Neath Port Talbot County Borough Council

DATA PROTECTION POLICY

Version 2

May 2018

1. Neath Port Talbot County Borough Council [hereinafter referred to as "the Authority"] is committed to ensuring its compliance with the requirements of the General Data Protection Regulation 2016 ("GDPR") and the Data Protection Act 2018 ("DPA") ('the Legislation'). We recognise the importance of personal data to our organisation and the importance of respecting the privacy rights of individuals. This Data Protection Policy ('the Policy') sets out the principles which we will apply to our processing of personal data so that we not only safeguard one of our most valuable assets, but also process personal data in accordance with the law.

2. It is the responsibility of all our employees to assist the Authority to comply with this Policy. In order to help employees comply, we have produced a Data Protection Policy Guidance Note ('the Guidance') which explains in more detail the requirements of the Legislation. Employees must familiarise themselves with both this Policy and the Guidance and apply their provisions in relation to any processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal. Furthermore, serious breaches of the legislation could also result in personal criminal liability for the staff concerned.

3. In addition, a failure to comply with this Policy could expose the business to enforcement action by the Information Commissioner (which could result in restrictions being imposed on our use of personal data) or to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.

4. For the purpose of this policy:

Data	means information which – (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should

	form part of a relevant filing system, (d) is recorded information held by a public authority which falls outside (a) to (c) above
Data Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Data Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller
Data Subject	means an identified or identifiable natural person
Inaccurate Data	means information or data that is incorrect or misleading as to any matter of fact
Personal Data	means any information relating to an identified or identifiable natural person (data subject) An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as; • Collection

	• Recording • Organisation • Structuring • Storage • Adaptation or alteration • Retrieval • Consultation • Use • Disclosure • Restriction • Erasure • Destruction of personal data
Recipient	in relation to personal data, means any person to whom the data is disclosed whether a third party or not, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law
Special Categories of Personal Data	means personal data consisting of information as to - (a) the racial or ethnic origin of the data subject, (b) his/her political opinions, (c) his/her religious beliefs or philosophical beliefs, (d) whether he/she is a member of a trade union,

	(e) his/her physical or mental health, (f) his/her sexual life, or sexual orientation, (g) genetic data, or (h) biometric data (for the purposes of uniquely identifying a natural person)
Third Party	means any person other than – (a) the data subject, (b) the data controller, or (c) any data processor or other person authorised to process data for the data controller or processor
Criminal Convictions and Offences Personal Data	means the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of criminal proceedings or the sentence of any Court in such proceedings

Data Protection Principles

5. The Authority will comply with the following principles in respect of any personal data which it processes as a data controller. Personal data shall be:-

5.1 processed lawfully, fairly and in a transparent manner in relation to the data subject (Lawfulness, Fairness and Transparency);

5.2 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 (Purpose Limitation);

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

5.4 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 (Accuracy);

5.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for achieving 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 the data subject (Storage Limitation); and

5.6 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 (Integrity and Confidentiality)."

Basis of Processing

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

6.1 **Consent:** the individual has given clear consent for the Authority to process their personal data for one or more specific purposes.

6.2 **Contract:** the processing is necessary for the performance of a contract the Authority have with the individual, or because they have asked the Authority to take specific steps before entering into a contract.

6.3 **Legal obligation:** the processing is necessary for the Authority to comply with the law (not including contractual obligations).

6.4 **Vital interests:** the processing is necessary to protect someone's life.

6.5 **Public task:** the processing is necessary for the Authority to perform a task carried out in the public interest or in the exercise of official authority vested in the Council and the task or function has a clear basis in law.

6.6 **Legitimate interests:** the processing is necessary for the Authority's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This condition cannot be relied upon if the Authority is a public authority processing data to perform the Authority's official tasks.)

Accountability

7. The Authority must:

7.1 implement appropriate technical and organisational measures that ensure and demonstrate that we comply with both GDPR and the DPA. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;

7.2 maintain relevant documentation on processing activities;

7.3 appoint a data protection officer;

7.4 implement measures that meet the principles of data protection by design and data protection by default. Measures could include data minimisation, pseudonymisation or transparency;

7.5 allowing individuals to monitor processing;

7.6 create and improve security features on an ongoing basis, and

7.7 use data protection impact assessments where appropriate.

External Arrangements

8. The Authority must:

8.1 where the Authority passes personal data to any external organisation to process it on the Authority's behalf officers must ensure a Data Processing Agreement is in place. A suitable Data Processing Agreement can be obtained from the Legal Services Section;

8.2 in addition, any external contracts with our service providers/contractors must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the Authority. Specific terms must also be included and advice should be sought from the Legal Services Section in this regard;

8.3 where the Authority shares personal data it holds with third parties on a regular basis, it should endeavor to enter into a Data Sharing Agreement with those third parties (e.g. Welsh Government; Health Authority; Police and other Local Government Authorities).

Information Asset Register

9. One of the requirements of GDPR is to maintain a record of all the data processing activities that take place within the Authority. For this, we need to identify:

9.1 what personal data we process and why we process it;

9.2 what is the lawful basis for processing;

9.3 how we store and keep the data secure;

9.4 who has access to it;

9.5 who we share the data with and what sharing agreements are in place;

9.6 how long we keep it for.

10. The Authority has a dedicated Information Asset Register which must be completed for all information that is held within each of the Authority's Directorates. Officers should update this register whenever changes are made to the matters in 9.1 to 9.6 above.

Data Protection Officer

11. The Council has appointed the Head of Legal Services as the Data Protection Officer for this Authority.

12. The Data Protection Officer and his officers will work in conjunction with the ICT Section and all Directorates of the Council to ensure compliance with the Legislation

13. The role of the Data Protection Officer includes:

13.1 informing and advising officers of the Authority of their data protection obligations under GDPR and DPA;

13.2 monitoring compliance of policies and procedures. This includes monitoring responsibility and training of staff involved in data processing;

13.3 ensuring the Information Asset Register is an active registry that identifies all systems that hold personal data (i.e. it is kept up to date);

13.4 advising on the necessity of carrying out Data Protection Impact Assessments, the manner of their implementation and data breach reporting;

13.5 serve as contact point for individuals on privacy matters, including subject access requests;

13.6 to serve as the contact point for dealings with the Information Commissioners Office.

Additional Requirements

14. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

15. To view the Authority's policies in relation to Incident Reporting and Information Security please view the documents on the following link:

http://intranet.neath-porttalbot.gov.uk/default.aspx?page=9414

16. Personal data must not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. It is the responsibility of officers to ensure that if they are engaging processors to carry out work on behalf of the Authority that such processing is carried out in a European Union state: unless a specific exemption has been granted by the European Union to permit processing to be carried out in a county outside of the European Union.

17. This Policy may be amended from time to time to reflect any changes in legislation.