POLISI DIOGELU DATA

Ym mhob un o bolisïau'r ysgol fe anelwn at gyflawni saith nod ac amcan craidd Agenda Gweithredu'r Hawliau ar gyfer Pobl Ifanc Cymru.

"DYRO DY LAW I MI AC FE AWN I BEN Y MYNYDD"

Drwy gydweithio ac ymddiried yn ein gilydd, rydym am sicrhau bod pob disgybl yn cyrraedd pen mynydd ei allu a'i dalentau. Gwnawn hynny drwy gynnig cyfle, cynhaliaeth ac arweiniad mewn cymdeithas bositif, eangfrydig, diogel a gwar.

Gweledigaeth ar gyfer ein disgyblion

Rydym am feithrin disgyblion sy'n rhugl yn y Gymraeg a'r Saesneg ac sy'n falch o draddodiad ac etifeddiaeth eu hardal a'u gwlad. Rydym am feithrin dinasyddion cytbwys a chyfrifol sy'n parchu hawliau unigolion eraill ac sy'n gyfforddus â'u hunain. Bydd ganddynt barch at eu meddyliau, eu hysbryd, a'u cyrff a bydd ganddynt orwelion eang a chwilfrydedd am wybodaeth newydd. Byddant yn meddu ar y sgiliau angenrheidiol i fanteisio ar her y dyfodol m myd gwaith ac mewn cymdeithas a byddant am barhau i dyfu a datblygu fel dysgwyr gydol oes a dinasyddion y byd.

Mynegai

1. Cyflwyniad

Mae'r polisi hwn yn nodi sut y bydd Cyngor Bro Morgannwg yn cydymffurfio â'i gyfrifoldebau o dan y Rheoliad Cyffredinol ar Ddiogelu Data a'r Ddeddf Diogelu Data sydd ar ddod, canllawiau presennol a deddfwriaeth diogelu data berthnasol arall. Mae'r polisi hwn yn ategu polisïau eraill y Cyngor mewn perthynas â rheoli gwybodaeth.

Mae angen i'r Cyngor gasglu a defnyddio mathau penodol o wybodaeth bersonol i weithredu'n effeithiol. Mae hyn yn cynnwys gwybodaeth am gyflogeion presennol, cyn-gyflogeion a darpar gyflogeion, ynghyd ag Aelodau, cyflenwyr, cleientiaid / cwsmeriaid, preswylwyr, tenantiaid, partneriaid presennol a blaenorol ac eraill y mae'r cyngor yn cyfathrebu â nhw. Rhaid i'r wybodaeth bersonol hon gael ei thrin yn briodol ni waeth sut y caiff ei chasglu, ei chofnodi na'i defnyddio – p'un a yw ar bapur, ar gyfrifiadur neu wedi'i chofnodi mewn ffordd wahanol.

2. Llywodraethu ac Atebolrwydd

Mae gan bob aelod o'r staff gyfrifoldeb am sicrhau y caiff Gwybodaeth y Cyngor ei chadw'n ddiogel fel y nodir yn y ddogfen ar gyfrifoldebau cyflogeion am ddiogelu gwybodaeth, y Cod Ymddygiad TGCh ac unrhyw ganllawiau ategol eraill a gyhoeddwyd.

Caiff hyfforddiant priodol gan gynnwys e-hyfforddiant ei ddarparu i bob aelod o'r staff sy'n prosesu data personol. Mae'n ofynnol i bob aelod o'r staff sy'n prosesu gwybodaeth bersonol fynychu hyfforddiant o'r fath.

Caiff cyfrifoldebau'r Prif Swyddog eu nodi yn Rheolau Gweithdrefn Ariannol y Cyngor yng Nghyfansoddiad y Cyngor.

Caiff y cyfrifoldeb o ddydd i ddydd am sicrhau y caiff y polisi hwn ei roi ar waith ei gyflawni o dan nawdd Bwrdd Mewnwelediad y Cyngor, a gaiff ei gefnogi gan y Bwrdd Llywodraethu yn ei dro.

