Ysgol Cybi

Polisi Asesiad Effaith Diogelu Data Ysgolion (DPIA) / *Schools Data Protection Impact Assessment (DPIA) Policy*

(Fersiwn 1, Ebrill 2022 / *Version 1, April 2022)*

Ynglŷn â'r polisi hwn

Mae DPIA yn ddull strwythuredig o nodi'r risgiau preifatrwydd sy'n gysylltiedig â phrosesu data personol ac ar gyfer gweithredu rheolaethau priodol i reoli'r risgiau hynny.

Mae'r polisi hwn yn gosod y fframwaith ar gyfer asesiad ffurfiol i sicrhau bod prosesau a systemau newydd a gyflwynir yn bodloni rhwymedigaethau cyfreithiol o ran cyfrinachedd, diogelu data a diogelwch.

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

About this policy

A DPIA is a structured approach to identifying the privacy risks associated with the processing of personal data and for implementing appropriate controls to manage those risks.

This policy lays the framework for a formal assessment to ensure that new processes and systems introduced meet legal obligations regarding confidentiality, data protection and security.

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

Fersiwn / *Version*	**Dyddiad / *Date***	**Crynodeb o newidiadau / *Summary of changes***	**Dyddiad a Dderbyniwyd gan Fwrdd o Lywodraethwyr / *Date Accepted by Board of Governors***
F1 / *V1*	Ebrill 2022 / *April 2022*	Polisi newydd / *New policy.*	

Dyddiad yr adolygiad nesaf / *Date of next review*	
Bydd y polisi hwn yn cael ei adolygu yn: / *This policy will be reviewed in:*	Ebrill 2025 / *April 2025*
Yr unigolyn a fydd yn ymgymryd â'r adolygiad fydd: / *The review will be undertaken by:*	Swyddog Diogelu Data Ysgolion / *Schools Data Protection Officer*

Manylion Cyswllt:

Swyddog Diogelu Data Ysgolion

E-bost:
dpoysgolionmon@ynysmon.gov.uk

Rhif ffôn: 01248 751833

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

Contact Details:

Schools Data Protection Officer

E-mail:
dpoysgolionmon@ynysmon.gov.uk

Telephone: 01248 751833

Address:
Learning Service
Isle of Anglesey County Council
Council Offices
Llangefni
Anglesey
LL77 7TW

Rydym yn hapus i ddarparu'r polisi hwn ar ffurfiau eraill ar gais. Defnyddiwch y manylion cyswllt uchod. / *We are happy to provide this policy in alternative formats on request. Please use the above contact details.*

Dogfen: Templed polisi ar y fframwaith ar gyfer asesiad ffurfiol i sicrhau bod prosesau a systemau newydd a gyflwynir yn bodloni rhwymedigaethau cyfreithiol o ran cyfrinachedd, diogelu data a diogelwch.

Document: *Policy template on the framework for a formal assessment to ensure that new processes and systems introduced meet legal obligations regarding confidentiality, data protection and security.*

Cyfrifoldeb: *Cyfrifoldeb llywodraethwyr yr ysgol a'r Pennaeth fel y Rheolydd Data yw sicrhau bod gweithdrefnau ar waith i sicrhau bod yr ysgol yn cydymffurfio â deddfwriaeth diogelu data. Cyfrifoldeb y Pennaeth yw sicrhau bod holl staff yr ysgol yn gweithredu ac yn cydymffurfio.*

Responsibility: *It is the responsibility of the school governors and Headteacher as the Data Controller to ensure procedures are in place to ensure that the school complies with data protection legislation. It is the responsibility of the Headteacher to ensure implementation and compliance by all school staff.*

Cynnwys **Tudalen**

1. Datganiad Polisi

Mae'r ysgol wedi ymrwymo'n llwyr i ddiogelu data personol yn unol â gofynion *Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR)* a *Deddf Diogelu Data 2018*.

Mae'r *UK GDPR* yn cynnwys rhwymedigaeth i gynnal Asesiad Effaith Diogelu Data (DPIA) ar gyfer mathau o brosesu sy'n debygol o arwain at *risg uchel* i fuddiannau unigolion.

Mae'r polisi hwn yn gosod y fframwaith ar gyfer asesiad ffurfiol i sicrhau bod prosesau a systemau newydd a gyflwynir yn bodloni rhwymedigaethau cyfreithiol o ran cyfrinachedd, diogelu data a diogelwch.

Bydd yr ysgol yn cwblhau DPIAs, lle y bo'n briodol, i ddangos atebolrwydd a chydymffurfiaeth â'r *UK GDPR.*

2. Sgôp

Mae'r polisi hwn yn berthnasol i bob aelod o staff yr ysgol, gan gynnwys gweithwyr dros dro, contractwyr, gwirfoddolwyr, llywodraethwyr a sefydliadau partner sy'n cyflwyno prosesau neu systemau newydd sy'n debygol o gynnwys defnydd newydd neu newid yn sylweddol i'r ffordd y caiff data personol ei drin a'i brosesu.

Mae'r polisi hwn hefyd yn berthnasol pan fo digwyddiad sylweddol wedi digwydd mewn perthynas â phroses/system gyfredol neu lle mae prosesau presennol yn cael eu diwygio, megis ymgymryd â phrosesu cyfredol mewn gwahanol ffyrdd.

Mae'r ysgol wedi ymrwymo i sicrhau bod proses DPIA ar waith a bod yr holl brosiectau, prosesau a systemau newydd (gan gynnwys meddalwedd a chaledwedd) sy'n cael eu cyflwyno, yn bodloni rhwymedigaethau cyfreithiol a statudol o ran preifatrwydd, cyfrinachedd, diogelu data a diogelwch.

Mae'r polisi hwn yn berthnasol i bob math o ddata personol a gedwir gan yr ysgol.

Mae'r gyfraith yn mynnu bod yr ysgol yn ymgynghori â'r Swyddog Diogelu Data Ysgolion fel rhan o'r broses DPIA, ac er mwyn helpu i benderfynu a oes angen DPIA ai peidio.

3. Deddfwriaeth, Canllawiau a Pholisïau

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

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

Dylid darllen y polisi hwn hefyd ar y cyd â'r *Polisi Diogelu Data Ysgolion; Polisi Diogelwch Gwybodaeth Ysgolion; Polisi Prosesu Data Ysgolion* ac *Cyfnodau Cadw Ysgolion.*

4. Diffiniadau

Data personol	Unrhyw wybodaeth ynglŷn ag unigolyn naturiol yr adnabyddir neu y gellir ei adnabod yn uniongyrchol neu'n anuniongyrchol drwy'r wybodaeth honno. Gellir ei storio'n ddigidol, ar gyfrifiadur, neu mewn systemau ffeilio ar bapur.
Data categori arbennig	Gwybodaeth ynglŷn â hil, tarddiad ethnig, barn wleidyddol, credoau crefyddol neu athronyddol, aelodaeth undeb llafur (neu ddiffyg aelodaeth), gwybodaeth enetig, gwybodaeth fiometreg (i adnabod unigolyn) unigolyn, a gwybodaeth ynglŷn ag iechyd, bywyd rhywiol neu ogwydd rhywiol unigolyn. Data categori arbennig yw data personol sydd angen amddiffyniad bellach oherwydd ei fod yn sensitif.
Defnyddwyr data	Yn cynnwys gweithwyr sydd â'u gwaith yn ymwneud â data personol. Mae gan ddefnyddwyr data ddyletswydd i ddiogelu'r wybodaeth y maent yn ymdrin â hi drwy ddilyn polisïau diogelu data a diogelwch bob amser. Mae staff a gyflogir gan ysgolion yn ddefnyddwyr data.
Proseswyr data	Yn cynnwys unrhyw berson sy'n prosesu data personol ar ran rheolydd data (heblaw am y sawl sy'n gyflogedig gan y rheolydd data). Gall proseswyr data gynnwys cyflenwyr sy'n ymdrin â data personol ar ran yr ysgol.
Gwrthrych y data	Yr unigolyn y mae'r wybodaeth bersonol yn ymwneud ag ef.
Prosesu gwybodaeth	Casglu, meddiannu, cofnodi, trefnu, strwythuro, storio, dargadw, diwygio, addasu, altro, adennill, ymgynghori, lledaenu, cyfyngu, datgelu, dinistrio, dileu gwybodaeth neu ei defnyddio neu wneud unrhyw beth â hi.
Risg	Effaith ansicrwydd ar amcanion. Risgiau i unigolion: y potensial am ddifrod neu drallod. Nodweddir risg yn aml gan gyfeirio at "ddigwyddiadau" a "chanlyniadau" posibl, neu gyfuniad o'r rhain.
Asesiad Risg	Adnabod a dadansoddi risgiau i amcanion busnes y sefydliad.
Tebygolrwydd	Pa mor debygol yw hi y bydd y risg yn digwydd - ansicrwydd, cyfle a thebygolrwydd.
Effaith	Beth yw canlyniadau'r risg pe bai'n digwydd. Ystyrir bod effaith naill ai'n cael effaith uniongyrchol neu effaith yn y dyfodol.
Rheoli	Mesur sy'n addasu risg.
Data genetig	Data personol sy'n ymwneud â nodweddion genetig a etifeddwyd neu a gaffaelwyd gan berson naturiol sy'n rhoi gwybodaeth unigryw am ffisioleg neu iechyd y person naturiol hwnnw ac sy'n deillio, yn benodol, o ddadansoddiad o sampl biolegol gan y person naturiol dan sylw.
Data biometrig	Data personol sy'n deillio o brosesu technegol penodol sy'n ymwneud â nodweddion corfforol, ffisiolegol neu ymddygiadol person naturiol, sy'n caniatáu neu'n cadarnhau adnabyddiaeth unigryw'r person naturiol hwnnw, megis delweddau wyneb neu ddata dactyloscopig. Mae adnabod olion bysedd yn enghraifft o ddata dactyloscopig.

