Ffedarasiwn Cwrt Henri, Ffairfach a Talyllychau

Pennaeth / Headteacher - Mr Gethin Richards MA, BSc

richardsg75@hwbcymru.net

Penaethiaid Cynorthwyol / Assistant Headteacher

Mrs A Vaughan-Owen / Mrs A Morgan / Miss A Walker

Polisi a Gweithdrefnau Trin Gwybodaeth Bersonol

Handling Personal Information

Policy & Procedure

Cynnwys

1. Cyflwyniad

1.1 Mae Ffederasiwn Ysgolion Talyllychau, Cwrt Henri a Ffairfach yn casglu ac yn defnyddio ystod eang o ddata personol am ein disgyblion a'n staff er mwyn darparu addysg a gofal bugeiliol. Os methwn â gofalu'n ddigonol am y data personol sy'n cael ei drin gennym, a'i fod yn cael ei golli, ei ddwyn, ei ddatgelu mewn modd amhriodol, neu ei gamddefnyddio mewn modd arall, gallai effaith hynny ar yr unigolion dan sylw fod yn ddifrifol, gan amrywio o boen meddwl i niwed corfforol. Felly mae gwybodaeth bersonol yn ased gwerthfawr, ond byddwn hefyd yn atebol os byddwn yn trin y wybodaeth honno mewn modd anghywir.

1.2 Lluniwyd y polisi hwn a'r gweithdrefnau hyn felly er mwyn sicrhau bod gwybodaeth bersonol yn cael ei thrin yn ddiogel, ac yn enwedig o ran ei storio a'i throsglwyddo, er mwyn cynorthwyo i gydymffurfio â rhwymedigaethau cyfreithiol yr Ysgol.

2. Diffiniad o wybodaeth bersonol

2.1 Gwybodaeth bersonol neu ddata personol yw unrhyw wybodaeth sy'n ymwneud ag unigolyn byw y mae modd adnabod pwy ydyw yn uniongyrchol neu'n anuniongyrchol drwy ddefnyddio'r wybodaeth.

2.2 Yn ymarferol, mae hyn yn debygol o gynnwys amrywiaeth eang iawn o ddata, gan gynnwys y canlynol, ond nid y canlynol yn unig:

- Enwau, cyfeiriadau a dyddiadau geni
- Cyfeirnodau megis Rhifau Unigryw Disgyblion
- Gwybodaeth ariannol bersonol megis manylion banc
- Gwybodaeth ddisgrifiadol neu fywgraffyddol am unigolyn
- Ffotograffau neu ddelweddau eraill

2.3 Defnyddir y termau 'gwybodaeth bersonol' a 'data personol' drwy gydol y polisi hwn a'r weithdrefn hon a'r un yw eu hystyr.

2.4 Hefyd mae categorïau arbennig o wybodaeth bersonol ac mae'n rhaid inni fod yn ofnadwy o ofalus wrth ymdrin â'r rhain. Y categorïau arbennig hyn yw gwybodaeth bersonol ynghylch:

- Hil neu gefndir ethnig
- Barn Wleidyddol
- Credoau crefyddol neu athronyddol
- Aelodaeth o Undeb Llafur
- Data genetig
- Data biometrig
- Iechyd
- Bywyd rhywiol neu gyfeiriadedd rhywiol

2.5 Yn ogystal mae gofynion penodol ar gyfer gwybodaeth mewn perthynas â chollfarnau troseddol a throseddau.

3. Cefndir cyfreithiol

3.1 Mae'r ddeddfwriaeth Diogelu Data yn cyflwyno rheolau mewn perthynas â phrosesu data personol. Diffinnir prosesu fel casglu, cofnodi, storio a gwneud unrhyw ddefnydd o'r data personol, gan gynnwys ei ddatgelu a'i waredu.

3.2 Mae'n ofynnol i ni ddilyn chwe egwyddor mewn perthynas â phrosesu data personol. Mae'r chweched egwyddor yn nodi'n benodol bod yn rhaid defnyddio mesurau technegol neu gyfundrefnol priodol er mwyn diogelu rhag prosesu data personol heb ganiatâd neu'n anghyfreithlon a diogelu rhag colli, difetha neu ddifrodi data personol yn ddamweiniol.

3.3 Os methir â thrin data personol yn gywir gallai olygu y bydd canlyniadau difrifol i'r Ysgol, gan y gellir rhoi dirwyon gweinyddol o hyd at €20,000,000 am achosion difrifol o dorri rheolau Diogelu Data.

4. Datganiadau polisi

4.1 Mae Ffederasiwn Ysgolion Talyllychau, Cwrt Henri a Ffairfach wedi ymrwymo i brosesu gwybodaeth bersonol yn unol â gofynion y ddeddfwriaeth Diogelu Data.

