Data Protection Policy

1. POLICY STATEMENT

1.1 Isle of Anglesey County Council is fully committed to compliance with the requirements of the Data Protection Act 1998 which came into force on 1 March 2000.

1.2 The Council will therefore follow procedures which aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the Council who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties under the Data Protection Act 1998.

1.3 Any breach of this policy will be taken seriously and may result in disciplinary action.

1.4 In order to operate efficiently, the Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition it may be required by law to collect and use information in order to comply with the requirements of central government.

1.5 This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

1.6 The Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those for whom it provides / arranges services and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly.

2. DEFINITION OF DATA PROTECTION TERMS

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

2.2 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.

2.3 Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as matters relating to the performance of a staff member).

2.4 Data controllers are the people, or organisations, which determine the purposes for which, and the manner in which, 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 in our business.

2.5 Data users include 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 at all times.

2.6 Data processors include any person who processes personal data on behalf of a data controller (other than an employee of the data controller). As noted above, the Council is the data controller and therefore employees of Council are excluded from this definition. Data Processors therefore could include suppliers which handle personal data on our behalf.

2.7 Processing is any activity that involves use of the data. It includes obtaining, recording or holding 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.

2.8 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. DATA PROTECTION PRINCIPLES

3.1 Anyone processing personal data must comply with the eight enforceable principles of good practice. 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) Secure.

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

4. FAIR AND LAWFUL PROCESSING

4.1 The Data Protection Act is not intended 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 or the data controller's representative, the purpose for which the data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred.

4.2 For personal data to be processed lawfully, certain conditions have to 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.

4.3 Data about staff may be processed for legal, personnel, administrative and management purposes and to enable the Council to meet its legal obligations as an employer, for example to pay staff, monitor their performance and to confer benefits in connection with their employment. Examples of when sensitive personal data of staff is likely to be processed are set out below:

(a) information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;

(b) the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;

(b) in order to comply with legal requirements and obligations to third parties.

4.4 The Council's Privacy Notice Statement and the Privacy Notice Template are attached at Appendix 1

5. PROCESSING FOR LIMITED PURPOSES

5.1 Personal data will 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 will 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 will be informed of the new purpose before any processing occurs.

6. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

6.1 Personal data will 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 will not be collected in the first place.

7. ACCURATE DATA

7.1 Personal data will be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps will 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 will be destroyed.

8. DATA RETENTION

8.1 Personal data will not be kept longer than is necessary for the purpose. For guidance on how long certain data needs to be kept before being destroyed, please consult the guidance issued by your Head of Service as applicable to your area of work.

9. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

9.1 Data will 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 unwarranted and / or substantial damage or distress to themselves or anyone else.

(e) Object to any decision that significantly affects them being taken solely by a computer or other automated process.

10. DATA SECURITY

10.1 We will 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.

10.2 The Act requires us 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 they

agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

10.3 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.

10.4 Security procedures include:

(a) Entry controls. Any stranger seen in entry-controlled areas should be reported.

(b) Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold protected or restricted information of any kind. (As a minimum, personal information is always considered protected)

(c) Methods of disposal. Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

(d) Equipment. Data users should ensure that individual monitors do not show protected information to passers-by and that they log off from their PC when it is left unattended.

11. SUBJECT ACCESS REQUESTS

11.1 A formal request from a data subject for information that we hold about them must be made in writing. A £10 fee is payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to their Line Manager and notify the Corporate Information Officer.

12. PROVIDING INFORMATION TO THIRD PARTIES

12.1 Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal information held by us. In particular they should:

(a) Require that the third party has or does put the request in writing with an explanation or reasoning as to their entitlement to receive the information.

(b) Check the identity of the person making the request and also verify that they are legally entitled to receive the information.

(c) Seek the advice of the Head of Service in the first instance and thereafter the Corporate Information Officer if further assistance required.

(d) Where providing information to a third party, do so in accordance with the eight data protection principles, as noted at 3.1.

13. IMPLEMENTATION

13.1 This policy takes effect immediately. All Heads of Service must ensure that staff are aware of this policy and its requirements. This should be undertaken as part of induction and supervision. If staff have any queries in relation to the policy, they should discuss this with their line manager in the first instance.

14. POLICY COMPLIANCE

14.1 This policy will be monitored through the Information Governance Group. Breach of this policy may be dealt with under the Council's Disciplinary Procedure

15. POLICY REVIEW

15.1 This policy will be reviewed and implemented by the Information Governance Group as it is deemed appropriate, but no less frequently than every 12 months.