch yn dda…….

Gall methu â darparu prawf adnabod a dogfennau sy'n ofynnol yn adran 2 achosi oedi gyda'ch cais

Section 4 – Manylion yr wybodaeth y gofynnir amdani

Helpwch ni i ddelio â'ch cais yn gyflym ac yn effeithlon trwy roi cymaint o fanylion â phosibl am yr wybodaeth rydych chi ei heisiau **YN CYNNWYS** yr Ysgol(ion) a fynychwyd a dyddiadau

Rhan 5 – Mynediad at yr wybodaeth

Gellir anfon gwybodaeth yn **Electroneg** neu drwy **Bost Cofnodedig**. Oso es gennych unrhyw anghenion arbennig wrth edrych ar wybodaeth, nodwch hynny yma;

Electroneg ☐

Post Cofnodedig ☐

Unrhyw anghenion arbennig wrth edrych ar wybodaeth;

Rhan 6 – Datganiad

Rwyf yn ardystio bod yr wybodaeth a roddwyd ar y ffurflen hon yn wir. Deallaf nad oes rheidrwydd ar Gyngor Gwynedd i gydymffurfio â'm cais oni bai eu bod yn derbyn yr wybodaeth y bydd ei hangen yn rhesymol arnynt er mwyn bodloni eu hunain ynghylch pwy ydw i ac i ddod o hyd i'r wybodaeth yr wyf yn ei cheisio

Enw (Prif Lythrennau) .....

Llofnod .....

Dyddiad.....

Cyn dychwelyd y ffurflen hon, gwiriwch:
Ydych chi wedi cwblhau POB adran?
Ydych chi wedi amgáu'r dogfennau adnabod?
Ydych chi wedi llofnodi a dyddio'r ffurflen?

Anfonwch y ffurflen hon at; Louise Jones, Swyddog Diogelu Data Ysgolion, Cyngor Gwynedd, Stryd y Jêl, Caernarfon, Gwynedd. LL55 1SH

SDDYsgolion@Gwynedd.llyw.cymru

Sut rydym yn defnyddio eich gwybodaeth Bydd y wybodaeth bersonol ar y ffurflen yn cael ei defnyddio i brosesu eich cais. Bydd yn cael ei brosesu o dan ddeddfwriaeth diogelu data. Ni fydd yn cael ei rannu y tu allan i'r Cyngor a bydd yn cael ei gadw am gyfnod o 3 blynedd. I gael rhagor o wybodaeth am eich hawliau a manylion am sut i gwyno, gweler Polisi Diogelu Data Ysgolion

Request for information– Personal Information (SAR)

This application form is used to allow individuals access to information held about them

Section 1 – The Request

I am the person the information is about ☐
If yes, please tick the box and complete parts 3,4,5 and 6

OR

I am acting on behalf of someone else ☐
If yes, please tick and complete parts 2,3,4,5,and 6

Section 2 – Someone else' Information

I am the child's parent ☐ I enclose proof of parental responsibility

The child is over the age of 12 ☐ I enclose consent to share from the child

OR

I am requesting the information on behalf of someone else ☐ I enclose a signed consent to share letter

Section 3 – 'Data Subject' (Person the information relates to)

Title ..... Surname ..... First Name……

Maiden, previous or other names……

Date of birth……

Current Address…….

Telephone Number……
Email Address (optional)……

Identification Documents - please select one from each section

Section 1 – **proof of address** Bank Statement ☐ Utility Bill ☐

Other please state .....

Section 2 – **photographic proof of identification** Passport ☐ Driving Licence ☐

Other please state……

Failure to provide proof of identity and documents required in section 2 may delay your application

Section 4 – Details of the information being requested

Please help us deal with your request quickly and efficiently by giving as much detail as possible about the information you want **INCLUDING** school(s) attended and dates

Section 5 – Access to the information

Information can be sent **Electronically** or by **Recorded Delivery.** If you have any special needs when viewing the information, please state here;

Electronically ☐

Recorded Delivery ☐

Any special needs when viewing the information;

Section 6 – Declaration

I certify the information provided on this form is true. I understand the School is not obliged to comply with my request unless they are supplied with such information as they may reasonably require in order to satisfy themselves as to my identity and to locate the information requested**.**

Name (Block Capitals) .....