4.2 Mae'r Ysgolion yn ystyried bod trin data personol mewn modd cywir yn hanfodol wrth ddarparu ein gwasanaethau a chynnal hyder y bobl rydym yn ymdrin â nhw.

4.3 Bydd unrhyw ddata personol a gedwir gan yr Ysgol nad yw'n agored i'r cyhoedd yn cael ei drin bob amser yn gwbl gyfrinachol.

4.4 Bydd yr Ysgol yn defnyddio dulliau electronig diogel gymaint â phosibl i storio a throsglwyddo data personol.

4.5 Mae'r polisi hwn wedi cael ei gymeradwyo gan Gorff Llywodraethu'r Ysgol, ac mae'n cael ei gefnogi'n llwyr ganddo.

5. Cwmpas

5.1 Mae'r polisi hwn a'r gweithdrefnau hyn yn berthnasol i'r holl ddata personol sy'n eiddo i'r Ysgol.

5.2 Mae'r polisi hwn a'r gweithdrefnau hyn yn berthnasol i holl weithwyr yr Ysgol, gan gynnwys:

- Gweithwyr dros dro a gweithwyr asiantaeth
- Gwirfoddolwyr
- Contractwyr sy'n gweithredu fel proseswyr data

6. Cyfrifoldebau

6.1 Mae gweithwyr yr ysgol yn gyfrifol am y canlynol:

- Diogelu'r wybodaeth bersonol y maent yn ei phrosesu drwy gadw'n llawn at y polisi hwn a'r gweithdrefnau hyn.

6.2 Mae penaethiaid yn gyfrifol am y canlynol:

- Sicrhau bod eu gweithwyr yn gwybod am y polisi hwn a'r gweithdrefnau hyn ac yn deall eu gofynion
- Sicrhau bod gofynion y polisi a'r gweithdrefnau'n cael eu gweithredu'n llawn o fewn yr Ysgol
- Sicrhau bod eu gweithwyr wedi derbyn hyfforddiant priodol ynghylch gofynion Diogelu Data
- Cymryd camau priodol pan fydd y polisi a'r gweithdrefnau wedi cael eu torri

6.3 Os torrir y polisi a'r gweithdrefnau hyn yna gall arwain at gymryd camau disgyblu yn erbyn y gweithwyr sy'n gyfrifol am wneud hynny.

7. Defnyddio dyfeisiau cludadwy, cyfryngau symudadwy a storio ar gwmwl

7.1. Mae'r dyfeisiau cludadwy yn cynnwys y canlynol, ond nid y canlynol yn unig:

- Gliniaduron a llechi
- Ffonau clyfar

7.2. Mae'r cyfryngau symudadwy yn cynnwys y canlynol, ond nid y canlynol yn unig:

- Cof bach USB/dyfeisiau storio
- Cardiau SD
- CD-Roms a DVDs

7.3 Rhaid peidio â phrosesu gwybodaeth bersonol ar gyfryngau symudadwy nad ydynt yn eiddo i'r Ysgol.

7.4 Rhaid peidio â phrosesu gwybodaeth bersonol ar ddyfeisiau cludadwy nad ydynt yn eiddo i'r Ysgol oni bai bod dyfais rheoli briodol a ddarperir gan yr Ysgol ar waith.

7.5. Rhaid defnyddio dyfeisiau cludadwy neu gyfryngau symudadwy i gasglu, i storio, i gludo neu i drosglwyddo gwybodaeth bersonol dim ond os oes gwir angen gwneud hynny ac nad oes opsiwn arall ar gael.

7.6 Cyn defnyddio dyfeisiau cludadwy neu gyfryngau symudadwy i gasglu, i storio, i gludo neu i drosglwyddo gwybodaeth bersonol, rhaid cael caniatâd gan y Pennaeth, y Dirprwy Bennaeth neu Bennaeth y Flwyddyn.

7.7 Rhaid peidio byth â chadw data personol ar ddyfeisiau cludadwy neu gyfryngau symudadwy oni bai ei fod wedi'i amgryptio.

7.8 Rhaid i ddyfeisiau cludadwy neu gyfryngau symudadwy sy'n cynnwys gwybodaeth bersonol gael eu storio a'u cludo'n ddiogel.

8. Storio gwybodaeth bersonol yn ddiogel

8.1 Rhaid i gofnodion papur, dyfeisiau cludadwy a chyfryngau symudadwy sy'n cynnwys gwybodaeth bersonol gael eu cadw'n ddiogel yn yr Ysgol. Bydd hyn yn golygu eu cadw mewn cypyrddau clo pan nad ydynt yn cael eu defnyddio a sicrhau na all unigolion anawdurdodedig gael gafael ar yr allweddi. Rhaid defnyddio offer diogelu adeiladau digonol.