Storio cwmwl	Mae storio cwmwl yn fodel cyfrifiadura cwmwl lle caiff data ei storio ar weinyddion o bell a gyrchir o'r rhyngrwyd, neu "gwmwl". Mae'n cael ei gynnal, ei weithredu a'i reoli gan ddarparwr gwasanaeth storio cwmwl ar weinyddion storio sy'n cael eu hadeiladu ar dechnegau rhithiol.
Swyddfa'r Comisiynydd Gwybodaeth (ICO)	Yr ICO yw corff annibynnol y DU (awdurdod goruchwylio) a sefydlwyd i gynnal hawliau gwybodaeth. Rôl yr ICO yw cynnal hawliau gwybodaeth er budd y cyhoedd. Mae hyn yn cynnwys ymdrin â chwynion ynghylch problemau, cael gafael ar wybodaeth bersonol gan sefydliad, neu os oes pryderon ynghylch sut mae sefydliad wedi ymdrin â gwybodaeth - os yw'r wybodaeth yn anghywir, wedi'i cholli neu ei datgelu i rywun arall. Adroddir am ddigwyddiadau diogelwch data sy'n risg uchel i unigolion i'r ICO.

5. Cyfrifoldebau

5.1. Corff Llywodraethu'r Ysgol

Corff llywodraethu'r ysgol sy'n gyfrifol am:

- sicrhau bod y polisi hwn wedi'i fabwysiadu'n ffurfiol gan yr ysgol;
- monitro cydymffurfiaeth ac atebolrwydd cyffredinol yr ysgol mewn perthynas â'r polisi hwn;
- sicrhau y gall yr ysgol ddangos tystiolaeth o gydymffurfiad â deddfwriaeth diogelu data.

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

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

- sicrhau bod staff yr ysgol yn ymwybodol o'r broses DPIA ac yn cydymffurfio'n llawn â'r polisi;
- cysylltu â'r Swyddog Diogelu Data Ysgolion wrth weithredu neu newid proses neu system, er mwyn penderfynu a oes angen DPIA ai peidio;
- adnabod rhanddeiliaid allweddol y mae angen ymgynghori â hwy fel rhan o'r broses DPIA;
- sicrhau bod y broses DPIA yn cael ei hailystyried pe bai newid sylweddol i'r broses neu risg preifatrwydd sylweddol yn cael ei chodi;
- integreiddio canlyniadau'r DPIA i gynlluniau prosiect;
- cadw cofnod o holl DPIAs yr ysgol fel rhan o'r *Cofnod o Weithgareddau Prosesu (ROPA*);
- monitro perfformiad parhaus y DPIA;
- cadw cofnod o'r risgiau o fewn Cofrestr Risg;
- cyhoeddi DPIAs os yw'n briodol;
- sicrhau bod y DPIA yn cael ei storio'n ddiogel.

5.3. Holl Staff yr Ysgol

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

- gydymffurfio â'r polisi hwn i sicrhau bod prosesu yn parhau i gydymffurfio â'r ddeddfwriaeth gyfredol os yw'n gweithredu neu'n newid proses neu system;
- gallu adnabod pryd y gallai fod angen DPIA a hysbysu'r Pennaeth;
- ymgymryd ag unrhyw hyfforddiant a ddarperir ynghylch DPIAs os yw hyn yn berthnasol i rôl y swydd.

5.4. Swyddog Diogelu Data Ysgolion

Mae'r Swyddog Diogelu Data Ysgolion yn gyfrifol am:

- gynorthwyo'r Pennaeth i benderfynu a oes angen DPIA ai peidio wrth weithredu neu newid proses neu system;
- cynorthwyo'r Pennaeth i gwblhau *Rhestr Wirio Sgrinio DPIA*;
- cefnogi'r ysgol i gwblhau DPIA;
- rhoi cyngor ar ba fesurau a mesurau diogelu y gall yr ysgol eu cymryd i liniaru risgiau;
- cadarnhau bod y DPIA wedi'i gwblhau'n gywir;
- hwyluso'r broses o ymgynghori â Swyddfa'r Comisiynydd Gwybodaeth (ICO) lle mae risg weddilliol uchel;
- rhoi cyngor ar ganlyniad y DPIA ac a all y prosesu fynd yn ei flaen;
- rhoi cyngor i'r Pennaeth ynghylch cyhoeddi DPIAs;
- darparu cyngor ac arweiniad mewn perthynas ag adolygu DPIAs;
- darparu cyngor ac arweiniad sy'n ymwneud â mentrau neu systemau etifeddol;
- cadw cofnod o DPIAs ar ran pob ysgol;
- monitro perfformiad parhaus y DPIA, gan gynnwys pa mor dda y mae'r ysgol wedi gweithredu camau gweithredu wedi'u cynllunio i fynd i'r afael â'r risgiau;
- sicrhau bod yr holl gytundebau prosesu data yn cynnwys y gofyniad i broseswyr data gynorthwyo'r ysgol i ddogfennu gweithgareddau prosesu ac i nodi unrhyw risgiau cysylltiedig;
- sicrhau y bydd y DPIA yn cysylltu ac yn cydymffurfio â phob un o'r Egwyddorion Diogelu Data;
- darparu hyfforddiant ar sut i gwblhau DPIAs i staff yr ysgol a fydd yn rhan o gwblhau DPIAs.

6. Beth yw Asesiad Effaith Diogelu Data (DPIA)?

Mae DPIA yn ddull strwythuredig o nodi risgiau diogelu data sy'n gysylltiedig â phrosesu data personol; helpu'r ysgol i nodi a lleihau'r risgiau ac ar gyfer gweithredu rheolaethau priodol i'w rheoli. **Mae DPIA yn ofyniad cyfreithiol ar gyfer prosesu sy'n debygol o fod yn *risg uchel*.**

Mae'r DPIA yn offeryn gwerthuso sydd wedi'i gynllunio i ddadansoddi, adnabod, lleihau a mynd i'r afael â risgiau diogelu data, preifatrwydd a diogelwch prosesu yn systematig ac yn gynhwysfawr. Mae DPIA yn asesu tebygolrwydd ac effaith cyfaddawd i gyfrinachedd, uniondeb a/neu argaeledd data personol.

Gall DPIA gwmpasu un gweithrediad prosesu neu grŵp o weithrediadau prosesu tebyg. Gall grŵp o reolwyr wneud DPIA ar y cyd.

Dylai DPIAs ystyried risgiau cydymffurfio, ond hefyd risgiau ehangach i hawliau a rhyddid unigolion, gan gynnwys y potensial ar gyfer unrhyw anfantais gymdeithasol neu economaidd sylweddol. Mae'r ffocws ar y *potensial* ar gyfer niwed – i unigolion neu i gymdeithas yn gyffredinol, boed yn gorfforol, yn faterol neu'n ansylweddol.

Bydd yr ysgol yn gwneud asesiad gwrthrychol o'r risgiau a bydd yn defnyddio *Matrics Risg Diogelu Data Ysgolion* (ATODIAD A) i feddwl am debygolrwydd a difrifoldeb y risgiau. Mae'r *Matrics Risg Diogelu Data Ysgolion* hefyd ar gael ar y dudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

Dylid datblygu a gweithredu pob prosiect, rhaglen, proses, system wybodaeth newydd (gan gynnwys meddalwedd a chaledwedd) ac asedau gwybodaeth perthnasol eraill mewn modd diogel a strwythuredig a chydymffurfio â gofynion cyfreithiol a statudol. Rhaid iddynt gydymffurfio â gofynion cyfrinachedd, preifatrwydd a diogelu data. Rhaid profi pob proses neu system newydd yn erbyn y gofynion hyn cyn iddynt gael eu cyflwyno.