Signature .....

Date.....

Before returning this form please check:
Have you completed ALL sections?
Have you enclosed the identification documents?
Have you signed and dated the form?

Please send this form to; Louise Jones, Schools Data Protection. Gwynedd Council, Shirehall Street, Caernarfon, Gwynedd. LL55 1SH

SchoolsDPO@Gwynedd.llyw.cymru

How we use your information
The personal information on the form will be used in order to process your request. It will be processed under data protection legislation. It will not be shared outside the Council and will be kept for a period of 3 years. For further information about your rights and details of how to complain, please see the Schools Data Protection Policy.

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. Nodwch fod dwy ran i'r ffurflen os gwelwch yn dda.

Rhan A i'w chwblhau a'i llofnodi gan y Pennaeth a'i throsglwyddo i'r Swyddog Diogelu Data Ysgolion

Rhan B i'w chwblhau gan y Swyddog Diogelu Data Ysgolion

Rhan A

Y Rheolwr Llinell sy'n ymchwilio ddylai gwblhau a llofnodi'r rhan hon a'i throsglwyddo i'r Swyddog Llywodraethu Gwybodaeth

Amdanoch chi	
• Enw	
• Cyfeiriad E-bost	
• Rhif Ffôn Cyswllt	
Manylion am yr achos	
• Enw a rôl aelod staff oedd yn gyfrifol am y digwyddiad?	
• Pa bryd y digwyddodd yr achos?	
• Pa bryd y darganfuwyd yr achos?	
• Rhowch grynodeb byr o'r achos os gwelwch yn dda	
• Nodwch y camau a gymerwyd unwaith daethoch i wybod am y digwyddiad	

• Amlinellwch y math o ddata personol oedd yn rhan o'r digwyddiad. Data personol, e.e. enw, rhif ffon, cyfeiriad ebost, dyddiad geni Data sensitif, e.e. iechyd, crefydd, ethnigrwydd	
• Yn eich barn chi, ydi data personol unrhyw unigolyn wedi ei beryglu o ganlyniad i'r achos? o Pa mor ddifrifol ydi'r risg i'r unigolion?	
• Nodwch pa fath o unigolion sydd wedi eu heffeithio E.e. staff, disgyblion, rhieni, ymwelwyr • Tua faint o bobl sydd wedi eu heffeithio?	
• Ydi'r unigolion hyn wedi cael gwybod am yr achos? o Os ydynt sut, pa bryd a gan bwy? o Os nad ydynt, esboniwch pam os gwelwch yn dda.	
• A gymerwyd unrhyw gamau i ostwng/lleddfu'r effaith ar y bobl a effeithir? o 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? Os yw'n berthnasol, pa bryd ydych yn bwriadu cyflwyno'r newidiadau angenrheidiol i'ch arferion gwaith?	
• Ydych chi wedi gofyn am gyngor y Tim Rheoli Gwybodaeth mewn perthynas â'r achos?	

Anghenion Hyfforddi a Datblygu	
• Ydych chi'n ystyried fod unrhyw ffactorau rheolaethol wedi cyfrannu at y digwyddiad data (E.e. pwysau gwaith, newydd i'r rôl a.y.b)	
• Oedd yr aelod o staff wedi derbyn hyfforddiant diogelu data? Hyfforddiant Rhithiol neu Mewn person	
• Ydych chi wedi cael sgwrs efo'r aelod staff am y digwyddiad? Ydych chi wedi adnabod unrhyw anghenion datblygu yn deillio o'r sgwrs?	
• Ydych chi'n ystyried bod angen cymryd camau disgyblu? Ydy hyn wedi digwydd o'r blaen?	
A fyddech cystal â llofnodi a dyddio'r rhan hon. Llofnod:	Dyddiad:

Rhan B

I'w gwblhau gan y SDDY
Penderfyniad i hysbysu'r ICO ac unigolion

Dyddiad ac amser daeth y SDDY i wybod am y digwyddiad	

Yn ol y GDPR rhaid i'r sefydliad hysbysu digwyddiad heb oedi a lle bod modd dim hwyrach na 72 awr ar ol dod yn ymwybodol.

