Bridgend County Borough Council

Data Protection Policy

Date:	January 2021
Author/s:	Data Protection Officer
Consultee/s:	Corporate Management Board; Senior Information Risk Owner; Information Governance Board, Data Protection Officer
Approved by:	Cabinet
Review frequency:	Every 2 years
Next review date:	January 2022

Data Protection Policy

1. Policy objective

1.1 Bridgend County Borough Council holds Personal Data about its citizens, employees, suppliers, job applicants and other individuals for a variety of business purposes, including its public task as a local authority, its status as a major local employer and as a commissioner of services.

1.2 Compliance with the policy will assist the Council in meeting the requirements of the UK General Data Protection Regulation (GDPR) and the accompanying Data Protection Act. Failure to effectively implement this policy creates risks for the Council of non-compliance with legislation, substantial monetary penalties, distress or harm to individuals whose data we hold, reputational damage to the Council and detriment to the Council's ability to deliver effective and reliable services.

2. Scope and definitions

2.1 This policy applies to all staff and Elected Members who have access to Council records and information in whatever format in the course of their work.

2.2 'Personal Data' is defined as any information relating to an identified or identifiable natural person who can be directly or indirectly identified, eg. name, address, data of birth, location data, online identifier.

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' is a person or organisation who determines the purposes for which, and the manner in which, any Personal Data are, or are to be, Processed. For the purposes of this policy the Council is the registered Data Controller.

2.4 A 'Data Processor' is any third party that Processes the data on behalf of the Data Controller.

2.5 A 'Data Subject' is a living individual who is the subject of the Personal Data.

2.6 'Processing' 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.

2.7 A 'Privacy Notice' outlines information to data subjects about how and why their Personal Data is being Processed (including the identity of the Data Protection Officer, how and why the Council will use, Process, disclose, protect and retain that Personal Data). These are published on the Council's website and are provided to individuals when Personal Data is collected.

2.8 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 data in a manner that is compliant with the Data Protection Principles.

3. Data protection principles

3.1 The Council will ensure that all the Personal Data processing it undertakes accords with the following six principles:

- **Personal Data must be processed lawfully, fairly and in a transparent manner**

Processing of Personal Data must only be undertaken where the Council has a lawful basis for carrying out the activity. UK GDPR specifies six lawful bases for Processing as outlined at section 4.

Privacy Notices are in place for services which Process Personal Data including special categories of Personal Data. These notices make clear what data is being Processed and set out the lawful basis for Processing this Personal Data. These are published on the Council's website and are provided to individuals when Personal Data is collected.

- **Personal Data can only be collected for specified, explicit and legitimate purposes**

When gathering Personal Data the Council will ensure that Data Subjects receive appropriate Privacy Notices to inform them how their data will be used and identify the lawful basis for the Processing.

- **Personal Data must be adequate, relevant and not excessive**

The Council will ensure that data Processed is adequate, relevant and proportionate for the purpose for which it was obtained.

- **Personal Data must be accurate and, where necessary, kept up to date**

Individuals have the right to ask the Council to correct Personal Data relating to them which they consider to be inaccurate and such requests will be carefully considered by the Data Protection Officer (please see sections 7 and 8 for further information). If the Council does not agree that the Personal Data held is inaccurate then a record will still be kept recording the fact that it is disputed.

- **Personal Data must be kept for no longer than necessary**

The Council has a Data Retention Policy with standard retention periods where possible, in line with documentation obligations. The Council carefully considers how long it keeps Personal Data.

- **Personal Data must be processed in a manner that ensures appropriate security**

The Council must keep Personal Data secure against loss or misuse and has clear policies and procedures in place which require staff to keep Personal Data secure. Where the Council uses Data Processors on its behalf, additional security arrangements need to be implemented in Data Processing Agreements with those organisations to safeguard the security of Personal Data. The Council provides training and communication to staff which place an emphasis on data security.

3.2 There is a further overarching principle of accountability which means that the Council must not only comply with the six principles but must be seen to be complying with them in its public face and be able to demonstrate compliance if inspected by regulatory bodies. Further information is available at section 8.

4. Conditions for Processing

4.1 In order for it to be legal and appropriate for the Council to Process Personal Data, at least one of the following conditions outlined below must be met. No single basis is 'better' or more important than the others – which basis is most appropriate will depend on the purpose and relationship with the individual:

- The Data Subject has given consent
- Processing is required due to a contract
- Necessary due to a legal obligation
- Protect the vital interests of the Data Subject or another person
- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller
- It is necessary for the purposes of legitimate interests pursued by the controller or a third party (***this condition cannot be used by the public authorities in performance of their public tasks. It should be noted that under UK GDPR, the Council is classified as a public authority***)

4.2 There is a stronger legal protection for more sensitive information (known as "Special Category Data"), such as ethnic background, political opinions, health, religious beliefs, criminal records. Processing of Special Category Data will only be carried out by the Council if one of the following applies in addition to:

- Explicit consent of the Data Subject
- Necessary for obligations under employment, social security or social protection law or a collective agreement
- Protect the vital interests of the Data Subject or another person where the Data Subject is incapable of giving consent
- Processing carried out by a not-for-profit body and provided there is no disclosure to a third party without consent
- Personal Data made public by the Data Subject

- Necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Necessary for reasons of substantial public interest on the basis of Union or Member State law
- Necessary for reasons of public interest in the area of public health
- Necessary for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes
- Necessary for the purposes of preventative or occupational medicine

5. Supplementary Conditions for Processing

5.1 Section 10 and Schedule 1 of the Data Protection Act set out the exceptions from the prohibitions in the UK GDPR relating to Processing Special Category Personal Data and criminal convictions data.

