Scarborough Borough Council
Data Protection Policy

This is a statement of the data protection policy adopted by Scarborough Borough Council.

Scarborough Borough Council needs to collect and use certain types of information about people with whom it deals in order to perform its functions. This information includes current, past and prospective employees, suppliers, clients, customers, service users and others with whom it communicates. Scarborough Borough Council is required by law to collect and use certain types of information to fulfil its statutory duties and also to comply with the requirements of the Government. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or on other material – and there are safeguards to ensure this in the Data Protection Act 1998.

Scarborough Borough Council regards the lawful and correct treatment of personal information as critical to successful operations and to maintaining confidence between those with whom we deal and ourselves. It is essential that it treats personal information lawfully and correctly.

To this end the Council fully endorses and adheres to the Principles of data protection as enumerated in the Data Protection Act 1998.

The Data Protection Principles are as follows:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;

2. 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;

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;

4. Personal data shall be accurate and, where necessary, kept up to date;

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;

6. Personal data shall be processed in accordance with the rights of data subjects under the Act;

7. 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;

8. 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.

Therefore, Scarborough Borough Council will, through appropriate management, and strict application of criteria and controls:

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

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

iii. Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or 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 information is held, can be fully exercised under the Act. (These include: 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 rectify, block or erase information which is regarded as wrong information);

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

viii. Ensure that any third party processors contracted by the Authority adhere to appropriate controls.

In addition Scarborough Borough Council will ensure that:

i. There are persons with specific responsibility for data protection in the organisation;

ii. Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;

iii. Everyone managing and handling personal information is appropriately trained to do so;

iv. Everyone managing and handling personal information is appropriately supervised;

v. Methods of handling personal information are clearly described;

vi. A regular review and audit will be made of the way personal information is managed;

vii. Documents and any storage media containing input to and output from systems (paper or electronic) detailing personal information will be held, transported and disposed of with due regard to its sensitivity. Confidential paper output no longer required will be shredded before it is included in the recycling process. The disposal of confidential waste may be arranged with firms who provide a certificated secure disposal service. Individual service areas will be responsible for ensuring appropriate arrangements are made. Where arrangements are made with external companies for paper data disposal, or other media holding personal data then checks must be made to ensure that the arrangements are secure and that disposal certificates are provided and recorded.

Responsibilities and Roles

In legal terms, the overall responsibility for the notification of the Council as a data controller and for ensuring compliance rests with the Chief Executive. However, the nominated officer for Data Protection within the Authority is the IT Manager.

It is NOT the responsibility of the Data Protection Officer to apply the provisions of the Act. This is the responsibility of the individual collectors, keepers and users of personal data. Therefore staff are required to be aware of the provisions of the Data Protection Act 1998, such as keeping records up to date and accurate, and its impact on the work they undertake on behalf of the Authority,

It is the responsibility of the Heads of Service that all computer and manual systems within their service areas that contain personal data must be identified and the Data Protection Officer informed for notification purposes.

Any breach of the Data Protection Policy, whether deliberate or through negligence, may lead to disciplinary action being taken or even a criminal prosecution.

Data Security

All employees are responsible for ensuring that:

Any personal data they hold, whether in electronic or paper format, is kept securely.

Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

Subject Access

An individual is entitled, on making a written request, to be supplied with a copy of all, with limited exceptions, information which forms the personal data held about them. A request for subject access must be responded to within 40 days. If it is not, the individual is entitled to complain to the Information Commissioner.

All data subject access requests must be referred to the Data Protection Officer, who will co-ordinate the processing of the requests.