Er mwyn penderfynu a yw unrhyw newidiadau arfaethedig i brosesau'r ysgol ac asedau gwybodaeth yn effeithio ar gyfrinachedd, uniondeb a hygyrchedd data personol a/neu sensitif, bydd yr ysgol yn defnyddio'r DPIA i brofi yn erbyn y gofynion hyn.

Bydd DPIAs yn cael eu cynnwys ym mhrosesau a fframwaith rheoli risg yr ysgol. Mae gofynion y DPIA wedi'u cynnwys ym mhob polisi, proses a gweithdrefn berthnasol.

Bydd yr ysgol yn sicrhau bod y canlyniad yn gallu dylanwadu ar gynlluniau'r ysgol. Mae DPIA yn cael ei gychwyn a'i gynnal drwy gydol y gwaith o ddatblygu a gweithredu prosiect, proses neu system.

7. Diben Asesiadau Effaith Diogelu Data

Diben y DPIA yw tynnu sylw at unrhyw risgiau preifatrwydd sy'n gysylltiedig â phrosiect neu broses a sicrhau bod y defnydd arfaethedig o ddata personol yn cael ei ddeall yn llawn.

Mae'r DPIA yn adrodd ac yn casglu manylion yr effeithiau posibl a adnabuwyd a'r atebion neu'r camau gweithredu a fydd yn lleihau'r effaith neu'n lliniaru'r risg. Mae'r *UK GDPR* yn ei gwneud yn ofynnol i lefel o asesiad gael ei chwblhau sy'n gymesur â'r risgiau sy'n gysylltiedig â'r prosesu.

Mae DPIAs wedi'u mandadu'n benodol gan *UK GDPR* i asesu'r risgiau i hawliau preifatrwydd a diogelu data gwrthrychau data sy'n deillio o weithgareddau prosesu'r ysgol.

Mae DPIAs yn ofyniad cyfreithiol ar gyfer prosesu sy'n debygol o fod yn risg uchel. Gall DPIA effeithiol hefyd ddod â chydymffurfiaeth ehangach; buddion ariannol ac enw da; helpu i ddangos atebolrwydd ac adeiladu ymddiriedaeth ac ymgysylltiad ag unigolion.

8. Elfennau Allweddol Proses Asesiad Effaith Diogelu Data

Dylai DPIA ddechrau'n gynnar ym mywyd prosiect, proses neu system, ***cyn*** i'r prosesu ddechrau, a rhedeg ochr yn ochr â'r broses gynllunio a datblygu.

Dylai DPIA gynnwys y camau hyn:

Cam 1: nodi'r angen am DPIA;
Cam 2: disgrifio'r prosesu;
Cam 3: ystyried ymgynghori;
Cam 4: asesu angenrheidrwydd a chymesuredd;
Cam 5: nodi ac asesu risgiau;
Cam 6: nodi mesurau i liniaru'r risgiau;
Cam 7: cymeradwyo a chofnodi canlyniadau.

Bydd yr ysgol yn graddio'r amser a'r adnoddau sydd eu hangen ar gyfer DPIA i gyd-fynd â natur y broses.

9. Manteision Allweddol Asesiadau Effaith Diogelu Data

Mae manteision allweddol DPIAs yn cynnwys:

- cyflawni rhwymedigaethau statudol yr ysgol;
- cyfrannu at reoli risg yn effeithiol a chynyddu ymwybyddiaeth o breifatrwydd a diogelu data ar draws yr ysgol;
- rhoi hyder i unigolion bod yr ysgol yn cymryd camau i ddiogelu eu preifatrwydd, a gwell dealltwriaeth o'r ffyrdd y mae eu data personol yn cael ei ddefnyddio;
- gwella perthynas yr ysgol ag unigolion a gwella dealltwriaeth yr ysgol o anghenion, pryderon a disgwyliadau unigolion;
- dangos bod yr ysgol yn cymryd camau sy'n llai tebygol o fod yn ymwthiol o ran preifatrwydd ac sy'n cael effaith negyddol ar unigolion;
- sicrhau bod mentrau'n debygol o fod yn llwyddiannus oherwydd bod risgiau preifatrwydd yn cael eu nodi'n gynnar, gan ganiatáu i reolaethau gael eu cynllunio am lai o gost a llai o effaith ar gyflawni.

10. Adnabod yr angen am Asesiad Effaith Diogelu Data

Er mwyn penderfynu a oes angen DPIA, rhaid i'r ysgol nodi a yw data personol yn cael ei brosesu. Mae rhai enghreifftiau o wybodaeth o'r fath yn cynnwys:

- gwybodaeth sy'n gysylltiedig neu y gellir ei chysylltu ag unigolyn;
- dyddiad geni, man geni, hil, crefydd, pwysau, dangosyddion daearyddol; gwybodaeth cyflogaeth, meddygol, addysg ac ariannol;
- enw (e.e. enw llawn, enw cyn priodi, enw'r fam cyn priodi, neu enw arall);
- gwybodaeth am gyfeiriadau (e.e. cyfeiriad stryd neu e-bost);
- gwybodaeth sy'n adnabod eiddo sy'n eiddo personol (e.e. rhif cofrestru cerbydau);
- rhifau ffôn, rhifau ffôn symudol a rhifau personol;

- nodweddion personol, gan gynnwys lluniau (nodweddion wyneb neu nodweddion nodedig), olion bysedd, data biometrig (sgan retina, ac ati);
- rhif adnabod personol (e.e. Rhif Yswiriant Gwladol, rhif pasbort, trwydded gyrrwr, cyfrif ariannol neu rif credyd).

11. Pa bryd y dylid ymgymryd ag Asesiadau Effaith Diogelu Data

Mae'n orfodol ymgymryd â DPIA cyn dechrau unrhyw brosesu sy'n cynnwys data personol sy'n *debygol o arwain at risg uchel.* Mae hyn yn sicrhau bod risgiau preifatrwydd yn cael eu nodi a'u hystyried cyn iddynt gael eu rhoi ar waith yn y dyluniad a'u hadolygu'n rheolaidd drwy gydol y cylch bywyd.

Defnyddir *Rhestr Wirio Sgrinio DPIA* fel cam rhagarweiniol i gynorthwyo'r ysgol i benderfynu pryd y mae angen DPIAs.

Nid yw'r gofyniad am DPIAs wedi'i gyfyngu i brosiectau ffurfiol. Gall risg i breifatrwydd unigolion godi mewn llawer o senarios neu fentrau.

Efallai y bydd angen DPIAs i wneud cynigion i ymgymryd â phrosesu data personol newydd neu lle caiff prosesau presennol eu diwygio, megis ymgymryd â phrosesu cyfredol mewn gwahanol ffyrdd.

Rhaid i bob proses neu brosiect newydd neu wedi'u newid yn sylweddol sy'n cynnwys data personol y bwriedir eu cyflwyno gydymffurfio â deddfwriaeth a gofynion cyfrinachedd, preifatrwydd a diogelu data.

Bydd DPIA yn cael ei gynnal yng nghamau cynnar menter. Mae'r gyfraith yn ei gwneud yn ofynnol i'r ysgol ymgymryd â DPIA os yw'n bwriadu:

- defnyddio proffilio systematig a helaeth gydag effeithiau sylweddol;
- prosesu data categori arbennig neu drosedd (data sensitif) ar raddfa fawr; neu
- monitro lleoedd sy'n hygyrch i'r cyhoedd yn systematig ar raddfa fawr.

Mae'r ICO hefyd yn ei gwneud yn ofynnol i'r ysgol ymgymryd â DPIA os yw'n bwriadu:

- defnyddio technolegau newydd, arloesol;
- defnyddio proffilio neu ddata categori arbennig i benderfynu ar fynediad at wasanaethau;
- proffilio unigolion ar raddfa fawr;
- prosesu data biometrig (e.e. cydnabyddiaeth wyneb a ddefnyddir i ganiatáu mynediad i systemau);
- prosesu data genetig;
- paru data neu gyfuno setiau data o wahanol ffynonellau;
- casglu data personol o ffynhonnell heblaw'r unigolyn heb ddarparu:
    - hysbysiad preifatrwydd iddynt ('prosesu anweledig');
    - olrhain lleoliad neu ymddygiad unigolion;

- proffilio plant neu dargedu gwasanaethau marchnata neu ar-lein atynt; neu
- brosesu data a allai beryglu iechyd neu ddiogelwch corfforol yr unigolyn pe bai diogelwch yn cael ei dorri.

Mae enghreifftiau o senarios neu fentrau a allai fod angen DPIA yn cynnwys:

- cynnig i adeiladu system TG newydd ar gyfer storio neu gyrchu data personol;
- gweithredu technoleg gwyliadwriaeth mewn adeilad, megis system CCTV;
- defnyddio gwasanaeth cwmwl ar gyfer storio data;
- datblygu polisïau neu strategaethau sydd â goblygiadau preifatrwydd.