Dirprwywyd y cyfrifoldeb cyffredinol am ddiogelu data i'r Rheolwr Gwybodaeth (Cyfreithiwr), a fydd yn gweithredu fel Swyddog Diogelu Data y Cyngor ac yn atebol i'r Uwch-swyddog Risg Gwybodaeth (SIRO), y Tîm Rheoli Corfforaethol a'r Cabinet.

Caiff cofnod o weithgareddau prosesu mewnol ei gynnal. Caiff polisïau a gweithdrefnau preifatrwydd clir, cynhwysfawr a thryloyw eu cynnal. Mae angen i bob aelod o'r staff fodloni'r gofynion, sydd ar gael i'r staff ar StaffNet.

3. Diffiniadau

Mae dau fath o ddata personol,

'Data Personol' – unrhyw wybodaeth sy'n ymwneud â pherson adnabyddadwy y gellir ei adnabod yn uniongyrchol neu'n anuniongyrchol yn enwedig drwy gyfeirio at ddynodwr.

Mae'r diffiniad hwn yn berthnasol i amrywiaeth eang o ddynodwyr personol i gynnwys data personol megis enw, rhif adnabod, data am leoliad neu ddynodwr ar-lein, gan adlewyrchu newidiadau mewn technoleg a'r ffordd y mae sefydliadau'n casglu gwybodaeth am bobl.

'Data personol sensitif' – Mae Erthygl 9 o'r Rheoliad Cyffredinol ar Ddiogelu Data (GDPR) yn cyfeirio at ddata personol sensitif fel "categorïau arbennig o ddata personol". Mae data personol sy'n datgelu tarddiad hiliol neu ethnig, safbwyntiau gwleidyddol, credoau crefyddol neu athronyddol neu aelodaeth o undeb llafur a'r dull o brosesu data genetig, data biometrig er mwyn adnabod person naturiol, data yn ymwneud ag iechyd neu ddata yn ymwneud â bywyd rhywiol neu gyfeiriadedd rhywiol person naturiol.

4. Egwyddorion Diogelu Data

Mae'r Cyngor yn cydnabod bod trin gwybodaeth bersonol yn gyfreithlon ac yn briodol yn hanfodol er mwyn cyflawni ei amcanion yn effeithiol ac mae'n hollbwysig ar gyfer cynnal y berthynas a'r ffydd rhwng y Cyngor a'r cyhoedd y mae'n ei wasanaethu.

Mae'r egwyddorion diogelu data fel rhan o'r GDPR yn nodi prif gyfrifoldebau sefydliadau.

Mae Erthygl 5 o'r GDPR yn ei gwneud yn ofynnol i ddata personol:

a) gael eu prosesu'n gyfreithlon, yn deg ac mewn modd tryloyw mewn perthynas ag unigolion;

b) cael eu casglu at ddibenion penodol, pendant a dilys heb gael eu prosesu ymhellach mewn ffordd sy'n anghydnaws â'r dibenion hynny; ni chaiff prosesu pellach at ddibenion archifo er budd y cyhoedd, at ddibenion ymchwil wyddonol neu hanesyddol neu at ddibenion ystadegol ei ystyried yn anghydnaws â'r dibenion cychwynnol;

c) bod yn ddigonol, yn berthnasol ac yn gyfyngedig i'r hyn sy'n angenrheidiol mewn perthynas â'r dibenion y cânt eu prosesu'n unol â nhw;

d) bod yn gywir a, lle y bo'n berthnasol, cael eu cadw'n gyfredol; rhaid cymryd pob cam rhesymol i sicrhau y caiff data personol sy'n anghywir, gan ystyried y dibenion y cânt eu prosesu'n unol â nhw, eu dileu neu eu cywiro'n ddi-oedi;

e) cael eu cadw ar ffurf lle gellir adnabod testun yn dda am gyfnod nad yw'n hwy na'r hyn sy'n angenrheidiol ar gyfer y dibenion y caiff y data personol eu prosesu'n unol â nhw; gellir cadw data personol am gyfnodau hwy ar yr amod y cânt eu prosesu at ddibenion archifo er budd y cyhoedd, at ddibenion ymchwil wyddonol neu hanesyddol neu at ddibenion ystadegol yn unol â'r mesurau technegol a sefydliadol priodol sy'n ofynnol gan y GDPR er mwyn diogelu hawliau a rhyddid unigolion;