8.2 Lle bo'n bosibl, dylid lleihau achosion o storio data personol ar ffurf cofnodion papur.

8.3 Ar safle'r Ysgol, rhaid peidio â gadael data personol heb neb yn gofalu amdano lle gall unrhyw un gael gafael ynddo, megis ar ddesgiau, siliau ffenestri, coridorau, argraffwyr a llun-gopïwyr.

8.4 Rhaid peidio â phrosesu gwybodaeth bersonol ar offer cyfrifiadurol nad ydynt yn eiddo i'r Ysgol.

8.4 Rhaid sicrhau bod data personol sy'n cael ei brosesu ar gyfrifiaduron yn y swyddfa wedi'i ddiogelu gyda chyfrinair ac ni ddylid byth adael y data hwn ar sgrîn lle gellir ei weld, os nad oes rhywun wrth y cyfrifiadur.

8.5 Rhaid peidio byth â storio gwybodaeth bersonol sy'n cael ei phrosesu ar gyfrifiaduron ar ddisg caled y cyfrifiadur. Mae hyn yn diogelu'r data os bydd y cyfrifiadur yn methu neu'n cael ei ddwyn.

8.6 Rhaid peidio byth â llwytho/storio data personol ar gwmwl nad yw wedi cael ei ddarparu gan yr ysgol. Mae hyn yn cynnwys y canlynol, ond nid y canlynol yn unig:

- Cyfrifon e-bost personol (megis Gmail, Hotmail)
- Dropbox
- Microsoft OneDrive

8.7 Pan fo gwybodaeth bersonol yn cael ei dangos ar sgriniau cyfrifiaduron a ddefnyddir mewn man cyhoeddus, rhaid sicrhau nad yw disgyblion nac ymwelwyr i'r Ysgol yn gallu gweld y wybodaeth honno.

9. Cymryd gwybodaeth bersonol allan o'r Ysgol

9.1 Rhaid peidio â chymryd gwybodaeth bersonol o safle'r Ysgol oni bai bod hynny'n gwbl angenrheidiol a hefyd mae'n rhaid cael caniatâd y rheolwr perthnasol neu'r Pennaeth, y Dirprwy Bennaeth neu Bennaeth y Flwyddyn.

.

9.2 Pan fydd cofnodion papur, dyfeisiau cludadwy neu gyfryngau symudadwy sy'n cynnwys gwybodaeth bersonol yn cael eu cymryd allan o'r swyddfa, rhaid eu cadw'n ddiogel, eu cludo'n ddiogel

a rhaid peidio byth â'u gadael yn rhywle heb neb yn gofalu amdanynt lle gall unigolion anawdurdodedig gael mynediad iddynt megis mewn cerbydau neu mewn mannau sy'n agored i'r cyhoedd.

9.3 Rhaid peidio â mynd â chofnodion papur sy'n cynnwys gwybodaeth bersonol adref heb yn gyntaf gael caniatâd y Pennaeth, y Dirprwy Bennaeth neu Bennaeth y Flwyddyn, sy'n gyfrifol am sicrhau bod amgylchedd gwaith addas ar gael gan gynnwys lle y gellir storio papurau yn ddiogel megis drôr neu gabinet â chlo. Dylid gwneud cofnod o'r wybodaeth sy'n cael ei chymryd oddi ar y safle, pa bryd y cafodd ei chymryd, gan bwy a pha bryd y caiff ei dychwelyd.

9.4 Rhaid peidio â chadw cofnodion papur yn y cartref am gyfnod hwy na'r hyn sy'n angenrheidiol a rhaid eu dychwelyd i safle'r swyddfa cyn gynted ag y bo modd.

9.5 Rhaid peidio â chaniatáu i aelodau o'r teulu, nac i unrhyw unigolion eraill anawdurdodedig, gael gweld unrhyw wybodaeth bersonol, mewn unrhyw fformat, sy'n cael ei chludo adref.

10. Trosglwyddo gwybodaeth bersonol y tu allan i'r Ysgol

10.1. Mae hyn yn cynnwys anfon data personol at y canlynol:

- Llywodraeth Cymru
- Ysgolion Eraill
- Cyngor Sir Caerfyrddin ac awdurdodau lleol eraill
- Asiantaethau, cwmnïau a sefydliadau allanol
- Rhieni a disgyblion

10.2 Rhaid peidio ag anfon gwybodaeth bersonol y tu allan i'r Ysgol oni bai fod hynny'n gwbl angenrheidiol a bod hynny'n unol â'r gyfraith.

