Bridgend County Borough Council

Data Protection Policy

Version:	Version 1
Date:	April 2018
Author/s:	Data Protection Officer
Consultee/s:	Corporate Management Board; Senior Information Risk Owner; Legal Services; Information Governance Board
Approved by:	Cabinet
Review frequency:	Every 2 years
Next review date:	April 2020

Data Protection Policy

1. Policy objective

1.1 Bridgend County Borough Council will at all times comply with its duties under the Data Protection Act 2017 and General Data Protection Regulation 2016 ((EU) 2016/679) and, in particular is committed to the observation, wherever possible, of the highest standard of conduct mandated by the legislation.

1.2 This policy describes Bridgend County Borough Council's approach to personal data.

2. Scope and definitions

2.1 This policy covers the Council's obligations under all legislation applicable in the UK covering data protection and privacy, and references the definitions in the General Data Protection Regulation 2016 (GDPR).

2.2 'Personal data' is defined as any information relating to an identified or identifiable person who can be directly or indirectly identified. Special categories of personal data are subject to additional protections, and include:

- Criminal allegations, proceedings, outcomes and sentences
- Physical or mental health or condition
- Politics
- Racial or ethnic origin
- Religion or other beliefs of a similar nature
- Sex life
- Sexual orientation
- Trade union membership
- Genetics
- Biometrics (where used for identification purposes)

2.3 The 'Data Controller' (the Council) determines the purposes and means of processing personal data. The GDPR places further obligations on the Council as data controller to ensure its contracts with processors comply with the GDPR.

2.4 A 'Data Processor' is any organisation responsible for processing data on behalf of the data controller. The GDPR places specific legal obligations on processors including the requirement to maintain records of personal data and processing activities. A processor will have legal liability if responsible for a breach.

2.5 'Processing' personal data means any activity involving personal information throughout the information lifecycle, from collecting and creating the personal information, to using it, making it available to others when necessary, storing it, and disposing of it when no longer required.

2.6 This policy applies to all employees, Elected Members, and other individuals/organisations acting on behalf of the Council who have access to personal data that the Council is responsible for. Detailed procedures accompany

this policy to direct the processing of personal information in a fair, lawful and transparent manner.

3. Data protection principles

3.1 Personal data of all stakeholders – current, former and prospective service users, employees, suppliers and others - will only be processed in compliance with laws on privacy and data protection, specifically adhering to the GDPR principles that personal information must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than necessary; and
- processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2 The Council will demonstrate accountability in adhering to the rights of individuals set out in data protection law, including their right:

- to be informed
- of access
- to rectification
- to erasure
- to restrict processing
- to data portability
- to object
- and rights in relation to automated decision making and profiling.

4. Accountability and monitoring

4.1 A statutory Data Protection Officer (DPO) is designated to oversee the management of personal data Council-wide, reporting to the Council's Senior Information Risk Owner (SIRO).

4.2 Heads of Service as Information Asset Owners adhere to the Council's data policies, supported by the Data Protection Officer.

4.3 Data Protection/Privacy Impact Assessments will be undertaken at an early stage whenever use of personal data is proposed and particularly during new projects.

4.4 A record of personal data processing activities is maintained by each Service Area and the DPO, and the way that the information is managed is regularly evaluated using Data Protection Impact Assessments where appropriate.

4.5 Clear and timely privacy notices are communicated that enable the subject of the data to understand how their personal data is being used.

4.6 Sharing of personal information is carried out in compliance with approved protocols, including the Wales Accord on Sharing Personal Information, Data Disclosure Agreements and Data Processing Agreements.

4.7 Disposal of personal information will be strictly in line with the Council's Data Retention Policy.

4.8 Everyone processing personal information understands their responsibilities and receives appropriate information to support them, including data protection training.

5 Complaints and data security incidents

5.1 The Council is dedicated to being compliant with the legislation. Any individual wishing to report concerns relating to data protection should contact the Data Protection Officer.

5.2 Failure to comply with the law on data protection may result in:

- Serious consequences for individuals that the data relates to, including embarrassment, distress, financial loss
- Irreparable damage to the Council's reputation and loss of confidence in the Council's ability to manage information properly
- Monetary penalties and compensation claims
- Enforcement action from the Information Commissioner
- Personal accountability for certain criminal offences and for breaching the Employee or the Elected Member Code of Conduct

6 Training

6.1 The Council has developed an online training policy in data protection. It is mandatory for Elected Members and all staff who process personal data.

7 Status of this policy / related policies and resources

7.1 This policy does not form part of the contract of employment for staff but it is a condition of employment that staff will abide by the rules and policies of the Council.

7.2 This policy should be read in conjunction with ICT policies and documents, the Code of Practice for Data Breaches and the Data Retention Policy.

7.3 Additional guidance and resources:

- For the public – please see the Council's website page on data protection

- For employees – the data protection pages on the intranet

8 The Information Commissioner

8.1 The Information Commissioner is the supervisory authority in the UK responsible for monitoring the application of the applied GDPR and Data Protection Act in order to protect the fundamental rights and freedoms of natural persons relating to processing. The Information Commissioner's Office (ICO) provides information and advice, and their website contains useful sources of best practice documents and practitioner guides: www.ico.org.uk.

8.2 The ICO are able to conduct an assessment or audit of the Council's processing of personal data in order to establish whether that processing follows good practice.

9 Further Information

9.1 Further Information is available from Data Protection Officer, Tel (01656) 643565, E-mail: Charlotte.Branford@bridgend.gov.uk.