f) cael eu prosesu mewn ffordd sy'n sicrhau y caiff y data personol eu diogelu mewn modd priodol, gan gynnwys eu diogelu rhag dulliau prosesu anghyfreithlon neu heb awdurdod a rhag cael eu colli'n ddamweiniol, eu dinistrio neu eu difrodi, gan ddefnyddio mesurau technegol neu sefydliadol priodol.

Mae Erthygl 5(2) yn pennu'r gofynion canlynol:

Y rheolydd fydd yn gyfrifol am gydymffurfio â'r egwyddorion ac am ddangos y gydymffurfiaeth honno.

Bydd y Cyngor yn prosesu'r holl wybodaeth bersonol er mwyn helpu i sicrhau y caiff ei chyflawni'n effeithiol i wasanaethau yn unol ag amcanion, cyfrifoldebau a rhwymedigaethau'r Cyngor.

Caiff yr holl ddata personol eu prosesu yn unol â'r egwyddorion gan ddilyn y canllawiau diweddaraf a luniwyd gan Swyddfa'r Comisiynydd Gwybodaeth, Cymdeithas Llywodraeth Leol Cymru a chyrff perthnasol eraill ac yn unol ag arferion da cydnabyddedig.

5. Y Sail Gyfreithlon dros Brosesu

Dim ond pan fydd sail gyfreithlon dros brosesu gwybodaeth bersonol y gwneir hynny. Mae chwe sail gyfreithlon dros brosesu. Bydd y sail fwyaf priodol i'w defnyddio yn dibynnu ar eich diben a'ch cydberthynas â'r unigolyn.

Mae'r seiliau cyfreithlon dros brosesu wedi'u nodi yn Erthygl 6 o'r GDPR. Rhaid i o leiaf un o'r canlynol fod yn wir pan fyddwch yn prosesu data personol:

(a) Cydsyniad: mae'r unigolyn wedi rhoi cydsyniad clir i chi brosesu ei ddata personol at ddiben penodol.

(b) Contract: mae'r gwaith prosesu yn angenrheidiol ar gyfer contract sydd gennych ag unigolyn neu am ei fod wedi gofyn i chi gymryd camau penodol cyn ymrwymo i gontract.

(c) Rhwymedigaeth gyfreithiol: mae'r gwaith prosesu yn angenrheidiol er mwyn i chi gydymffurfio â'r gyfraith (ac eithrio rhwymedigaethau contractiol).

(d) Buddiannau hanfodol: mae'r gwaith prosesu yn angenrheidiol er mwyn diogelu bywyd rhywun.

(d) Tasg gyhoeddus: mae'r gwaith prosesu yn angenrheidiol er mwyn i chi gyflawni tasg er budd y cyhoedd neu ar gyfer eich swyddogaethau swyddogol, ac mae gan y dasg neu'r swyddogaeth sail glir yn y gyfraith.

Er mwyn prosesu data personol sensitif yn gyfreithlon, rhaid i chi nodi sail gyfreithlon o dan Erthygl 6 ac amod ar wahân ar gyfer prosesu data categori arbennig o dan Erthygl 9. Nid oes rhaid i'r rhain fod yn gysylltiedig â'i gilydd.

Mae'r ddogfen hon yn gweithredu fel Dogfen Bolisi yn unol â pharagraff 30 yn Atodlen 1, Rhan 4 o'r Bil Diogelu Data. Caiff gweithdrefnau'r Rheolydd eu nodi mewn gweithdrefnau canllawiau a hyfforddiant perthnasol i'r staff yn unol â pharagraff (a). Mae Polisïau Cadw'r Rheolydd fel y'u nodir yn yr Amserlen Cadw, yn unol â pharagraff (b).