10.3 Rhaid peidio â darparu data personol i unrhyw sefydliad allanol os gellid defnyddio gwybodaeth heb enwau neu wybodaeth ystadegol fel dewis arall. Os ydym yn darparu gwybodaeth bersonol yna dylai fod yn berthnasol ac ni ddylai fod yn fwy na'r hyn sy'n gwbl angenrheidiol at bwrpas penodedig.

11. Defnyddio dull electronig i drosglwyddo gwybodaeth

11.1 Y ffordd fwyaf diogel a chyflym o drosglwyddo gwybodaeth bersonol y tu allan i'r Ysgol yw trwy ddull electronig diogel. Rhaid ystyried hyn fel y dewis cyntaf bob amser a'i ddefnyddio lle bynnag y gellir. Gallai dulliau o'r fath gynnwys y canlynol, ond nid y canlynol yn unig:

- Y System Drosglwyddo Gyffredin/School2School
- Anfon neges e-bost drwy ddefnyddio system e-bost ddiogel megis Egress Switch
- Anfon y wybodaeth drwy rwydwaith e-bost diogel megis Zimbra, lle mae cyfrifon gan yr anfonwr a'r derbynnydd
- Anfon neges e-bost drwy Zimbra i gyfeiriadau e-bost Cyngor Sir Caerfyrddin

11.2 Wrth ddefnyddio e-bost diogel, dylid osgoi anfon at grwpiau neu restri o gysylltiadau gan fod hynny'n golygu bod perygl y gellid datgelu gwybodaeth bersonol i dderbynwyr sydd heb yr awdurdod i gael mynediad i'r wybodaeth honno. Rhaid cymryd yr un gofal wrth ateb negeseuon e-bost, oherwydd trwy ddewis 'ateb i bawb' gallai hynny arwain at anfon gwybodaeth at dderbynwyr nas bwriedir ac sydd heb awdurdod i dderbyn y wybodaeth honno.

11.3 Wrth ddechrau teipio cyfeiriad e-bost, yn aml bydd y meddalwedd e-bost yn awgrymu amryw o gyfeiriadau tebyg a ddefnyddiwyd eisoes. Mae'n hanfodol bod y cyfeiriad cywir yn cael ei ddewis cyn anfon y neges.

11.4 Rhaid cynnwys cyfarwyddiadau clir ynghylch y modd y dylai'r derbynnydd drin y wybodaeth, er enghraifft, os na ddylid anfon y wybodaeth ymlaen heb gysylltu â'r anfonwr yn gyntaf.

11.5 Pan nad oes dull electronig diogel ar gael ac nad yw'r wybodaeth yn ddata personol sensitif, neu fel arall yn debygol o achosi niwed neu ofid os caiff ei ddatgelu i drydydd parti, yna gellir ei hanfon drwy neges e-bost safonol heb angen unrhyw asesiad pellach o risg. Enghraifft o hyn fyddai ateb gohebiaeth unigolyn ynghylch mater amlwg sydd eisoes yn wybodaeth gyhoeddus. Er hynny, rhaid cymryd gofal i sicrhau bod y wybodaeth yn cael ei hanfon i'r cyfeiriad e-bost cywir.

12. Defnyddio dulliau eraill i drosglwyddo data personol

12.1 Mae dulliau eraill o drosglwyddo data personol yn cynnwys y canlynol, ond nid y canlynol yn unig:

- Y Post Brenhinol
- Negesydd
- Dosbarthu/casglu â llaw

12.2 Pan nad oes dull electronig diogel ar gael ac nad yw'r wybodaeth yn ddata personol sensitif, yna gellir anfon y wybodaeth drwy'r Post Brenhinol heb angen unrhyw asesiad pellach o risg. Enghraifft o hyn fyddai llythyr yn rhoi gwybod i berson ei fod wedi bod yn llwyddiannus yn ei gais am swydd. Hefyd mae angen inni fel mater o drefn anfon llythyrau sy'n cynnwys gwybodaeth bersonol at ein cwsmeriaid, er enghraifft, mewn perthynas â hawliadau am fudd-daliadau. Er hynny, rhaid cymryd gofal i sicrhau bod y wybodaeth yn cael ei hanfon i'r cyfeiriad cywir at dderbynnydd a enwir.