Bydd angen i'r Pennaeth ystyried a oes angen DPIA ar unrhyw brosesu a bydd yn ymgynghori â'r Swyddog Diogelu Data Ysgolion.

Ymhlith y ffactorau i'w hystyried mae pryd bynnag y bydd y prosesu:

- yn cynnwys casglu gwybodaeth newydd am unigolion;
- yn defnyddio gwybodaeth am unigolion at ddiben nad yw'n cael ei ddefnyddio ar ei gyfer ar hyn o bryd, neu mewn ffordd nad yw'n cael ei defnyddio ar hyn o bryd;
- yn golygu defnyddio technoleg newydd y gellid ystyried ei bod yn ymyrraeth preifatrwydd;
- arwain at wneud penderfyniadau, neu gymryd camau yn erbyn unigolion mewn ffyrdd a all gael effaith sylweddol arnynt;
- yn cynnwys gwybodaeth am unigolion o fath sy'n arbennig o debygol o godi pryderon neu ddisgwyliadau preifatrwydd fel unigolion sy'n agored i niwed.

Ystyrir bod plant yn agored i niwed o brosesu eu data personol gan y gallent fod yn llai abl i ddeall sut mae eu data'n cael ei ddefnyddio, rhagweld sut y gallai hyn effeithio arnynt, a diogelu eu hunain rhag unrhyw ganlyniadau diangen.

Os oes ansicrwydd ynghylch a yw'n briodol cynnal DPIA ar gyfer prosiect, proses neu system benodol, dylai'r Pennaeth ymgynghori â'r Swyddog Diogelu Data Ysgolion i gael eglurhad a chyngor.

12. Pwy ddylai ymgymryd ag Asesiad Effaith Diogelu Data

Yr ysgol fel y rheolydd data sy'n gyfrifol yn y pen draw ac yn atebol am gydymffurfio â deddfwriaeth diogelu data. Mae'r Pennaeth yn gyfrifol am sicrhau bod DPIAs yn cael eu cynnal. Mae'n bwysig bod staff yn gallu nodi pryd y gallai fod angen DPIA a hysbysu'r Pennaeth.

Bydd y Pennaeth yn ymgynghori â'r Swyddog Diogelu Data Ysgolion fel rhan o'r broses DPIA, ac er mwyn helpu i benderfynu a oes angen DPIA ai peidio. Rhaid i'r Swyddog Diogelu Data Ysgolion roi cyngor a mewnbwn.

Dylai perchennog y broses gynnal DPIA a'i gynorthwyo gan y rhai sy'n ymwneud â'r broses fusnes sydd â'r wybodaeth gywir a dealltwriaeth gref o'r broses ei hun ynghyd â'r

Pennaeth a'r Swyddog Diogelu Data Ysgolion. Gall hefyd fod yn briodol gofyn am gyngor neu gyngor cyfreithiol gan arbenigwyr annibynnol eraill megis arbenigwyr TG, lle bo hynny'n briodol.

Os yw'r ysgol yn defnyddio unrhyw broseswyr data, bydd yr ysgol yn gofyn iddynt ddarparu gwybodaeth, cymorth a mewnbwn lle bo hynny'n briodol (ac os yw'n berthnasol). Bydd proseswyr data yn dogfennu eu gweithgareddau prosesu ac yn nodi unrhyw risgiau cysylltiedig. Bydd unrhyw gontractau gyda phroseswyr data yn nodi'r gofyniad i gynorthwyo. Bydd yr ysgol yn parhau i fod yn gyfrifol am y DPIA fel y rheolwr data.

13. Ymgynghori â Rhanddeiliaid Allweddol

Efallai y bydd angen ymgynghori fel rhan o'r DPIA. Gall ymgynghori â rhanddeiliaid allweddol wasanaethu llawer o ddibenion drwy gydol y broses DPIA, megis:

- esbonio'r fenter i randdeiliaid;
- esbonio i randdeiliaid sut y bydd y broses DPIA yn cael ei defnyddio o fewn y fenter i reoli risgiau preifatrwydd;
- sefydlu arferion gwaith cyfredol y mae'r fenter yn anelu at eu diweddaru neu eu disodli;
- sefydlu sut y mae'r system neu'r broses newydd yn debygol o gael ei defnyddio'n ymarferol ac yn achos cyfleusterau pwrpas cyffredinol, eu diben tebygol;
- sefydlu pryderon preifatrwydd rhanddeiliaid;
- nodi awgrymiadau ar gyfer rheolaethau;
- esbonio'r rheolaethau a nodwyd i randdeiliaid.

Mae rhanddeiliaid allweddol yn debygol o gynnwys:

- unigolion sy'n deall y fenter o safbwynt technegol ac o ran prosesu data personol;
- unigolion a fydd yn defnyddio'r system neu'r broses newydd;
- unigolion y bydd eu data personol yn cael ei brosesu gan y system neu'r broses newydd;
- partneriaid cydweithredol;
- cyflenwyr system.

Lle y bo'n briodol, bydd yr ysgol yn ceisio ac yn dogfennu barn unigolion neu eu cynrychiolwyr ar y prosesu arfaethedig, oni bai bod rheswm da dros beidio â gwneud hynny. Os penderfynir nad yw hyn yn briodol, bydd cofnod o'r penderfyniad hwn, gydag esboniad clir, yn cael ei gofnodi fel rhan o'r DPIA.

Bydd yr ysgol hefyd yn dogfennu os yw penderfyniad y DPIA yn wahanol i farn unigolion, a bydd yn dogfennu'r rhesymau dros ddiystyru eu barn neu farn ymgyngoreion eraill.

14. Asesu Effaith

Bydd y DPIA yn ystyried yr effaith bosibl ar unigolion ac unrhyw niwed neu ddifrod a allai gael ei achosi drwy brosesu, gan gynnwys:

- anallu i arfer hawliau (gan gynnwys ond heb fod yn gyfyngedig i hawliau preifatrwydd);
- anallu i gael mynediad at wasanaethau neu gyfleoedd;
- colli rheolaeth dros ddefnyddio data personol;
- gwahaniaethu;
- dwyn hunaniaeth neu dwyll;
- colled ariannol;
- niwed i enw da;
- niwed corfforol;
- colli cyfrinachedd;
- ail-adnabod neu ddad-adnabod data; neu
- unrhyw anfantais economaidd neu gymdeithasol sylweddol arall.

15. Canlyniadau Asesiad Effaith Diogelu Data

Bydd y DPIA yn rhoi manylion am ganlyniadau'r asesiad, gan gynnwys:

- disgrifiad o natur, cwmpas, cyd-destun a dibenion y prosesu;
- disgrifiad systematig o'r gweithrediadau prosesu a ragwelir a dibenion y prosesu, gan gynnwys, lle y bo'n berthnasol, y buddiant cyfreithlon a ddilynir gan yr ysgol;
- asesiad o fesurau angenrheidiol a chymesuredd a chydymffurfiaeth y gweithrediadau prosesu mewn perthynas â'r dibenion;
- asesiad o'r risgiau i hawliau a rhyddid unigolion; a
- y mesurau a ragwelir i fynd i'r afael â'r risgiau, gan gynnwys mesurau diogelu, mesurau diogelwch a mecanweithiau i sicrhau bod data personol yn cael ei ddiogelu ac i ddangos cydymffurfiaeth, gan ystyried hawliau a buddiannau cyfreithlon gwrthrychau data a phersonau eraill dan sylw.

Bydd y DPIA yn:

- nodi goblygiadau diogelu data'r broses/system;
- ystyried effeithiau neu brosesu o safbwynt yr holl randdeiliaid;
- nodi ffyrdd y gellir osgoi effeithiau negyddol ar breifatrwydd;
- nodi ffyrdd o leihau effeithiau negyddol ar breifatrwydd;
- rhoi eglurder ynglŷn â'r angen busnes am brosesu lle na ellir osgoi effaith negyddol ar breifatrwydd.

Bydd y DPIA yn cofnodi:

- pa fesurau ychwanegol sydd wedi'u cynllunio;
- a yw pob risg wedi'i dileu, ei lleihau neu ei derbyn;
- lefel gyffredinol y 'risg weddilliol' ar ôl cymryd camau ychwanegol;
- a oes angen ymgynghori â'r ICO;
- ymatebion i farn gwrthrychau data ac unrhyw ymgyngoreion eraill, gan gynnwys y Swyddog Diogelu Data Ysgolion.

Bydd y DPIA yn cysylltu â'r Egwyddorion Diogelu Data a bydd yr Egwyddorion Diogelu Data yn cael eu cymhwyso drwy gydol cylchoedd bywyd y broses:

1. Wedi'i brosesu'n gyfreithlon, yn deg ac mewn modd tryloyw;
2. Wedi'i gasglu at ddibenion penodedig, penodol a dilys;
3. Digonol, perthnasol a chyfyngedig i'r hyn sy'n angenrheidiol (lleihau data);
4. Cywir a, lle bo angen, yn cael ei ddiweddaru;
5. Wedi'i gadw am gyhyd ag sy'n angenrheidiol yn unig;
6. Wedi'i brosesu mewn modd priodol i gynnal diogelwch.