6. Hawliau Unigol

Mae'r Cyngor yn ystyried hawliau unigolion yn hollbwysig i'w ddinasyddion ac felly mae'n cymeradwyo'r penderfyniad i wella hawliau unigolion o ran data fel y nodir yn y ddeddfwriaeth. Caiff pob cais am wybodaeth bersonol ei drin yn unol â hawliau statudol yr unigolyn. Caiff ymholiadau am waith prosesu data personol y Cyngor eu trin yn brydlon ac mewn ffordd gwrtais.

Mae'r GDPR yn darparu'r hawliau canlynol i unigolion:

1. Yr hawl i gael gwybodaeth

2. Yr hawl i fynediad

3. Yr hawl i gywiro

4. Yr hawl i ddileu

5. Yr hawl i gyfyngu ar brosesu

6. Yr hawl i gludadwyedd data

7. Yr hawl i wrthod

8. Hawliau mewn perthynas â phenderfyniadau awtomataidd a phroffilio.

Hawliau Plant

Mae'r GDPR yn cynnwys darpariaethau newydd sydd â'r nod o ddiogelu data personol plant yn well. Os bydd plentyn yn cael cynnig gwasanaethau yn uniongyrchol, rhaid i sefydliadau sicrhau bod yr hysbysiad preifatrwydd wedi'i ysgrifennu mewn ffordd glir sy'n ddealladwy i blentyn.

7. Hysbysiadau Preifatrwydd

Oni bai bod eithriad priodol yn gymwys, bydd y Cyngor yn hysbysu unigolion ar adeg casglu eu gwybodaeth bersonol am y diben neu'r dibenion penodol y caiff y wybodaeth ei defnyddio. Er mwyn sicrhau y caiff y wybodaeth sy'n ofynnol yn ôl Erthygl 13 ei chyfathrebu â'r unigolyn, bydd y Cyngor yn defnyddio dull haenog ar gyfer Hysbysiadau Preifatrwydd.

8. Yr Hawl i Gywiro a Dileu

Mae'r GDPR yn rhoi'r hawl i unigolion ofyn am i'w data personol gael eu cywiro os ydynt yn anghywir neu'n anghyflawn. Bydd y Cyngor yn ei gwneud yn hawdd i unigolion gael gafael ar eu gwybodaeth bersonol a'i chywiro. Y terfyn amser statudol ar gyfer ymdrin â chais i gywiro data yw mis. Gellir ymestyn y cyfnod hwn i ddeufis os yw'r cais i gywiro yn gymhleth.

Caiff yr hawl i ddileu data ei chydnabod fel "yr hawl i gael eich anghofio" ac mae'n galluogi unigolyn i ofyn am i'w ddata personol gael eu dileu neu eu hepgor os nad oes rheswm cymhellol dros barhau i'w prosesu. Mae rhai amgylchiadau penodol lle nad yw'r hawl i ddileu data yn gymwys.

9. Rheoli Cofnodion

Caiff gwybodaeth bersonol ei chadw am y cyfnod a nodir yn amserlen cadw'r Cyngor. Bydd disgwyl i bob aelod o'r staff gydymffurfio â Chod Ymddygiad yr Arglwydd Ganghellor ar gyfer Rheoli Cofnodion.

10. Diogelwch

Mae'r GDPR yn ei gwneud yn ofynnol i ddata personol gael eu prosesu mewn ffordd sy'n sicrhau eu bod yn ddiogel. Mae hyn yn cynnwys eu diogelu rhag dulliau prosesu anghyfreithlon neu heb awdurdod a rhag cael eu colli'n ddamweiniol, eu dinistrio neu eu difrodi.

Caiff mesurau technegol a sefydliadol priodol eu cymryd er mwyn sicrhau diogelwch data o'r fath, gan gynnwys:

Anonymeiddio ac amgryptio data personol;

Y gallu i sicrhau cyfrinachedd, uniondeb, argaeledd a gwydnwch parhaus systemau a gwasanaethau prosesu;

Y gallu i adfer argaeledd a mynediad at ddata personol mewn modd amserol yn achos damwain ffisegol neu dechnegol;

Profi, asesu a gwerthuso effeithiolrwydd mesurau technegol a sefydliadol yn rheolaidd er mwyn sicrhau diogelwch y prosesu.