12.3 Os nad oes dull electronig diogel a bod y wybodaeth sydd i'w hanfon yn wybodaeth bersonol sensitif, yna rhaid ystyried y canlynol bob amser wrth benderfynu pa ddull trosglwyddo sy'n briodol:

- Union natur y wybodaeth, pa mor sensitif, cyfrinachol neu werthfawr ydyw
- Y niwed neu'r gofid y gellid ei achosi i unigolion petai'r wybodaeth yn cael ei cholli neu petai unigolion anawdurdodedig yn cael mynediad i'r wybodaeth
- Yr effaith y byddai unrhyw golled yn ei chael ar yr Ysgol
- I ba raddau mae angen darparu'r wybodaeth ar fyrder, gan gymryd i ystyriaeth effaith peidio ag anfon y data, neu unrhyw oedi o ran anfon y data

12.5 Os bernir ei bod yn briodol anfon gwybodaeth bersonol sensitif drwy'r Post Brenhinol, rhaid dilyn y camau canlynol:

- Rhaid i'r amlen yr anfonir y wybodaeth ynddi fod â chyfeiriad wedi'i nodi'n glir arni at dderbynnydd a enwir
- Rhaid anfon y wybodaeth drwy ddull y gellir ei olrhain

12.6 Pan ddefnyddir negesydd i gludo unrhyw wybodaeth bersonol, rhaid cymryd camau priodol i sicrhau bod y negesydd yn gweithredu o fewn safonau diogeledd priodol.

12.7 Os bernir nad yw'n briodol trosglwyddo gwybodaeth bersonol drwy'r Post Brenhinol neu negesydd ac os na ellir defnyddio dull electronig diogel, dylid darparu'r wybodaeth â llaw i'r derbynnydd, neu dylid trefnu i'r data gael ei gasglu a chadw cofnod sy'n cynnwys:

- Disgrifiad byr o'r wybodaeth a ddarparwyd
- Pryd y cafodd y wybodaeth ei darparu
- Enw a manylion cyswllt y derbynnydd, ac os yw'n berthnasol, ei swydd

12.8 Lle bo'n briodol, dylai cofnodion papur sy'n cynnwys data personol fod â dyfrnod sy'n nodi “Disclosed Copy/Copi wedi'i ryddhau". Gallai hyn gynnwys achosion lle mae cofnodion disgyblion yn cael eu rhyddhau i rieni.

13. Gwirio gwybodaeth cyn ei hanfon

13.1 Pan fydd data personol sensitif, neu wybodaeth bersonol a fyddai fel arall yn debygol o achosi niwed neu ofid os yw'n cael ei datgelu i drydydd parti, yn cael ei hanfon y tu allan i'r Ysgol mewn unrhyw fformat, dylai'r anfonwr ystyried cael rhywun arall i wirio'r wybodaeth cyn ei hanfon.

13.2 Mae'r unigolyn sy'n anfon y wybodaeth yn gyfrifol am y canlynol:

- Sicrhau bod y cyfeiriad e-bost neu bost yr anfonir y wybodaeth iddo yn gywir
- Sicrhau pan ddarperir gwybodaeth ar ffurf copi caled, bod y derbynnydd a enwir sy'n mynd i dderbyn y wybodaeth yn cael ei nodi'n glir
- Sicrhau nad oes dim gwybodaeth mewn perthynas â thrydydd parti wedi cael ei chynnwys mewn camgymeriad, naill ai mewn llythyr/neges e-bost neu ddogfen atodedig

13.3 Os bernir ei bod yn angenrheidiol i unigolyn arall wirio'r wybodaeth, mae'r unigolyn arall yn gyfrifol am y canlynol:

- Gwirio bod y cyfeiriad e-bost neu bost yr anfonir y wybodaeth iddo yn gywir
- Pan ddarperir gwybodaeth ar ffurf copi caled, gwirio bod enw cywir y derbynnydd a enwir sy'n mynd i dderbyn y wybodaeth wedi cael ei nodi
- Gwirio nad oes dim gwybodaeth mewn perthynas â thrydydd parti wedi cael ei chynnwys mewn camgymeriad, naill ai mewn llythyr/neges e-bost neu ddogfen atodedig
- Cofnodi eu bod wedi gwirio'r neges e-bost, y llythyr neu/a'r atodiadau

15. Cadw gwybodaeth bersonol

15.1 Pan nad oes angen cadw data personol ar ddyfeisiau cludadwy neu gyfryngau symudadwy bellach, dylid ei ddileu ar unwaith.

15.2 Os defnyddir dyfais gludadwy i gasglu gwybodaeth bersonol, ni ddylid cadw'r wybodaeth arni ond cyhyd ag sy'n gwbl angenrheidiol. Dylid cadw'r wybodaeth ar rwydwaith yr Ysgol cyn gynted ag y bo modd a'i dileu oddi ar y ddyfais.