Bydd y DPIA yn nodi'n benodol sut mae'r ysgol yn cydymffurfio â phob un o'r Egwyddorion Diogelu Data o dan *UK GDPR* ac yn egluro'n glir y sail gyfreithlon ar gyfer prosesu.

16. Camau i'w cymryd yn dilyn Cwblhau Asesiad Effaith Diogelu Data

Cyfrifoldeb y Pennaeth yw sicrhau bod y DPIA yn cael ei storio'n ddiogel.

Bydd yr ysgol yn integreiddio canlyniadau'r DPIA i gynlluniau prosiect. Bydd pwyntiau gweithredu'n cael eu nodi a phwy sy'n gyfrifol am eu gweithredu.

Bydd yr ysgol yn monitro perfformiad parhaus y DPIA.

Nid oes rhaid i DPIA ddangos bod yr holl risgiau wedi'u dileu. Ond dylai helpu'r ysgol i'w dogfennu ac asesu a oes cyfiawnhad dros unrhyw risgiau sy'n weddill ai peidio.

Os bydd yr ysgol yn penderfynu derbyn risg uchel, naill ai am nad yw'n bosibl lliniaru neu oherwydd bod costau lliniaru yn rhy uchel, bydd yr ysgol yn ymgynghori â'r ICO cyn bwrw ymlaen â'r prosesu. Nid oes rhaid i'r ysgol ddileu pob risg bob amser. Gellir penderfynu bod rhai risgiau gweddilliol, a hyd yn oed risg uchel, yn dderbyniol o ystyried manteision prosesu a/neu anawsterau lliniaru.

Bydd yr ysgol yn cadw cofnod o'r risgiau o fewn Cofrestr Risg. Bydd y Gofrestr Risg yn cofnodi, yn asesu ac yn monitro'r risgiau a nodwyd. Mae templed Cofrestr Risg ar gael ar y dudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

Mae'n arfer da i'r ysgol gyhoeddi DPIAs. Os yw'r ysgol yn pryderu y gallai cyhoeddi ddatgelu gwybodaeth fasnachol sensitif, tanseilio diogelwch neu achosi risgiau i eraill, bydd yr ysgol yn ystyried dileu manylion sensitif os oes angen, neu gyhoeddi crynodeb.

Fel rhan o'r broses gymeradwyo, bydd y Swyddog Diogelu Data Ysgolion yn cynghori a yw'r prosesu'n cydymffurfio ac yn gallu mynd yn ei flaen. Bydd cyngor y Swyddog Diogelu Data Ysgolion yn cael ei gofnodi yn y DPIA. Os nad yw'r ysgol yn dilyn cyngor y Swyddog Diogelu Data Ysgolion, dylid cofnodi'r rhesymau ac mae angen i'r ysgol sicrhau y gall gyfiawnhau ei phenderfyniad.

17. Adolygu'r Asesiad Effaith Diogelu Data

Bydd gan yr ysgol broses ar waith i adolygu'r DPIAs yn barhaus er mwyn sicrhau eu bod yn parhau'n berthnasol. Dylid monitro risgiau diogelu data a phreifatrwydd drwy gydol cylch rheoli'r broses a bydd y mesurau sydd wedi'u rhoi ar waith yn cael eu hadolygu. Dylid ystyried DPIA yn broses barhaus gydag adolygiadau rheolaidd yn seiliedig ar lefel y risg a natur y gweithgaredd prosesu.

Dylai'r Pennaeth sicrhau bod y broses DPIA yn cael ei hailystyried pe bai newid sylweddol i'r broses neu risg preifatrwydd sylweddol yn cael ei chodi.

Bydd angen ailadrodd y DPIA os bydd newid sylweddol i unrhyw un o'r canlynol mewn perthynas â phrosesu yr ymgymerir ag ef; cwmpas; cyd-destun; diben y prosesu a'r sail gyfreithlon ar gyfer prosesu.

Mae angen i DPIAs asesu unrhyw risgiau newydd os oes unrhyw newidiadau sylweddol i'r rheswm pam mae'r ysgol yn prosesu data personol neu o ran faint o ddata a gesglir. Dylai newid allanol i gyd-destun ehangach y prosesu hefyd annog yr ysgol i adolygu'r DPIA.

Bydd y Swyddog Diogelu Data Ysgolion yn rhoi cyngor ac arweiniad mewn perthynas ag adolygu DPIAs.

18. Ymgynghori â Swyddfa'r Comisiynydd Gwybodaeth (ICO) lle mae Risg Gweddilliol Uchel

Os bydd canlyniadau'r DPIA yn dangos y byddai'r prosesu'n arwain at lefel uchel o risg weddilliol i unigolion na ellir eu lliniaru, mae'r gyfraith yn mynnu yr ymgynghorir â'r ICO *cyn* i unrhyw brosesu ddigwydd.

Nid yw'r ICO yn disgwyl y bydd pob DPIA yn cael ei anfon atynt, ond rhaid ymgynghori â'r ICO os yw'r DPIA yn nodi risgiau uchel ac na all yr ysgol gymryd camau i leihau'r risgiau hynny. Dylai'r Pennaeth ymgynghori â'r Swyddog Diogelu Data Ysgolion am gyngor a hwyluso'r broses hon.

Pan fydd ymgynghoriad yn dechrau, bydd yr ICO yn darparu cyngor ysgrifenedig o fewn 8 wythnos, er mewn achosion cymhleth, gellir ymestyn y cyfnod i uchafswm o 14 wythnos. Os caiff yr amser ymateb ei ymestyn, bydd yr ICO yn cyhoeddi hysbysiad o fewn mis i'r dyddiad y cyflwynwyd y DPIA ac yn esbonio ei resymau.

Bydd yr ICO yn rhoi barn ar y prosesu arfaethedig ac, os yw'n briodol, yn rhoi manylion am yr hyn y mae'n rhaid ei wneud i wneud y prosesu'n dderbyniol o dan *UK GDPR*; cyhoeddi rhybudd ffurfiol i beidio â phrosesu'r data, neu wahardd y prosesu'n gyfan gwbl.

Ni all yr ysgol ddechrau'r prosesu nes bod yr ymgynghoriad wedi'i gwblhau.

19. Systemau neu Dechnoleg Etifeddol

Nid yw'r ysgol yn ei gwneud yn ofynnol i bob menter neu system etifeddol gael DPIA, ond maent yn arf defnyddiol i roi sicrwydd o gydymffurfiaeth diogelu data a gellir eu gweithredu os yw'n briodol.

Ar gyfer prosesau sydd eisoes wedi cael DPIA o dan *Ddeddf Diogelu Data 1998*, dim ond os bu newid sylweddol i natur, cwmpas, sail gyfreithlon, cyd-destun neu ddibenion y prosesu ers yr asesiad blaenorol o dan ddeddfwriaeth flaenorol y mae angen gwneud hynny.

Argymhellir bod DPIA yn cael ei gynnal lle nad yw gweithrediad prosesu wedi cael asesiad blaenorol a lle mae'r prosesu'n debygol o arwain at risg uchel i hawliau a rhyddid pobl naturiol.

Bydd yr ysgol yn cofnodi rhesymau dros beidio â chynnal DPIA newydd lle bo hynny'n berthnasol fel y gall yr ysgol ddangos ei bod yn cydymffurfio â deddfwriaeth.

Bydd y Swyddog Diogelu Data Ysgolion yn rhoi cyngor ac arweiniad sy'n ymwneud â mentrau neu systemau etifeddol.

20. Hyfforddiant Staff

Bydd y Swyddog Diogelu Data Ysgolion yn darparu hyfforddiant ar sut i gwblhau DPIAs i staff ysgolion a fydd yn rhan o gwblhau DPIAs.

