Bridgend County Borough Council

Policy on Data Protection

Introduction

Bridgend County Borough Council will at all times comply with its duties under the Data Protection Act 1998 (the Act) and, in particular is committed to the observation, wherever possible, of the highest standard of conduct mandated by the Act.

All employees of the Authority must comply fully with this policy, the Act and other relevant legislation.

The Act establishes a framework of rights and duties which are designed to safeguard personal data and has two principal purposes:

- to provide certain rights to living individuals (known as data subjects) whose data is held by the Authority and
- to regulate the use by those (known as data controllers) who obtain, hold and process personal data on data subjects

Definitions

Appendix 1 sets out definitions in accordance with the Act.

Responsibilities under the Act

Bridgend County Borough Council is a data controller and has two main obligations under the Act:

- to notify the Information Commissioner that information about individuals is being collected, processed and held
- to follow the eight Data Protection Principles set out in the Act

Compliance with data protection legislation is the responsibility of all members of the Council who process personal data. Employees are expected to:

- abide by the Data Protection Principles
- acquaint themselves with, and understand this Policy
- understand what is meant by ‘personal data’ and ‘sensitive personal data’ and know how to handle such data
- contact the Information Officer (Legal Services) if in any doubt and not risk a contravention of the Act

The Monitoring Officer is authorised to act as the Senior Information Risk Owner on behalf of the Council and is responsible for coordinating the development and maintenance of information risk management policies, procedures and standards.

Data Protection Principles

This Council fully endorses and adheres to the Eight Principles, as detailed in the Act which specifically state that personal data must be processed in accordance with the Principles. These Principles are legally enforceable:

- Personal data shall be processed fairly and lawfully;
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Personal data shall be accurate and, where necessary, kept up to date;
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;
- Personal data shall be processed in accordance with the rights of the data subjects under this Act;
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- Personal data shall not be transferred to a country or territory outside the European Economic Area 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

Data Subject Rights

Data Subjects have the following rights under the Act:

- To be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of the data controller
- To make subject access requests regarding the nature of information held and to whom it has been disclosed. Any individual who wishes to exercise this right should apply in writing to the Authority's Information Officer (Legal Services). Any such request will normally be complied with within 40 calendar days of receipt of the written request
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To restrict automated decision making
- To sue for compensation if they suffer damage by any contravention of the Act
- To take action to rectify, block or erase or destroy inaccurate data

Wherever possible, personal data or sensitive personal data should not be obtained, held or disclosed unless the individual has given consent. If any member of staff is in any doubt about "consent", they should consult the Information Officer.

Disclosure of Personal Data

Employees are to be vigilant and exercise caution when asked to provide personal data held on another individual. In particular, they must ensure that personal data is not disclosed either orally or in writing to any other individual, family members, friends, government bodies and in certain circumstances the police, without the prior consent of the data subject. **This Policy determines that personal data may be legitimately disclosed where one of the following conditions apply:**

- The data subject has given their consent. If the information is sensitive personal data explicit consent may be needed
- Disclosure is permitted in accordance with the Act
- The disclosure is necessary for safeguarding national security
- The disclosure is necessary for the prevention or detection of crime, or the apprehension or prosecution of offenders
- The disclosure is necessary for the assessment or collection of any tax or duty or of any imposition of a similar nature
- The disclosure is necessary for the discharge of regulatory functions (including the health, safety and welfare of people at work)
- The data to be disclosed are to be used for research purposes
- The data are information which the Authority is obliged by legislation to provide to the public.
- The disclosure of the data is required by legislation, rule of law or the order of a court

Security of Data

All staff are responsible for ensuring that:

- personal data that they hold is kept securely using for example lockable cabinets, encrypted hardware etc
- computerised data is password protected and individual passwords are kept confidential
- personal data is not disclosed accidentally or otherwise to any unauthorised third party
- personal data should be accessible only to those who need to use it
- care is taken to ensure that appropriate security measures are in place for the deletion of personal data. Manual records should be shredded and disposed of securely and the hard drives of redundant PCs wiped clean
- personal data is only taken off-site when absolutely necessary and for the shortest possible time
- particular care is taken to ensure that laptops used to process personal data are kept secure at all times
- personal data is not transferred abroad without suitable safeguards

- the sharing of personal information with third parties is undertaken in accordance with the Wales Accord for Sharing Personal Information adopted by the Council

Information security breaches may cause real harm and distress to the individuals they affect and lives may even be put at risk.

If, despite security measures, a breach of security occurs (including 'near misses') it is important that staff report the breach to their line manager. All such breaches and near misses are recorded and monitored. The objective of doing so is to ensure that the matter is dealt with in accordance with the Council's Information Management Strategy.

Retaining Personal Data

The Act does not set out any specific minimum or maximum periods for retaining personal data. Instead it refers to the fifth data protection principle (see above). All staff will need to:

- A judgment must be made about the current and future value of the information
- Review the length of time you keep personal data
- Consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it
- Securely delete information that is no longer needed for this purpose
- Update, archive or securely delete information if it goes out of date

Status of this Policy

This Policy does not form part of the formal contract of employment for staff but it is a condition of employment that staff will abide by the rules and policies made by the Council from time to time.

All elected members must be made aware of the Policy and of their individual duties and responsibilities under the Act.

The Council has a number of policies and procedures related to data protection. These include the Code of Practice for Data Breaches and the Information Management Strategy.

Policy Review

This Policy will be reviewed from time to time in response to legislative changes and as part of the Council's mechanism for policy and procedural reviews.

Training

The Council has developed an online training module in data protection. All staff and elected members who process personal data **must** complete this short training module.

Complaints

The Authority is dedicated to being compliant with the Act. Any individual wishing to report concerns relating to the Act should contact the Authority's Complaints Officer:

Complaints Officer, Legal and Regulatory Services,
Bridgend County Borough Council, Civic Offices, Angel Street, Bridgend, CF31 4WB

Tel: 01656 643565

complaints@bridgend.gov.uk

The Information Commissioner's Office

The ICO is the UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. They provide information and advice, and their website contains useful sources of best practice documentations and practitioners guides: www.ico.gov.uk

The ICO maintains a public register of data controllers and this Council is registered as such. Under the Act, every data controller is required to notify and renew their notification on an annual basis. The Information Officer (Legal Services) will review the Data Protection Register annually prior to notification to the Information Commissioner.

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

Definitions

“Data”
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 (see definition below),

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

“Relevant filing system”
Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

“Personal Data”
Means data which relate to a living individual who can be identified
(a) from those data or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

****It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be “personal data”.***

“Sensitive Personal Data”
Personal data consisting of information as to
(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union,

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

“Inaccurate data”
For the purposes of the Act data are inaccurate if they are incorrect or misleading as to any matter of fact

“Data Controller”
A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

“Data Processor”

Any person (other than an employee of the data controller) who processes the data on behalf of the data controller

“Processing”
In relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including
(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data