15.3 Ym mhob achos arall, os penderfynir nad oes angen cadw gwybodaeth bersonol bellach, rhaid cyfeirio at y **Pecyn i Ysgolion gan y Gymdeithas Rheoli Cofnodion a Gwybodaeth** cyn dileu neu ddifetha cofnodion.

15.4 Rhaid cael gwared â chofnodion papur sy'n cynnwys gwybodaeth bersonol mewn modd diogel, drwy eu rhwygo'n fân neu drwy ddefnyddio'r gwasanaeth gwastraff cyfrinachol yn unol â **Gweithdrefn Gwaredu Cofnodion yr Ysgol.**

15.5 Gwasanaethau TG y Cyngor yn unig sydd â'r hawl i waredu offer TG a hynny'n unol â **Pholisi Diogeledd Gwybodaeth** y Cyngor.

16. Tor-diogeledd

16.1 Byddai'r rhain yn cynnwys achosion lle mae data personol, electronig neu ar bapur, yn cael ei golli neu ei ddwyn. Byddai'r enghreifftiau eraill yn cynnwys anfon data personol mewn neges e-bost at dderbynnydd nas bwriedir neu osod data personol ar wefan yr Ysgol yn ddamweiniol.

16.2 Rhaid rhoi gwybod ar unwaith am bob achos o dor-diogeledd i Swyddog Diogelu Data'r Ysgol.

16.3 Gall peidio â rhoi gwybod am dor-diogeledd, neu oedi cyn rhoi gwybod am hynny, olygu y bydd canlyniadau difrifol iawn i wrthrych y data, i'r staff, i unigolion eraill ac i'r Ysgol.

17. Sicrhau triniaeth gyfartal

17.1 Rhaid rhoi'r polisi hwn a'r gweithdrefnau hyn ar waith yn gyson, heb ystyried hil, lliw, cenedligrwydd, tarddiad ethnig neu genedlaethol, iaith, anabledd, crefydd neu gred, oedran, rhyw, hunaniaeth, rhywedd, cyfeiriadedd rhywiol, statws priodasol neu bartneriaeth sifil na chyfrifoldebau magu plant.

Os oes arnoch angen copi o'r ddogfen hon mewn fformat arall, cysylltwch â'r Pennaeth drwy ffonio 01558 822796.

Handling Personal Information

Policy & Procedure

Contents

1. Introduction

1.1 Cwrt Henri, Ffairfach and Talley Federation collects and uses a wide range of personal data about our pupils and staff in order to deliver education and pastoral care. If we fail to take adequate care of the personal data we deal with and it is lost, stolen, disclosed inappropriately or otherwise misused, this could have a serious impact on the individuals concerned ranging from distress to actual physical harm. Personal information is therefore a valuable asset, but also a liability if we handle it incorrectly.

1.2 This policy and procedure is therefore designed to ensure that personal information is handled securely, in particular its storage and transfer, to assist in complying with the School's legal obligations.

2. Definition of personal information

2.1 Personal information or data is any information that relates to a living individual, who can be identified from the information, directly or indirectly.

2.2 In practice, this is likely to include a very wide range of data, including, but not limited to:

- Names, addresses and dates of birth
- Reference numbers such as Unique Pupil Numbers
- Personal financial information such as bank details
- Descriptive or biographical information regarding an individual
- Photographs or other images

2.3 The terms personal information and personal data are used throughout this policy and procedure and have the same meaning.

2.4 There are also special categories of personal information and we must be particularly careful when dealing with these. The special categories are personal information regarding:

- Racial or ethnic origin
- Political Opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Genetic data
- Biometric data
- Health
- Sex life or sexual orientation

2.5 There are also specific requirements for information relating to criminal convictions and offences.

3. Legal background

3.1 Data Protection legislation sets out rules relating to the processing of personal data. Processing is defined as collecting, recording, storing and making any use of personal data, including its disclosure and disposal.

3.2 We are required to observe six principles relating to the processing of personal data. The sixth principle sets out a specific requirement that appropriate technical or organisational measures must be used to protect against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data.

3.3 The consequences of not handling personal data correctly could have serious consequences for the School, as administrative fines of up to €20,000,000 can be imposed for serious Data Protection breaches.

4. Policy statements

4.1 Cwrt Henri, Ffairfach and Talley Federation is committed to processing personal information in accordance with the requirements of Data Protection legislation.

4.2 The School views the proper handling of personal data as essential in delivering our services and maintaining the confidence of the people that we deal with.

4.3 Any personal data held by the School which is not in the public domain will always be treated as being strictly confidential.