21. Torri'r Polisi

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

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

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

22. Adolygu'r Polisi a Threfniadau Arolygiaeth

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

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

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

E-bost: dpoysgolionmon@ynysmon.gov.uk

Ffôn: 01248 751833

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

Mae rhagor o wybodaeth am Asesiadau Effaith Diogelu Data ar gael ar wefan Swyddfa'r Comisiynydd Gwybodaeth: https://ico.org.uk/

ATODIAD A- Matrics Risg Diogelu Data Ysgolion

TEBYGOLRWYDD									
	Digwyddiad bron yn sicr o ddigwydd dan y rhan fwyaf o amgylchiadau	**>70%**	**Bron yn bendant**	**A**					
	Digwyddiad yn debygol o ddigwydd dan y rhan fwyaf o amgylchiadau	**30-70%**	**Tebygol**	**B**					
	Mae'n bosibl y bydd y digwyddiad yn digwydd ar ryw amser	**10-30%**	**Posibl**	**C**					
	Digwyddiad yn annhebygol ond gall ddigwydd ar ryw amser	**1-10%**	**Annhebygol**	**D**					
	Anghyffredin yw'r digwyddiad a dim ond dan amgylchiadau eithriadol y gall ddigwydd	**<1%**	**Anghyffredin**	**E**					
					5	**4**	**3**	**2**	**1**
					Ansylweddol	**Mân**	**Cymedrol**	**Mawr**	**Trychinebus**
			Canlyniadau Diogelu Data		Effeithio nifer fach iawn o wrthrychau data.	Gall gynnwys nifer fach o wrthrychau data – dim data sensitif.	Gall gynnwys rhai gwrthrychau data neu ymwneud â data sensitif.	Gall effeithio nifer fawr o wrthrychau data. Mae camau adfer yn debygol o fod yn gymhleth a chymryd amser.	Effeithio nifer arwyddocaol o wrthrychau data. Mae camau adfer yn debygol o fod yn gymhleth a chymryd amser. Wedi'i olrhain ar lefel uwch ac yn gysylltiedig â gwybodaeth sensitif.
					EFFAITH				

Allwedd Difrifoldeb Risg

	Mân	Gall y Pennaeth reoli'r risg yn rhwydd
	Cymedrol	Gall y Pennaeth gyfyngu'r risg – efallai y bydd rhaid rhoi gwybod i'r Corff Llywodraethu
	Uchel	Ymyrraeth gan y Corff Llywodraethu Ysgol ac / neu ymglymiad Uwch Reolaeth y Gwasanaeth Dysgu
	Argyfyngus	Ymyrraeth arwyddocaol gan y Corff Llywodraethu Ysgol ac ymglymiad arwyddocaol gan Uwch Reolaeth y Gwasanaeth Dysgu

ATODIAD B

Polisi Asesiad Effaith Diogelu Data Ysgolion (DPIA)

Rhestr Wirio'r Pennaeth

Rhif	Camau i'w Cymryd	A oes gan yr ysgol hyn ar waith (Oes/Nac Oes)/ Sylwadau/Dyddiadau etc.)
1	Mae'r fersiwn gyfredol o'r Asesiad Effaith Diogelu Data *Ysgolion (DPIA)* wedi'i mabwysiadu'n ffurfiol gan Gorff Llywodraethu'r ysgol.	
2	Mae proses ar waith i fonitro cydymffurfiaeth yr ysgol â'r polisi hwn yn barhaus.	
3	Cysylltwyd â'r Swyddog Diogelu Data Ysgolion wrth ystyried gweithredu neu newid proses neu system, er mwyn penderfynu a oes angen DPIA ai peidio- mae hyn ar gyfer unrhyw ap, system, rhaglen neu wasanaeth lle mae data personol yn cael ei brosesu. Cysylltu â'r Swyddog Diogelu Data Ysgolion **cyn** prynu ac ar **ddechrau'r broses**.	
4	Cofnodir pob un o DPIAs yr ysgol ar *Gofnod Gweithgareddau Prosesu (ROPA*) yr ysgol ac mae'n cael ei ddiweddaru ac mae'n cynnwys unrhyw newidiadau/diwygiadau sy'n ymwneud â DPIAs.	
5	Cofnodir cofnod o'r holl risgiau a nodir o fewn DPIAs mewn Cofrestr Risg. Caiff risgiau eu monitro a chaiff y Gofrestr Risg ei diweddaru a'i chadw'n gyfredol.	
6	Mae'r holl DPIAs yn cael eu storio'n ddiogel ar system TG yr ysgol a gellir cael gafael arnynt yn hawdd pan fo angen.	
7	Adnabyddir rhanddeiliaid allweddol y mae angen ymgynghori â hwy fel rhan o'r broses DPIA.	
8	Cyhoeddir DPIAs lle ystyrir bod hyn yn briodol.	
9	Mae perfformiad parhaus y DPIA yn cael ei fonitro.	

Content **Page**

1. Policy Statement

The school is fully committed to protecting personal data in accordance with the requirements of the *UK General Data Protection Regulation (UK GDPR*) and the *Data Protection Act 2018.*

The *UK GDPR* includes an obligation to conduct a Data Protection Impact Assessment (DPIA) for types of processing likely to result in a *high risk* to individuals' interests.

This policy lays the framework for a formal assessment to ensure that new processes and systems introduced meet legal obligations regarding confidentiality, data protection and security.

The school will complete DPIAs, where appropriate, to demonstrate accountability and compliance with the *UK GDPR.*

2. Scope

This policy applies to all members of school staff, including temporary workers, contractors, volunteers, governors and partner organisations that introduce new processes or systems that are likely to involve a new use or significantly change the way in which personal data is handled and processed.

This policy also applies where a significant incident has occurred in relation to a current process/system or where existing processes are amended, such as undertaking current processing in different ways.

The school is committed to ensuring that a DPIA process is in place and that all new projects, processes and systems (including software and hardware) which are introduced, meet legal and statutory obligations regarding privacy, confidentiality, data protection and security.

This policy applies to all types of personal data held by the school.

The law requires that the Schools Data Protection Officer be consulted by the school as part of the DPIA process, and in order to assist to determine whether a DPIA is required or not.

3. Legislation, Guidance and Policies

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

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

This policy should also be read in conjunction with the *Schools Data Protection Policy; Schools Information Security Policy; Schools Data Processing Policy* and *Schools Retention Schedule.*

4. Definitions

Personal data	Any information relating to an identified or identifiable natural person that can be identified either directly or indirectly from that information. This can be stored electronically, on a computer, or in paper-based filing systems.
Special category data	Information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation. Special category data is personal data that needs more protection because it is sensitive.
Data controller	The people, or organisations, which determine the purposes for which, and the manner in which, any personal data is processed. The data controller has a responsibility to establish practices and policies in line with legislation. The school is the data controller.
Data 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.
Processing information	Collecting, obtaining, recording, organising, structuring, storing, retaining, amending, adapting, altering, retrieving, consulting, disseminating, restricting, disclosing, destroying, erasing information or using or doing anything with it.
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.
Risk Assessment	The identification and analysis of risks to the organisation's business objectives.
Likelihood	How likely is it that the risk will occur- uncertainty, chance and probability.
Impact	What are the consequences of the risk were it to occur. Impact is considered as having either an immediate effect or a future effect.
Control	Measure that is modifying risk.
Genetic data	Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural

	characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. Fingerprint recognition is an example of dactyloscopic data.
Cloud storage	Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the internet, or "cloud." It is maintained, operated and managed by a cloud storage service provider on storage servers that are built on virtualisation techniques.
Information Commissioner's Office (ICO)	The ICO is the UK's independent body (supervisory authority) set up to uphold information rights. The ICO's role is to uphold information rights in the public interest. This includes dealing with complaints regarding problems accessing personal information from an organisation, or if there are concerns about how an organisation has handled information- if the information is wrong, has been lost or disclosed to someone else. Data breaches that are a high risk to individuals are reported to the ICO.

5. Responsibilities

5.1. School Governing Body

The school governing body has the responsibility for:

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

5.2. Headteacher (and/or Person Responsible for Data Protection within the School)

The Headteacher and/or the person who is responsible for data protection within the school is responsible for:

- ensuring that school staff are aware of the DPIA process and fully comply with the policy;
- contacting the Schools Data Protection Officer when implementing or changing a process or system, in order to determine whether a DPIA is required or not;
- identifying key stakeholders that need to be consulted as part of the DPIA process;
- ensuring that the DPIA process is revisited should there be a substantial change to process or a significant privacy risk raised;
- integrating the outcomes of the DPIA into project plans;
- maintaining a log of all of the school's DPIAs as part of the *Record of Processing Activities (ROPA*);
- monitoring the ongoing performance of the DPIA;
- keeping a record of the risks within a Risk Register;
- publishing DPIAs if appropriate;
- ensuring that the DPIA is stored securely.

5.3 Staff within the School

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

- complying with this policy to ensure that processing remains compliant with current legislation if implementing or changing a process or system;
- being able to identify when a DPIA may be required and to notify the Headteacher;
- undertaking any training provided regarding DPIAs if this is relevant to job role.