- ICO Decision tree –

Ydi'r digwyddiad yn debygol o arwain at risg i ryddid a hawliau unigolion?			
Ydi	☐	**Nac ydi**	☐
Ydi'r digwyddiad yn debygol o arwain at risg uchel i ryddid a hawliau unigolion?			
Ydi:	☐	**Nac ydi:**	☐
Adrodd digwyddiad i'r ICO			
Pam fod angen i'r Ysgol adrodd neu beidio ag adrodd y digwyddiad?			
Adrodd ar y digwyddiad i unigolion:			
Pam fod yr Ysgol angen hysbysu/peidio a hysbysu unigolion?			

Enw'r Swyddog Diogelu Data		**Dyddiad**			

Audit Form for cases of Breach of Data Security Rules

This form must be completed whenever the security of personal data has been compromised, so that the School has evidence of the steps it has taken to put things right. The steps taken by the School may include referring itself to the Information Commissioner. As such, it is important to complete this form correctly so that all the facts and circumstances of the case can be addressed and positive steps can be taken to mitigate and reduce risks for individuals and the School.

Please note that there are **two parts** to the form.

Part A to be completed and signed by the Headteacher and passed on to the Schools Data Protection Officer.
Part B to be completed by the Schools Data Protection Officer

A
This part should be completed and signed by the Headteacher
and passed to the Schools Data Protection officer.

About You	
• Name	
• E-mail	
• Telephone Number	
Details of the incident	
• Name and role of staff member responsible for the incident?	
• When did the incident happen?	
• When the case was discovered?	
• Please provide a brief summary of the case	
• What steps were taken once you became aware of the incident	
• Outline the type of personal data that was involved in the incident. Personal data, e.g. name, phone number, email address, date of birth	

Sensitive data, e.g. health, religion, ethnicity	
• In your opinion, has the personal data of any individual been compromised as a result of the case? • How serious is the risk to the individuals?	
• • Identify what type of individuals have been affected E.G. staff, pupils, parents, visitors • Approximately how many people have been affected?	
• • Have these individuals been informed about the incident? If **Yes,** when, how and by who? If **No**, please explain why	
• Have any steps been taken to reduce/alleviate the impact on the people affected? o Please provide details;	
• In your opinion, what steps could be introduced to ensure that the same thing would not happen again? If applicable, when do you intend to introduce the necessary changes to your working practices?	
• Have you sought the advice of the Schools Data Protection Officer in relation to the case?	
Training and Development Needs	
• Do you consider that any managerial factors have contributed to the data event (E.g. workload, new to the role etc.)	

• Had the member of staff received data protection training? Virtual or In person Training	
• Have you had a conversation with the member of staff about the incident? Have you identified any development needs arising from the conversation?	
• Do you consider it necessary to take disciplinary action? Has this happened before?	
Please sign and date this section Signed:	Date:

Part B

To be Completed by the SDPO
Decision to notify the ICO and individuals

Date and time the SDPO became aware of the incident	

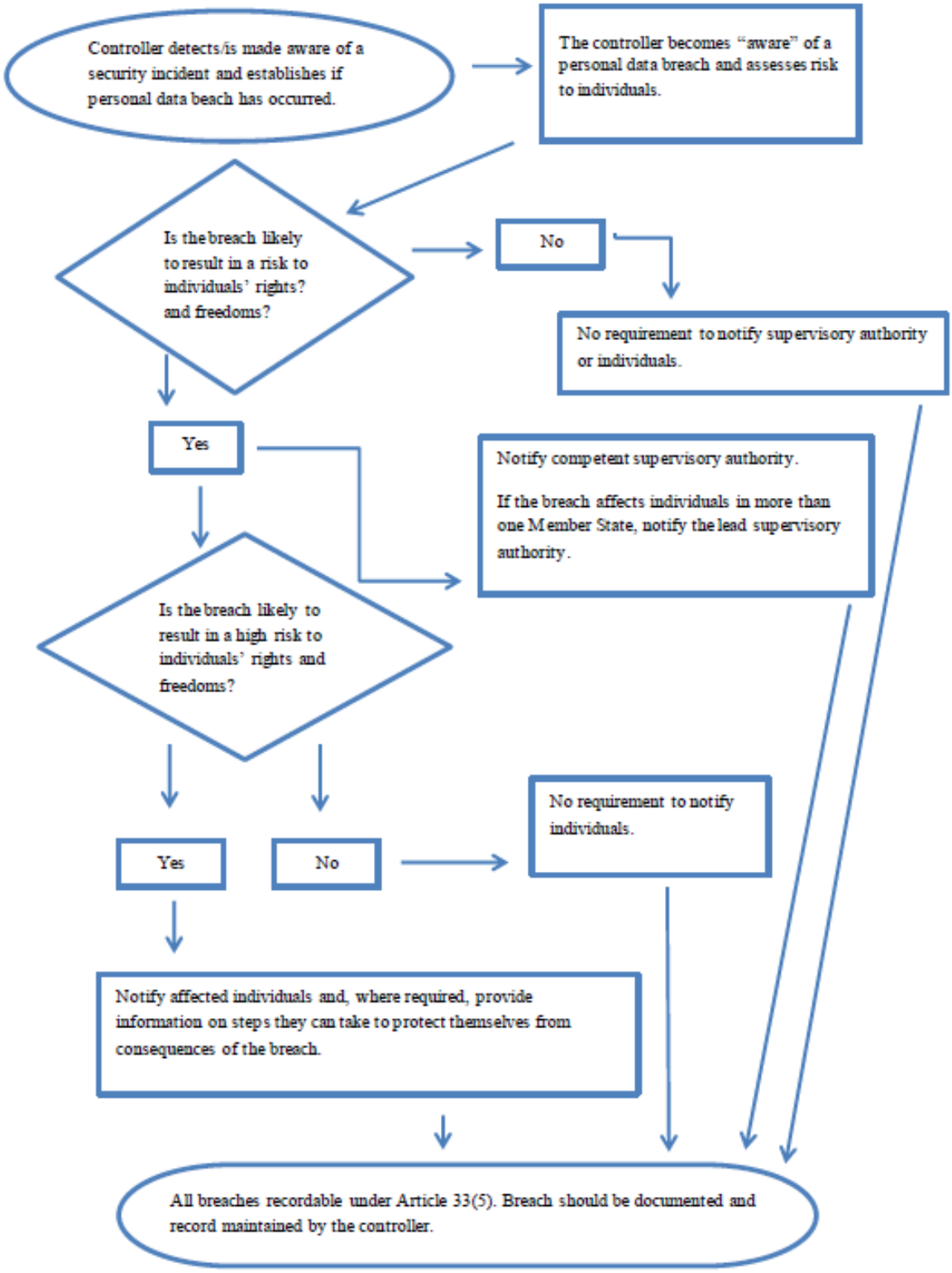
According to the GDPR the organization must notify an incident without delay and where possible no later than 72 hours after becoming aware.

ICO Decision tree –

Is the incident likely to lead to a risk to the freedom and rights of individuals?			
Yes	☐	**No**	☐
Is the incident likely to lead to a substantial risk to the freedom and rights of individuals?			
Yes	☐	**No**	☐
Report an incident to the ICO			
Why does the School need to report or not report the incident?			

Reporting the incident to individuals:					
Why does the School need to notify/not notify individuals?					
School DPO Name		**Date**			

