Data Protection Policy

Data Protection Policy

V1.0

Contents

V1.0

1. POLICY STATEMENT

1.1 Everyone has rights regarding how their personal information is handled. During the course of Bedlinog and Trelewis Community Council (BTCC) activities we will collect, store and process personal information about our Councillors and staff, and we recognise the need to treat it in an appropriate and lawful manner.

1.2 The types of information that we may be required to handle include details of current, past and prospective Councillors and employees, suppliers, customers, and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

1.3 This policy will apply to all Councillors and employees and of BTCC when processing personal data for and on behalf of BTCC. This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

2. STATUS OF THE POLICY

2.1 This policy has been approved by Council. It sets out BTCC rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 The registered Data Protection Compliance Officer is responsible for ensuring compliance with the Act and with this policy. That post is held by the Clerk to the Council. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Compliance Officer.

2.3 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the Clerk.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data Protection Act 1998 (DPA)** is the main UK legislation which governs the handling and protection of information relating to living people.

3.2 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.3 **Anonymised information** is information from which no individual can be identified.

3.4 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.5 **Personal data** means data relating to a living individual who can be identified from that data and other information in our possession or is likely to come into our possession. Personal data can be factual (such as a name, address, or date of birth) or it can be an opinion (such as a performance appraisal).

3.6 **Data controllers** are the people who or organisations which determine the purposes for which, and the way, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used within the Authority.

3.7 **Data users** include all employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies always.

3.8 **Data processors** include any person who processes personal data on behalf of BTCC. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

3.9 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.10 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

3.11 **Data sharing** relates to the disclosure of data from one or more organisations to a third-party organisation(s), or the sharing of data between different parts of an organisation. It can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one-off decisions to share data for any of a range of purposes.

3.12 **Data sharing agreements/protocols** set out a common set of rules to be adopted by the various organisations involved in a data sharing operation.

3.13 **Notification** relates to the Information Commissioner's Offices public register of data controllers. Each registry entry includes the name and address of the data controller and details about the types of personal data they process. Notification is the process by which a data controller's details are added to the register.

3.14 **Privacy impact assessment (PIA)** is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data.

4. DATA PROTECTION PRINCIPLES

BTCC Councillors and employees that process personal data must comply with the eight enforceable principles of good practice that are set out under Schedule 2 of the DPA. These provide that personal data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant, and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Kept secure.

(h) Not transferred to people or organisations situated in countries without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, in this case BTCC, the purpose for which

the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 For personal data to be processed lawfully, certain conditions must be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

6. PROCESSING FOR LIMITED PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

8. ACCURATE DATA

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate, and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, please see the Councils Corporate Records Retention and Disposal
Policy.

10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

(a) Request access to any data held about them by a data controller.

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended.

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. DATA SECURITY

11.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

11.2 The officer responsible for compliance with the DPA is the Data Protection Compliance Officer. The Legal Department is responsible for advising on compliance with the Act. The Clerk is responsible for ensuring that BTCC's notification to the Information Commissioner is current and fit for purpose, and for developing specific guidance notes and/or training on data protection for Councillors and employees of BTCC.

11.3 Any infringement of the Data Protection Act 1998 by Councillors or employees may expose BTCC and/or the individual to legal action, claims for substantial damages and fines from the Information Commissioner. Any infringement of the Act will be treated seriously by BTCC and may be considered under disciplinary procedures.

11.4 All alleged breaches of the data protection policy shall be notified to the Clerk in the first instance. Where there has been an unauthorised disclosure of personal data the Clerk shall advise on any remedial action.

11.5 All serious alleged breaches of the DPA must be referred to the Council, chaired by the Chair of BTCC, where it shall be considered whether the matter should be reported to the Information Commissioner.

11.6 The Act requires BTCC to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.7 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

12. COUNCILLORS AND EMPLOYEE'S OBLIGATIONS

12.1 Councillors and Employees shall only process personal data that is under the control of, or on behalf of, BTCC when there are lawful grounds to do so and where that Councillor and employee is so authorised by BTCC to process that personal data.

12.2 Unauthorised processing of personal data by Councillors and employees includes accessing personal data records for private interest and/or gain, even where access to the record system itself has been granted to the same member for business purposes. Unauthorised processing of personal data also includes disclosure of personal data (including verbal disclosures) to a third party where it is known that the third party is not entitled to receive that data.

12.3 Unauthorised processing of personal data is a potential disciplinary matter which will be considered under the relevant disciplinary procedures. Serious breaches of the Act may constitute a criminal offence.

12.4 Councillors and employees shall exercise personal responsibility in the secure handling of personal data and shall not knowingly or recklessly expose personal data to unauthorised access, disclosure or loss. Where Councillors and employees are unsure as to appropriate security measures they shall seek advice from the Clerk.

12.5 Where Councillors and employees are unsure as to any of the provisions of the Act or this policy they shall seek advice from the Clerk.

13. DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for information that we hold about them must be made in writing. A fee is payable by the data subject for provision of this information. Any Councillor or employee who receives a written request should forward it to the Clerk immediately. The Clerk is responsible for managing the response to subject access requests. All subject access requests must be conducted in accordance with the Information Commissioners Office guidelines.

BTCC shall take steps as appropriate to ensure that data subjects are aware of both their rights and obligations and BTCC's rights and obligations under the Act, and to make all Councillors and employees aware of the Act and the implications of processing personal data.

14. PROVIDING INFORMATION OVER THE TELEPHONE

Any member Councillor or employee dealing with telephone enquiries should be careful about disclosing any personal information held by us. They should:

(a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

(c) Refer the matter to the Clerk for assistance in difficult situations. No-one should be bullied into disclosing personal information.

15. PERSONAL DATA STORED IN COOKIES

15.1 Where the data contained in cookies can be linked to a name, a postal address or even an e-mail address, that information will amount to personal data and be subject to the DPA.

16. MONITORING AND REVIEW OF THE POLICY

16.1 This policy will be monitored by the Clerk. The policy is based on legislation and will be kept under review in accordance with legislative requirements and with reference to changes in legislation.

16.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.