5.4. Schools Data Protection Officer

The Schools Data Protection Officer is responsible for:

- assisting the Headteacher to determine whether a DPIA is required or not when implementing or changing a process or system;
- assisting the Headteacher in completing a *DPIA Screening Checklist*;
- supporting the school to complete a DPIA;
- providing advice on what measures and safeguards the school can take to mitigate risks;
- confirming that the DPIA has been completed correctly;
- facilitating the process of consulting with the Information Commissioner's Office (ICO) where there is a high residual risk;
- providing advice on the outcome of the DPIA and whether the processing can go ahead;
- providing advice to the Headteacher regarding publishing DPIAs;
- providing advice and guidance in relation to reviewing DPIAs;
- providing advice and guidance relating to legacy initiatives or systems;
- maintaining a log of DPIAs on behalf of all schools;
- monitoring the DPIA's ongoing performance, including how well the school has implemented planned actions to address the risks;
- ensuring that all data processing agreements include the requirement for data processors to assist the school to document processing activities and to identify any associated risks;
- ensuring that the DPIA will link and comply with each of the Data Protection Principles;
- providing training on how to complete DPIAs to school staff who will be a part of completing DPIAs.

6. What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a structured approach to identifying data protection risks associated with the processing of personal data; to help the school identify and minimise the risks and for implementing appropriate controls to manage them. **A DPIA is a legal requirement for processing that is likely to be *high risk*.**

The DPIA is an evaluation tool designed to systematically and comprehensively analyse, identify, minimise and address the data protection, privacy and security risks of

processing. A DPIA assesses the likelihood and impact of a compromise to the confidentiality, integrity and/or availability of personal data.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the *potential* for harm – to individuals or to society at large, whether it is physical, material or non-material.

The school will make an objective assessment of the risks and will use the *Schools Data Protection Risk Matrix* (APPENDIX A) to think about likelihood and severity of risks. The *Schools Data Protection Risk Matrix* is also available on the Data Protection page on the Learning Service Microsite.

All new projects, programmes, processes, information systems (including software and hardware) and other relevant information assets should be developed and implemented in a secure and structured manner and comply with legal and statutory requirements. They must comply with confidentiality, privacy and data protection requirements. All new processes or systems must be tested against these requirements before they are introduced.

To determine whether any proposed changes to the school processes and information assets impacts on the confidentiality, integrity and accessibility of personal and/or sensitive data, the school will utilise the DPIA to test against these requirements.

DPIAs will be imbedded into the school's processes and risk management framework. DPIA requirements are included in all relevant policies, processes and procedures.

The school will ensure the outcome can influence the school's plans. A DPIA is initiated and maintained throughout the development and implementation of a project, process or system.

7. Purpose of Data Protection Impact Assessments

The purpose of the DPIA is to highlight any privacy risks associated with a project or process and to ensure that the proposed uses of personal data are fully understood.

The DPIA reports and captures the details of potential impacts identified and the solutions or actions that will reduce the impact or mitigate the risk. The *UK GDPR* requires a level of assessment to be completed that is proportionate to the risks involved in the processing.

DPIAs are specifically mandated by the *UK GDPR* to assess the risks to data subjects' privacy and data protection rights arising out of the school's processing activities.

DPIAs are a legal requirement for processing that is likely to be *high risk*. An effective DPIA can also bring broader compliance; financial and reputational benefits; helping to demonstrate accountability and building trust and engagement with individuals.

8. Key Elements of a Data Protection Impact Assessment Process

A DPIA should begin early in the life of a project, process or system, ***before*** processing begins, and run alongside the planning and development process.

A DPIA should include these steps:

Step 1: identify the need for a DPIA;
Step 2: describe the processing;
Step 3: consider consultation;
Step 4: assess necessity and proportionality;
Step 5: identify and assess risks;
Step 6: identify measures to mitigate the risks;
Step 7: sign off and record outcomes.

The school will scale the time and resources needed for a DPIA to fit the nature of the process.

9. Key Benefits of Data Protection Impact Assessments

Key benefits of DPIAs include:

- fulfilling the school's statutory obligations;
- contributing towards effective risk management and increased privacy and data protection awareness across the school;
- giving individuals confidence that the school is taking steps to safeguard their privacy, and a better understanding of the ways in which their personal data is being used;
- improve the school's relationship with individuals and improve the school's understanding of individuals' needs, concerns and expectations;
- demonstrating that the school is taking actions which are less likely to be privacy intrusive and have a negative impact on individuals;
- ensuring that initiatives are likely to be successful because privacy risks are identified early, allowing controls to be designed at less cost and with less impact on delivery.

10. Identifying the need for a Data Protection Impact Assessment

To determine whether a DPIA is required, the school must identify whether personal data is being processed. Some examples of such information include:

- information linked or linkable to an individual;
- date of birth, place of birth, race, religion, weight, geographical indicators; employment, medical, education and financial information;

- name (e.g. full name, maiden name, mother's maiden name, or alias);
- address information (e.g. street or e-mail address);
- information identifying personally owned property (e.g. vehicle registration number);
- telephone numbers, mobile, and personal numbers;
- personal characteristics, including photo (face or distinguishing features), fingerprints, biometric data (retina scan, etc.);
- personal identification number (e.g. National Insurance Number, passport number, driver's licence, financial account or credit number).

11. When Data Protection Impact Assessments must be Undertaken

It is mandatory to undertake a DPIA before beginning any processing that involves personal data which is *likely to result in a high risk.* This ensures that privacy risks are identified and considered before they are implemented into the design and reviewed regularly throughout the lifecycle.

The *DPIA Screening Checklist* will be used as a preliminary stage to assist the school to determine when DPIAs are required.

Requirement for DPIAs is not restricted to formal projects. Risk to the privacy of individuals can arise in many scenarios or initiatives.

DPIAs may be required for proposals to undertake new processing of personal data or where existing processes are amended, such as undertaking current processing in different ways.

All new or significantly changed processes or projects that involve personal data that are planned to be introduced must comply with confidentiality, privacy and data protection legislation and requirements.

A DPIA will be undertaken in the early stages of an initiative. The law requires the school to undertake a DPIA if it intends to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data (sensitive data) on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires the school to undertake a DPIA if it intends to:

- use new, innovative, technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (e.g. facial recognition used to allow access to systems);
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing:

- them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

Examples of scenarios or initiatives which may require a DPIA include:

- a proposal to build a new IT system for storing or accessing personal data;
- implementing surveillance technology in a building, such as a CCTV system;
- using a cloud service for the storage of data;
- developing policies or strategies that have privacy implications.

The Headteacher will need to consider whether any processing requires a DPIA and will consult the Schools Data Protection Officer.

Factors to consider include whenever the processing:

- involves the collection of new information about individuals;
- uses information about individuals for a purpose it is not currently used for, or in a way it is not currently used;
- involves the use of new technology that might be perceived as being privacy intrusive;
- may result in making decisions, or taking action against individuals in ways that can have a significant impact on them;
- involves information about individuals of a kind particularly likely to raise privacy concerns or expectations such as vulnerable individuals.

Children are regarded as vulnerable to the processing of their personal data since they may be less able to understand how their data is being used, anticipate how this might affect them, and protect themselves against any unwanted consequences.

If there is uncertainty regarding whether it is appropriate to carry out a DPIA for a specific project, process or system, the Headteacher should consult the Schools Data Protection Officer for clarification and advice.

12. Who should undertake a Data Protection Impact Assessment?

The school as the data controller is ultimately responsible and accountable for compliance with data protection legislation. The Headteacher is responsible for ensuring that DPIAs are undertaken. It is important that staff are able to identify when a DPIA may be required and to notify the Headteacher.

The Headteacher will consult the Schools Data Protection Officer as part of the DPIA process, and in order to assist to determine whether a DPIA is required or not. The Schools Data Protection Officer must provide advice and input.

A DPIA should be conducted by the process owner and assisted by those involved in the business process that have the right knowledge and a strong understanding of the process itself along with the Headteacher and the Schools Data Protection Officer. It may also be appropriate to seek legal advice or advice from other independent experts such as IT experts, where appropriate.

If the school uses any data processors, the school will ask them to provide information, assistance and input where appropriate (and if applicable). Data processors will document their processing activities and identify any associated risks. Any contracts with data processors will note the requirement to assist. The school will remain responsible for the DPIA as the data controller.

13. Consultation with Key Stakeholders

Consultation may be required as part of the DPIA. Consultation with key stakeholders can serve many purposes throughout the DPIA process, such as:

- explaining the initiative to stakeholders;
- explaining to stakeholders how the DPIA process will be used within the initiative to manage privacy risks;
- establishing current working practices that the initiative aims to update or replace;
- establishing how the new system or process is likely to be used in practice and in the case of general purpose facilities, their likely purpose;
- establishing the privacy concerns of stakeholders;
- soliciting suggestions for controls;
- explaining identified controls to stakeholders.

Key stakeholders are likely to include:

- individuals who understand the initiative from a technical point of view and in terms of personal data processing;
- individuals who will be using the new system or process;
- individuals whose personal data will be processed by the new system or process;
- collaborative partners;
- the suppliers of a system.

Where appropriate, the school will seek and document the views of individuals or their representatives on the intended processing, unless there is a good reason not to. If it is decided that this is not appropriate, a record of this decision, with a clear explanation, will be documented as part of the DPIA.