Bydd pob aelod o'r staff (gan gynnwys staff asiantaeth) sy'n prosesu gwybodaeth bersonol ar ran y Cyngor yn cael yr hyfforddiant priodol.

Caiff mynediad at wybodaeth bersonol ei reoli'n gaeth gan ddefnyddio cyfrinair a chyfleusterau amgryptio. Bydd mynediad i systemau yn gyfyngedig i'r defnyddwyr hynny sydd ei angen i gyflawni eu dyletswyddau a chaiff hawliau mynediad eu hadolygu'n rheolaidd. Caiff mesurau diogelwch eu rhoi ar waith er mwyn sicrhau na chaiff gwybodaeth bersonol ei chyhoeddi'n eang yn awtomatig.

Mae'r Cyngor wedi datblygu cyfres gynhwysfawr o weithdrefnau a chanllawiau i gydymffurfio â'r gofyniad hwn. Mae'n ofynnol i bob aelod o'r staff gydymffurfio â'r darpariaethau hynny.

11. Contractau/Rhannu Data

Pan fydd trydydd partïon yn trin data ar ran y Cyngor megis contractwyr, asiantaethau, partneriaid, ymgynghorwyr ac ati, bydd cytundeb ysgrifenedig rhwng y Cyngor a'r trydydd parti yn cadarnhau bod ganddo fesurau diogelwch technegol a sefydliadol priodol ar waith i ddiogelu'r data personol a dim ond cyfarwyddiadau'r Cyngor y bydd trydydd partïon o'r fath yn eu dilyn. Bydd y Cyngor yn cydymffurfio â'r gofynion ar gyfer prosesu gan ddata trydydd partïon fel y'u nodir yn Erthygl 28 o'r GDPR. Dim ond contractwyr a all roi "gwarantau digonol" y caiff gofynion y GDPR eu bodloni ac y caiff hawliau unigolion eu diogelu y dylai'r Cyngor eu penodi.

Mae'r Cyngor wedi llofnodi Cytundeb Rhannu Gwybodaeth Bersonol Cymru a bydd yn sicrhau y caiff yr holl ddata personol eu rhannu yn unol â'r cytundeb hwnnw.

12. Asesiad o'r Effaith ar Ddiogelu Data (DPIA)

Gall asesiadau o'r effaith ar ddiogelu data helpu i nodi'r ffordd fwyaf effeithiol o gydymffurfio â rhwymedigaethau ar ddiogelu data a chyflawni disgwyliadau unigolion o ran preifatrwydd. Bydd DPIA effeithiol yn eich galluogi i nodi a datrys problemau yn gynnar, gan leihau'r costau cysylltiedig a'r niwed i enw da a allai ddigwydd fel arall.

Rhaid i swyddogion gynnal DPIA yn yr achosion canlynol:

• wrth ddefnyddio technolegau newydd;

• pan fydd y gwaith prosesu yn debygol o arwain at risg uchel i hawliau a rhyddid unigolion.

Cysylltwch â'r Swyddog Diogelu Data am gymorth os bydd angen i chi gynnal DPIA.

13. Achosion o Dor Diogelwch Data

Mae'r GDPR yn gosod dyletswydd ar bob sefydliad i roi gwybod i Swyddfa'r Comisiynydd Gwybodaeth am achosion penodol o dor diogelwch data.

Mae achos o dor diogelwch data personol yn achos o dor diogelwch sy'n arwain at ddinistrio data personol, eu colli, eu newid, eu datgelu heb awdurdod neu fynediad diawdurdod atynt. Mae hyn yn golygu bod achos o dor diogelwch yn golygu mwy na cholli data personol, er enghraifft mae mynediad diawdurdod hefyd yn achos o dor diogelwch.