4.4 The School will make maximum use of secure electronic methods to store and transfer personal data.

4.5 This policy is approved by, and has the full support of, the Governing Body of the School.

5. Scope

5.1 This policy and procedure applies to all personal data owned by the School.

5.2 This policy and procedure applies to all employees of the School, including:

- Temporary employees and agency workers
- Volunteers
- Contractors acting as data processors

6. Responsibilities

6.1 School employees are responsible for:

- Protecting the personal information they process by adhering in full to this policy and procedure.

6.2 Headteachers are responsible for:

- Ensuring that their employees are made aware of this policy and procedure and have understood its requirements
- Ensuring that the requirements of the policy and procedure are fully implemented within the School
- Ensuring that their employees have received appropriate training on Data Protection requirements
- Taking appropriate action when breaches of the policy and procedure occur

6.3 Breaches of this policy and procedure may lead to disciplinary action being taken against the employees responsible.

7. Use of portable devices, removable media and cloud storage

7.1 Portable devices include, but are not limited to:

- Laptop computers & tablets
- Smartphones

7.2 Removable media include, but are not limited to:

- USB memory sticks/storage devices
- SD cards
- CD-Roms and DVDs

7.3 Personal information must not be processed on removable media that are not owned by the School.

7.4 Personal information must not be processed on portable devices that are not owned by the School unless an appropriate control supplied by the School is in place.

7.5 Portable devices or removable media must only be used to collect, store, transport or transfer personal information when there is a genuine need to do so and there is no alternative method available.

7.6 Before using portable devices or removable media to collect, store, transport or transfer personal information, permission must be obtained from the Headteacher, Deputy Head or Head of Year.

7.7 Personal data must never be kept on portable devices or removable media unless it is encrypted.

7.8 Portable devices or removable media containing personal information must be stored and transported securely.

8. Secure storage of personal information

8.1 Paper records, portable devices and removable media containing personal information must be kept securely within School premises. This will involve keeping them in locked cupboards when not in use and ensuring that keys are not accessible to unauthorised persons. Adequate building security must be in use.

8.2 Storage of personal data in paper records should be minimised where possible.

8.3 Within School premises, personal data must not be left unattended where anyone can have access to it, such as on desks, window sills, corridors, printers and photocopying machines.

8.4 Personal information must not be processed on computer equipment that is not owned by the School.

8.4 Personal data processed on office based computers must be password protected and should never be left visible on a screen if the computer is unattended.

8.5 Personal information processed on computers must never be stored on the hard disk of the computer. This protects the data in the event of computer failure or theft.

8.6 Personal data must never be uploaded/stored in cloud storage not provided by the School. This includes, but is not limited to:

- Personal email accounts (such as Gmail, Hotmail)
- Dropbox
- Microsoft OneDrive

8.7 When personal information is displayed on computer screens used in a public area, it must not be visible to pupils or visitors to the School.

9. Taking personal information out of the School

9.1 Personal information must not be taken out of School premises unless it is absolutely necessary to do so and only with the permission of the relevant manager or the Headteacher, Deputy Head or Head of Year.

.

9.2 When paper records, portable devices or removable media containing personal information are taken out of office premises, they must be kept secure, carried safely and never be left unattended where they can be accessed by unauthorised persons such as within vehicles or in areas accessible to the public.

9.3 Paper records containing personal information must only be taken home with the permission of the Headteacher, Deputy Head or Head of Year, who is responsible for ensuring that a suitable working environment including a means of securely storing papers such as a lockable drawer or cabinet is available. A record should be kept of what information is taken off site, when it has been taken, by whom and when it is returned.

9.4 Paper records must not be kept in the home for longer than necessary and returned to the office premises at the earliest opportunity.

9.5 Family members, or any other unauthorised persons, must not be allowed access to any personal information, in any format, which is taken home.

10. Transferring personal information outside the School

10.1. This includes sending personal data to the following:

- The Welsh Government
- Other Schools
- Carmarthenshire County Council and other local authorities
- External agencies, companies and organisations
- Parents and pupils

10.2 Personal information must only be sent outside the School where this is in accordance with the law and it is absolutely necessary to do so.

10.3 Personal data must not be provided to any external organisation when anonymised or statistical information could be used as an alternative. Any personal information we do provide should be relevant and the minimum necessary for a specified purpose.

11. Using an electronic method to transfer information

11.1 The safest and quickest way of transferring personal information outside the School is a secure electronic method. This must always be considered as the first option and used whenever possible. Such methods could include, but are not limited to:

- The Common Transfer System/School2School
- Sending email using a secure email system such an Egress Switch
- Sending the information via a secure email network such as Zimbra, where the sender and recipient both have accounts
- Sending email via Zimbra to Carmarthenshire County Council email addresses

11.2 When using secure email, sending to groups or lists of contacts should be avoided as this introduces the risk of disclosing personal information to recipients who are not authorised to access it. The same care has to be taken when replying to emails, as choosing the 'reply to all' option may also result in the information being sent to unintended and unauthorised recipients.

