Bridgend County Borough Council
Cyngor Bwrdeistref Sirol Pen-y-bont ar Ogwr
www.bridgend.gov.uk

BRIDGEND COUNTY BOROUGH COUNCIL

CYNGOR BWRDEISTREF SIROL PEN-Y-BONT AR OGWR

DATA PROTECTION POLICY

SCOPE

This policy will apply to all employees of Bridgend County Borough Council.

Adopted by the Governing Body

1. Introduction and Scope

1.1 Bridgend County Borough Council (*the Council*) is committed to a policy of protecting the rights and privacy of individuals in accordance with Data Protection legislation.

1.2 This policy is applicable to all employees and workers of the Council including staff employed by Governing Bodies in educational establishments and those with "visitor" status such as agency workers. Governing Bodies will be expected to have their own arrangements in place in support of this Policy.

1.3 Any breach of the Data Protection Act, Data Protection principles or this Policy is considered to be misconduct and may lead to action being taken under the Council's Disciplinary Procedure. Staff employed by Governing Bodies in educational establishments will be subject to the adopted Disciplinary Policy and Procedure governed by the terms and conditions of their employment.

2. Policy Statement

2.1 The Council needs to collect and use certain types of information about people in order to carry on its business and meet the needs of the communities it serves. This may include current, past and prospective employees, suppliers, clients and customers. In addition, it may occasionally be required by law to collect and use certain types of information to comply with the requirements of Government Departments in the conduct of local government business.

2.2 All personal information must be dealt with properly however it is collected, recorded and used; whether on paper, in a computer, or recorded on other material. A requirement of the Data Protection Act 1998 makes it mandatory to provide safeguards.

3. Data Protection Principles

3.1 The lawful and correct treatment of personal information by the Council is very important to successful operations, and to maintaining confidence between employees and those with whom the Council conducts its business.

3.2 The Council endorses and adheres to the Data Protection Principles, as detailed in the Data Protection Act 1998, which specifically states that personal information will be:-

i. processed fairly and lawfully and, in particular, shall not be processed

unless specific conditions are met;

ii. 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;

iii. adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;

iv. accurate and, where necessary, kept up to date;

v. processed in accordance with the rights of data subjects under the Act; and

vi. subject to appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction, or damage;

The Principles also state that personal information will not be:-

vii. kept for longer than is necessary for that purpose or purposes;

viii. 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.

4. **Security of Data**

4.1 The Council will, through appropriate management, and the strict application of criteria and controls:-

i. observe fully conditions regarding the fair collection and use of information;

ii. meet its legal obligations to specify the purposes for which information is used;

iii. collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;

iv. ensure the quality of information used;

v. apply strict checks to determine the length of time information is held;

vi. ensure that the rights of people about whom the information is held, are able to be fully exercised under the act. (These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information);

vii. take appropriate technical and organisational security measures to safeguard personal information; and

viii. ensure that personal information is not transferred abroad without suitable safeguards.

5. **Responsibilities**

The Data Protection Officer

5.1 The Council will designate a Data Protection Officer with specific responsibility for data protection. (Ellen Franks)

The Data Protection Co-ordinator or other Designated Officer

5.2 The Council's Data Protection Co-ordinator or other Designated Officer will work in close liaison with the Data Protection Officer in co-ordinating legislative changes and in providing advice and guidance to managers.

5.3 In addition, the Data Protection Co-ordinator or other Designated Officer will conduct regular reviews and audits of the way personal information is managed, and will regularly assess and evaluate the methods used in handling personal information.

All Employees

5.4 All employees are responsible for ensuring that any personal data held is kept securely and not disclosed to any unauthorised third party. All personal data should be accessible only to those who need to use it. Employees should form a judgement based upon the sensitivity and value of the information in question, and if in any doubt, should contact their line manager or the Council's Data Protection Co-ordinator for clarification.

5.5 Care should be taken to ensure electronic technology, particularly, computer terminals/screens are locked when unattended and that computer passwords are kept confidential. The Council's ICT Code of Practice should be adhered to at all times. Manual records should not be left where they can be accessed by unauthorised personnel.

5.6 Care must be taken to ensure the appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

5.7 All employees managing or handling personal information will be:-

i. contractually responsible for following good data protection practice; and

ii. appropriately trained and supervised to do so.

To facilitate the above, managers and team leaders will ensure:-

i. any employee wanting to make enquiries about handling personal

information knows who to go to for advice;

ii. queries about handling personal information are promptly and courteously dealt with;

iii. methods of handling personal information are clearly described.

6. **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.

APPENDIX 1

DEFINITION OF DATA PROTECTION TERMS

DATA

Data means information:-

- stored in a form capable of being processed by computer (such as word processed documents, spreadsheets and databases);
- recorded in any form for later processing (such as registration forms, CCTV pictures);
- stored as part of a 'relevant filing system'. This definition is very broad and covers such things as card indexes and microfiche files as well as traditional paper-based files. All personal data held in any form falls within the scope of the DPA 1998

PERSONAL DATA

Personal data are defined as data which relate to a living individual who can be identified:-

- from those data;
- from those data and other information in the possession of (or likely to come into the possession of) the Data Controller (*the Council*);
- and includes any expression of opinion about the individual and any indications of the intentions of the Data Controller (*the Council*) or any other person on behalf of the Council.

It is always safer to assume data is personal rather than not.

SENSITIVE PERSONAL DATA

The 1998 Act distinguishes between ordinary "personal data" such as name, address and telephone number and "sensitive personal data" which includes information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. Under the Act the processing of sensitive personal data is subject to much stricter conditions.

DATA SUBJECT

A Data Subject is any living person who is the subject of personal data.

DATA SUBJECT ACCESS

This is the right of an individual to see personal data relating to them which is held by a Data Controller (*the Council*).

The individual (data subject) must make the request in writing, supply information to prove who they are, and supply appropriate information to help the Council locate the information they require. A fee is payable. The Council must respond to requests within 40 days.

DATA CONTROLLER

A Data Controller is any person who makes decisions with regard to particular personal data, including decisions about the purposes for which the data is to be processed and the way in which that processing takes place. The Council is the Data Controller, but this role also covers any member of staff if they make decisions about personal data and its processing, on behalf of (and with the approval of) the Council.

DESIGNATED DATA PROTECTION OFFICER

The Data Protection Officer has been designated by the Council and holds specific responsibility for data protection. The Data Protection Co-ordinator works alongside the DPO and provides operational advice on data protection issues.

PROCESSING

Processing covers almost anything you can do with data, and includes acquiring, recording, consulting, retrieving, and making the data available to others.

THIRD PARTY DATA

Any individual/organisation other than the data subject, the data controller or its agents.

RELEVANT FILING SYSTEM *(as defined in the Data Protection Act 1998)*

Any paper or manual filing system which is structured so that information about an individual is readily accessible.

N.B. Personal data, as defined and covered by the Act, can be held in any format, electronic (including websites and e-mails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Signed Chair of Governors
16.03.16