Mewn achos o dor diogelwch data personol, anfonwch e-bost i DPO@valeofglamogan.gov.uk

Mae gan y Cyngor 72 awr o'r adeg pan gaiff wybod am yr achos i roi gwybod i Swyddfa'r Comisiynydd Gwybodaeth amdano.

Mae rhagor o wybodaeth am roi gwybod am achosion o dor diogelwch data, gan gynnwys y ffurflen ar gyfer rhoi gwybod amdanynt a manylion cyswllt, ar gael ar StaffNet.

14. Statws Cydymffurfio

Mae cydymffurfio â'r polisi hwn a'r canllawiau i reolwyr yn orfodol. Os bydd cyflogeion y Cyngor yn mynd yn groes i'r polisi hwn, caiff ei ystyried yn achos o gamymddwyn difrifol a gall arwain at derfynu cyflogaeth.

DATA PROTECTION POLICY

In all school policies we aim to complete the seven core aims and objectives of the Rights to Action Agenda for the Young People of Wales.

"PUT YOUR HAND IN MINE AND WE WILL GO TO THE MOUNTAIN TOP"

By co-operating and trusting in each other we aim to ensure that each pupil reaches the summit of their ability and talents. We shall do so by offering opportunity, support and guidance within a positive, broadminded, safe and civilized society.

Vision for our pupils

We seek pupils who are fluent in Welsh and English and who are proud of the traditions and inheritance of their locality and their country. We seek balanced and responsible citizens who respect the rights of other individuals and who are comfortable with themselves. They will have a respect for their minds, their souls and their bodies and they will have wide horizons and a curiosity for new information. They will have the necessary skills to take advantage of the challenge of the future work place and society and they will wish to continue to grow and develop as lifelong learners and world citizens.

Index

1. Introduction

This policy outlines how the Vale of Glamorgan Council will comply with its responsibilities under the General Data Protection Regulations and the forthcoming Data Protection Act, current guidance and other related data protection legislation. This policy is supplemental to other Council policies in respect of information management.

The Council needs to collect and use certain types of personal information to operate effectively. This includes information on current, past and prospective employees, Members, suppliers, clients / customers, residents, tenants, partners and others with whom it communicates. This personal information must be dealt with properly no matter how it is collected, recorded and used – whether on paper, by computer or recorded on other material.

2. Governance and Accountability

All staff have responsibilities for ensuring the security and safekeeping of the Council's Information as set out in the Employees' Information Security Responsibilities Document, the ICT Code of Conduct and any other supplemental guidance issued.

Appropriate training including E-training will be provided to all staff processing personal data. All staff processing personal information are required to attend such training.

Chief Officer responsibilities are set out within the Council's Financial Procedure Rules, contained in the Council's Constitution.

Day to day responsibility for ensuring the implementation of this policy will operate under the auspices of the Council's Insight Board, which in turn will be supported by the Governance Board.

Overall responsibility for data protection has been delegated to the Information Manager (Lawyer) who will be the Council's Data Protection Officer and report to the Senior Information Risk Officer (SIRO), Corporate Management Team and Cabinet.

A record of internal processing activities will be maintained. Clear, comprehensive and transparent privacy policies and procedures will be maintained. All staff are required to adhere to the requirements, which are available to staff on the StaffNet.

3. Definitions

There are two classes of personal data,

'Personal Data' - any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier,

reflecting changes in technology and the way organisations collect information about people.

‘Sensitive personal data’ – Article 9 of the GDPR refers to sensitive personal data as “special categories of personal data”. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

4. Data Protection Principles

The Council regards the lawful and proper treatment of personal information as being fundamental to the effective delivery of its objectives and is key to the maintenance and confidence between the Council and the public it serves.

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Article 5(2) requires that:

The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

The Council will process all personal information to help support the effective delivery to services in accordance with the aims, responsibilities and obligations of the Council.

All personal data will be processed in accordance with the principles and by reference to the latest guidance produced by the Information Commissioner's Office, the Welsh Local Government Association and other relevant bodies, and in accordance with recognised good practice.

5. Lawful Basis for Processing

Personal information will only be processed where there is a lawful basis for doing so. There are six available lawful bases for processing. Which basis is most appropriate to use will depend on your purpose and relationship with the individual.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

In order to lawfully process sensitive personal data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.