11.3 When beginning to type an email address, several similar addresses that have been used previously will often be suggested by the email software. It is essential that the correct address is chosen before the message is sent.

11.4 Clear instructions must be included as to how the recipient is to handle the information, for example, if it is not to be passed on without first contacting the sender.

11.5 When a secure electronic method is not available and the information is not sensitive personal data, or otherwise likely to cause damage or distress if disclosed to a third party, then it can be sent by standard email without the need for any further assessment of risk. An example would be responding to an individual's correspondence about a prominent issue already in the public domain. Care must nonetheless be taken to ensure that the information is sent to the correct email address.

12. Using other methods to transfer personal data

12.1 Other methods of transferring personal data include but may not be limited to:

- Royal Mail
- Courier
- Hand delivery/collection

12.2 When a secure electronic method is not available and the information is not sensitive personal data, then it can be sent by Royal Mail without the need for any further assessment of risk. An example would be a letter informing a person that they have been successful in their job application. We also need to routinely send letters containing personal information to our customers, for example, in connection with benefit claims. Care must nonetheless be taken to ensure that the information is correctly addressed to a named recipient.

12.3 In the absence of a secure electronic method, when the information to be sent is sensitive personal information, then the following must always be considered when deciding what means of transfer is appropriate:

- The precise nature of the information, its sensitivity, confidentiality or value
- What damage or distress could be caused to individuals if the information was lost or accessed by unauthorised persons
- The effect any loss would have on the School
- The urgency of providing the information, taking into account the effect of not sending the data, or any delay in sending the data

12.5 If it is considered appropriate to send sensitive personal information by Royal Mail, the following steps must be taken:

- The envelope in which the information is sent must be clearly addressed to a named recipient
- The information must be sent by a traceable method

12.6 When using a courier to transport any personal information, steps must be taken to ensure that they operate within appropriate security standards.

12.7 When it is not deemed appropriate to transfer personal information by Royal Mail, or courier and a secure electronic method is not an option, the information should be provided by hand to the recipient, or an arrangement made for the data to be collected and a record kept which includes:

- A brief description of the information provided
- When it was provided
- The name and contact details of the recipient, and if relevant, their designation

12.8 Where it is considered necessary, records containing personal data should include a watermark stating "Disclosed Copy". This could include cases where pupil records are disclosed to parents.

13. Checking information before it is sent

13.1 When sensitive personal data, or personal information that is otherwise likely to cause damage or distress if disclosed to a third party, is being sent outside the School in any format, the sender should consider having the information checked by another person before it is sent.

13.2 The person sending the information is responsible for:

- Ensuring that the email or postal address the information is being sent to is correct
- Making sure that when information is supplied in hard copy, a named recipient of the information is clearly specified
- Ensuring that no information relating to third parties has been included in error, either in a letter/email or an attached document

13.3 If it is considered necessary for another person to check the information, the other person is responsible for:

- Checking that the email or postal address the information is being sent to is correct
- When information is being supplied in hard copy, checking that a correct named recipient of the information has been specified
- Checking that no information relating to third parties has been included in error, either in a letter/email or an attached document
- Recording that they have checked the email, letter and/or attachments

15. Retention of personal information

15.1 When it is no longer necessary to keep personal data on portable devices or removable media, it should be deleted immediately.

15.2 Where a portable device is used for the purpose of collecting personal information, the information should only be kept on it for as long as is absolutely necessary. The information should be saved on the School's network at the earliest opportunity and deleted off the device.

15.3 In all other cases, where it is decided that it is no longer necessary to retain personal information, the **Information & Records Management Society Toolkit for Schools** must be referred to before deleting or destroying records.

15.4 Paper records containing personal information must be disposed of securely, by shredding or the use of the confidential waste service in accordance with the **School's Records Disposal Procedure.**

15.5 Disposal of IT equipment must only be carried out by the Council's IT Services in accordance with the Council's **Information Security Policy.**

16. Breaches of security

16.1 These would include cases where personal data is lost or stolen, either in electronic or paper format. Other examples would include emailing personal data to an unintended recipient or accidentally placing personal data on the School's website.

16.2 All security breaches must be reported immediately to the School's Data Protection Officer.

16.3 Failure to report, or delay in reporting, security breaches can have potentially serious consequences for data subjects, staff, other individuals and the School.

17. Ensuring equality of treatment

17.1 This policy and procedure must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion or belief, age, sex, gender identity, sexual orientation, parental, marital or civil partnership status.

If you require this document in an alternative format, please contact the Headteacher on 01558 822796