5.2 The Council also processes Special Category Personal Data under the following conditions in Schedule 1, Part 2 of the DPA, on the grounds of substantial public interest:

- Statutory and government purposes
- Equality of opportunity or treatment
- Preventing or detecting unlawful acts
- Preventing fraud
- Counselling, advice or support services
- Safeguarding of children and of individuals at risk
- Insurance purposes
- Occupational pensions
- Elected representatives responding to requests
- Disclosure to elected representatives

5.3 Along with other conditions in Schedule 1, Part 3 of the Act the Council also extends the statutory and government purposes condition found in Part 2 to Process criminal convictions data. The Council must meet the substantial public interest test in order to Process this data. It is considered that in all the circumstances the public interest in the Processing of the criminal conviction data substantially outweighs the public interest in preserving the privacy of the Data Subject. This will be the case where the Processing is necessary and proportionate in order to protect the general public, children and vulnerable adults.

6. The Rights of an Individual

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

- to be informed about information held by the Council
- of access to their Personal Data that the Council holds via a Subject Access Request (as defined in the Act)
- to rectification of inaccurate data or incomplete data
- to erasure of their Personal Data in specific circumstances
- to restrict Processing in specific circumstances

- to data portability in specific circumstances
- to prevent Processing
- to object to decisions based solely on automated decision making and profiling
- make a complaint to the supervisory authority
- be notified of a Personal Data breach which is likely to cause damage or distress to the individual or anyone else
- to withdraw consent to Processing at any time (only where the legal basis for Processing is consent)

6.2 All of the above requests (whether made orally or in writing) should be escalated to the Data Protection Officer as soon as possible as there is a time limit for responding to these requests.

7. Complaints and data protection breaches

7.1 The Council will make every effort to avoid Personal Data breaches and in particular the loss of Personal Data. It is important that when a breach occurs the Council responds appropriately in accordance with the data protection laws. There is a requirement for the Council to notify relevant Personal Data breaches that will result in a risk to the rights and freedoms of individuals to the ICO when it becomes aware of the incident and to the individual Data Subjects in certain circumstances.

7.2 Any individual wishing to report concerns relating to data protection should contact the Data Protection Officer:

Charlotte Branford, Information and Data Protection Officer
Charlotte.branford@bridgend.gov.uk
Tel: 01656 643565

7.3 The Council will implement rules and procedures to ensure that it is able to respond to relevant data breaches within the 72 hour timeframe prescribed by legislation. The Data Protection Officer will carry out an assessment to determine whether the data subject should be informed of the breach/and or the Information Commissioner notified.

7.4 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

7.5 A Code of Practice for Data Breaches has been developed to assist the Council in responding effectively to Personal Data breaches.

8. Accountability and monitoring

8.1 The Council has a Data Protection Officer to oversee the management of Personal Data, Council-wide. The Data Protection Officer will work with the Senior Information Risk Owner and will ensure compliance with the Data Protection Principles. These positions will be supported by the Council's Information Governance Board comprising of a network of representatives from each Service within the Council. The existence of this Board in no way negates or reduces the individual accountability and responsibility of all staff and Elected Members for protecting the Personal Data to which they have access.

8.2 Data Protection Impact Assessments (a tool for identifying and assessing privacy risks throughout the development life cycle of a program or system containing Personal Data) will be undertaken at an early stage whenever use of Personal Data is proposed and particularly for new projects or the use of new technologies. In determining whether an assessment is necessary, officers will either decide this themselves, guided by internal screening mechanisms or they may consult the Data Protection Officer. They may be mandated by the Data Protection Officer to carry out the assessment.

8.3 As a Data Controller the Council is required to maintain a record of Processing activities which covers all the Processing of Personal Data carried out by the Council. A record of Personal Data Processing activities is maintained by each Service Area and the Data Protection Officer, and the way that the information is managed is regularly evaluated using Data Protection Impact Assessments where appropriate.

8.4 Clear and timely Privacy Notices are communicated that enable the Data Subject to understand how their Personal Data is being used.

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

8.6 Disposal of Personal Data will be strictly in line with the Council's Data Retention Policy.

3. Training and Responsibilities of Staff and Elected Members

9.1 All staff who have responsibilities for the collection, access or Processing of Personal Data should comply with the provisions of the applicable data protection laws in accordance with the Data Protection Principles.

9.2 All Elected Members are responsible and accountable for following established procedures and keeping their training and understanding up to date with regards to data protection.

9.3 The Council has developed an online training policy in data protection. It is mandatory for Elected Members and all staff who Process Personal Data.

10. Status of this policy / related policies and resources

10.1 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.

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

10.3 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

10.4 This policy is informed by the ICO's guidance on the implementation of UK GDPR which can be found on their website.

10.5 The Council will keep this policy under continuous review, amending it when necessary and formally reviewing it at intervals of not more than three years.

11. The Information Commissioner

11.1 The Information Commissioner is the supervisory authority in the UK responsible for monitoring the application of the UK 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.

11.2 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.