This document acts as the Policy Document in compliance with paragraph 30 of Schedule 1, Part 4 of the Data Protection Bill. The Controller's procedures will be set out in relevant guidance procedures and training to staff, to comply with paragraph (a). The Controller's Retention Policies are as set out in the Retention Schedule to comply with paragraph (b).

6. Individual Rights

The Council regards individuals' rights as fundamental to its citizens and therefore endorses the enhancement of individual data rights as set out in the legislation. All requests for personal information will be dealt with in accordance with the individual's

statutory rights. Queries regarding the Council's processing of personal data will be dealt with promptly and courteously.

The GDPR provides the following rights for individuals:

1. The right to be informed

2. The right of access

3. The right to rectification

4. The right to erase

5. The right to restrict processing

6. The right to data portability

7. The right to object

8. Rights in relation to automated decision-making and profiling.

Children's Rights

The GDPR contains new provisions intended to enhance the protection of children's personal data. Where services are offered directly to a child, organisations must ensure that the privacy notice is written in a clear, plain way a child understands.

7. Privacy Notices

The Council will, at the point of collection, unless an appropriate exemption applies, inform individuals of the specific purpose or purposes for which the Council will use their personal information. To ensure the information required by Article 13 is communicated to the individual, the Council will use a layered approach for Privacy Notices.

8. Right to Rectification and Erasure

The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete. The Council will make it easy for individuals to access and correct their personal information. Where a request for rectification is received, the statutory time limit is one month. This can be extended by two months where the request for rectification is complex.

The right to erasure is also known as "the right to be forgotten" and enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. There are some specific circumstances where the right to erasure does not apply.

9. Records Management

Personal information will be held for the duration specified in the Council's retention schedule. All staff will be expected to comply with the Lord Chancellor's Code of Practice for Record Management.

10. Security

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Appropriate technical and organisational measures will be taken to ensure the security of such data and including:

The pseudonymisation and encryption of personal data;

The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

The regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

All staff (including agency staff) processing personal information on the Council's behalf will be appropriately trained.

Access to personal information will be strictly controlled through the use of password and encryption facilities. Access to systems will be restricted to those users that need it to undertake their duties, access rights will be reviewed on a regular basis. Security measures will be implemented to ensure that personal information is not automatically made widely available.

The Council has developed a comprehensive set of procedures and guidance to comply with this requirement. All members of staff are required to comply those provisions.

11. Contracts/Data Sharing

When third parties handle data on behalf of the Council such as contractors, agents, partners, consultants, etc. there will be a written agreement between the Council and the third party confirming that they have appropriate technical and organisational security measures in place to safeguard the personal data and such third parties will only act on the instructions of the Council. The Council will comply with the requirements for third party processing as set out in Article 28 of the GDPR. The Council must only appoint contractors who can provide "sufficient guarantees" that the requirements of the GDPR will be met and the rights of individuals are protected.

In sharing personal data the Council has signed the Wales Accord on Sharing of Personal Information all data sharing will comply with that Accord.

12. Data Protection Impact Assessment (DPIA)

Data protection impact assessments are a tool which can help identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow you to identify and fix problems

at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

Officers must carry out a DPIA when:

• using new technologies; and

• the processing is likely to result in a high risk to the rights and freedoms of individuals.

Please contact the Data Protection Officer for assistance if you require a DPIA.

13. Data Breaches

The GDPR introduces a duty on all organisations to report certain types of data breach to the Information Commissioner's Office.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data, for example, unauthorised access is also a breach.

If a personal data breach has occurred, please email DPO@valeofglamorgan.gov.uk

The Council has 72 hours from the time they become aware of it, to report the breach to the Information Commissioner's Office.

Further information on reporting data breaches, including the data breach reporting form and contact details can be found on the StaffNet.

14. Compliance Status

Compliance with this policy and the guidance for managers is mandatory. Breach of this policy by Council employees will be regarded as gross misconduct and may lead to termination of employment.