A. Flowchart showing notification requirements



Appendix 4

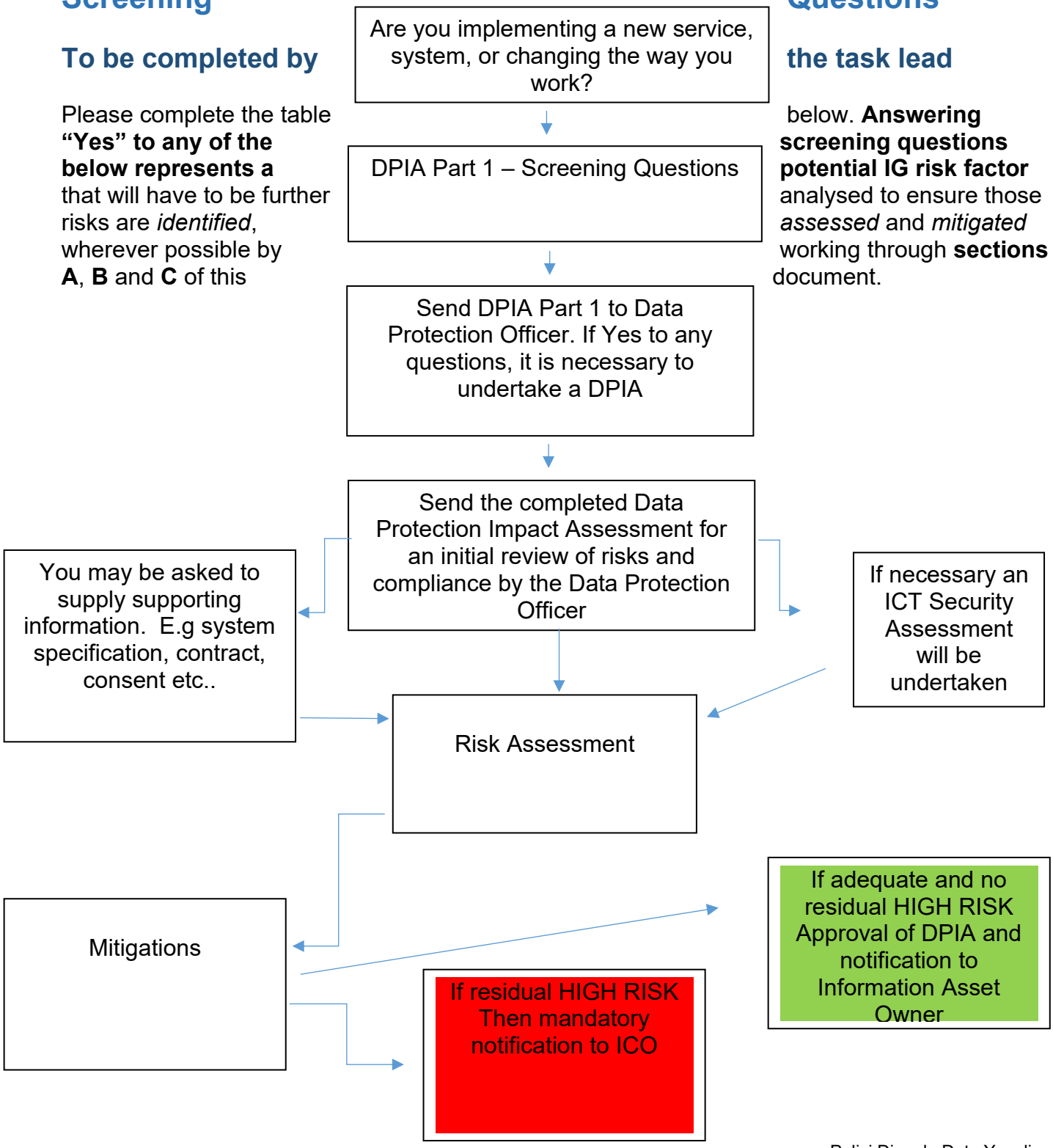
Data Protection Impact Assessment []

DPIA Process

Screening Questions

To be completed by the task lead

Please complete the table below. **Answering "Yes" to any of the screening questions potential IG risk factor** below **represents a** 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?	
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?	

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	Minimal risk
4 - 6	Moderate risk
8 - 12	High risk
15 - 25	Extreme risk

Appendix 5

Defnyddio Delweddau/Fideo
Use of 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:

tu fewn i'r ysgol, cylchlythyrrau / within the school, newsletters ☐

gwefan yr ysgol / the school website ☐

Facebook/Twitter/Instagram ☐

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……

Appendix 6

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.

Signature

Date