The school will also document if the DPIA decision differs from the views of individuals, and will document the reasons for disregarding their views or the views of other consultees.

14. Assessing Impact

The DPIA will consider the potential impact on individuals and any harm or damage that might be caused by processing, including:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification or de-identification of data; or
- any other significant economic or social disadvantage.

15. Outcomes of a Data Protection Impact Assessment

The DPIA will provide details around the outcomes of the assessment, including:

- a description of the nature, scope, context and purposes of the processing;
- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the school;
- an assessment of the necessity and proportionality and compliance measures of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of individuals; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance, taking into account the rights and legitimate interests of data subjects and other persons concerned.

The DPIA will:

- identify the data protection implications of the process/system;
- consider the impacts or processing from the perspectives of all stakeholders;
- identify ways in which negative impacts on privacy can be avoided;
- identify ways to lessen negative impacts on privacy;
- provide clarity as to the business need for processing where negative impact on privacy is unavoidable.

The DPIA will record:

- what additional measures are planned;
- whether each risk has been eliminated, reduced or accepted;
- the overall level of ‘residual risk’ after taking additional measures;
- whether the ICO needs to be consulted;

- responses to the views of data subjects and any other consultees, including the Schools Data Protection Officer.

The DPIA will link to the Data Protection Principles and the Data Protection Principles will be applied throughout the lifecycles of the process:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified, explicit and legitimate purposes;
3. Adequate, relevant and limited to what is necessary (data minimisation);
4. Accurate and, where necessary, kept up to date;
5. Retained only for as long as necessary;
6. Processed in an appropriate manner to maintain security.

The DPIA will explicitly state how the school is complying with each of the Data Protection Principles under *UK GDPR* and clearly explain the lawful basis for processing.

16. Steps to take following Completion of Data Protection Impact Assessment

It is the responsibility of the Headteacher to ensure that the DPIA is stored securely.

The school will integrate the outcomes of the DPIA into project plans. Action points will be identified and who is responsible for implementing them.

The school will monitor the ongoing performance of the DPIA.

A DPIA does not have to indicate that all risks have been eradicated. But it should help the school document them and assess whether or not any remaining risks are justified.

If the school decides to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, the school will consult the ICO before going ahead with the processing. The school does not always have to eliminate every risk. It may be decided that some residual risks, and even a high risk, are acceptable given the benefits of the processing and/or the difficulties of mitigation.

The school will keep a record of the risks within a Risk Register. The Risk Register will record, assess and monitor the identified risks. A Risk Register template is available on the Data Protection page on the Learning Service Microsite.

It is good practice for the school to publish DPIAs. If the school is concerned that publication may reveal commercially sensitive information, undermine security or cause others risks, the school will consider removing sensitive details if necessary, or publish a summary.

As part of the sign-off process, the Schools Data Protection Officer will advise on whether the processing is compliant and can go ahead. The Schools Data Protection Officer's advice will be recorded in the DPIA. If the school doesn't follow the Schools Data Protection Officer's advice, reasons should be recorded and the school needs to ensure it can justify its decision.

17. Review of the Data Protection Impact Assessment

The school will have a process in place to keep DPIAs under ongoing review to ensure they remain relevant. Data protection and privacy risks should be monitored throughout the process management cycle and the measures that have been put in place will be reviewed. A DPIA should be seen as an ongoing process with regular reviews based on the level of risk and the nature of the processing activity.

The Headteacher should ensure that the DPIA process is revisited should there be a substantial change to process or a significant privacy risk raised.

The DPIA will need to be repeated if there is a substantial change to any of the following in relation to processing being undertaken- nature; scope; context; purpose of the processing and lawful basis for processing.

DPIAs need to assess any new risks if there are any significant changes in why the school processes personal data or in the amount of data collected. An external change to the wider context of the processing should also prompt the school to review the DPIA.

The Schools Data Protection Officer will provide advice and guidance in relation to reviewing DPIAs.

18. Consultation with the Information Commissioner's Office (ICO) where there is High Residual Risk

In the event that the results of the DPIA indicate the processing would result in a high level of residual risk to individuals that cannot be mitigated, the law requires that the ICO is consulted *before* any processing takes place.

The ICO does not expect that every DPIA will be sent to them, but the ICO must be consulted if the DPIA identifies high risks and the school cannot take measures to reduce those risks. The Headteacher should consult the Schools Data Protection Officer for advice and to facilitate this process.

When a consultation is started, the ICO will provide written advice within 8 weeks, although in complex cases, the period may be extended to a maximum of 14 weeks. If the response time is extended, the ICO will issue a notification within one month of the date the DPIA was submitted and explain its reasons.

The ICO will provide a judgement on the proposed processing and, if appropriate, give details of what must be done to make the processing acceptable under the *UK GDPR*; issue a formal warning not to process the data, or ban the processing altogether.

The school cannot begin the processing until the consultation has been completed.

19. Legacy Systems or Technology

The school does not require all legacy initiatives or systems to have a DPIA, however they are a useful tool to provide assurance of data protection compliance and can be implemented if it is appropriate.

For processes that have already undergone a PIA under the *Data Protection Act 1998*, it is only necessary to conduct a DPIA if there has been a significant change to the nature, scope, lawful basis, context or purposes of the processing since the previous assessment under previous legislation.

It is recommended that a DPIA is conducted where a processing operation has not had a previous assessment and where the processing is likely to result in a high risk to the rights and freedoms of natural persons.

The school will document reasons for not conducting a new DPIA where relevant so that the school can demonstrate compliance with legislation.

The Schools Data Protection Officer will provide advice and guidance relating to legacy initiatives or systems.

20. Staff Training

The Schools Data Protection Officer will provide training on how to complete DPIAs to school staff who will be a part of completing DPIAs.

21. Breach of the Policy

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

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

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

22. Review of Policy and Oversight Arrangements

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

This policy will be approved by the Learning Service Senior Management Team and will be adopted by the school governing body. Compliance with this policy and related procedures will be monitored by the School Leadership Team and the governing body.

If there are any queries or concerns about anything contained in this policy, the Schools Data Protection Officer should be contacted without hesitation:

E-mail: dpoysgolionmon@ynysmon.gov.uk

Telephone: 01248 751833

Address:
Learning Service
Isle of Anglesey County Council
Council Offices
Llangefni
Anglesey
LL77 7TW

Further information regarding Data Protection Impact Assessments can be obtained from the ICO website: https://ico.org.uk

APPENDIX A- Schools Data Protection Risk Matrix

LIKELIHOOD									
	Event is almost certain to occur in most circumstances	**>70%**	**Almost certain**	**A**					
	Event likely to occur in most circumstances	**30-70%**	**Likely**	**B**					
	Event will possibly occur at some time	**10-30%**	**Possible**	**C**					
	Event unlikely and may occur at some time	**1-10%**	**Unlikely**	**D**					
	Event rare and may occur only in exceptional circumstances	**<1%**	**Rare**	**E**					
					5	**4**	**3**	**2**	**1**
					Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
			Data Protection Consequences		Affects a minimal number of data subjects.	May involve a small number of data subjects – no sensitive data.	May involve some data subjects or relates to sensitive data.	May affect a large amount of data subjects. Remediation is likely to be time consuming and complex.	Affects a significant numbers of data subjects. Remediation is likely to be time consuming and complex, tracked at a senior level and related to sensitive information.
					IMPACT				

Risk Severity Key

	Minor	Risk easily managed by the Headteacher
	Moderate	Risk containable by the Headteacher – School Governing Body may need to be informed
	Major	Intervention by the School Governing Body and / or Learning Service Senior Management involvement
	Critical	Significant School Governing Body and Learning Service Senior Management intervention

APPENDIX B

Schools Data Protection Impact Assessment (DPIA) Policy

Headteacher's Checklist

No	Actions to be Taken	Has the school got this in place (Yes/No)/ Comments/Dates etc.)
1	The current version of the *Schools Data Protection Impact Assessment (DPIA)* has been formally adopted by the School Governing Body.	
2	There is a process in place to continually monitor the school's compliance with this policy.	
3	The Schools Data Protection Officer has been contacted when considering implementing or changing a process or system, in order to determine whether a DPIA is required or not- this is for any app, system, programme or service where personal data is being processed. To contact the SDPO **before** purchasing and at the **very beginning of the process**.	
4	All of the school's DPIAs are recorded on the school's *Record of Processing Activities (ROPA*) and this is kept up-to-date and includes any changes/amendments relating to DPIAs.	
5	A record of all of the risks identified within DPIAs are recorded in a Risk Register. The risks are monitored and the Risk Register is kept up-to-date.	
6	All DPIAs are stored securely on the school's IT system and they can be easily accessed when needed.	
7	Key stakeholders that need to be consulted as part of the DPIA process are identified.	
8	DPIAs are published where this is considered appropriate.	
9	The ongoing performance of the DPIA is monitored.	