Stockton-on-Tees
BOROUGH COUNCIL

Data Protection Policy

Version 1: June 2014

Stockton-on-Tees
BOROUGH COUNCIL

Contents

1.0 Introduction

1.1 This policy is designed to ensure that Stockton-on-Tees Borough Council ("the Council") complies with the Data Protection Act 1998 ("the Act"). The policy brings together existing policies and processes to provide an overarching, corporate approach to Data Protection.

1.2 The Council is a registered data controller. Its registration reference number is Z590889X. The registered details can be accessed at www.ico.org.uk

2.0 Policy Statement

2.1 The Council collects and uses information about people with whom it deals in order to perform its functions. This includes information about current, past and prospective employees, suppliers, clients, customers, service users and others with whom it communicates. The Council is also required by law to collect and use certain types of information to fulfil its statutory duties and to comply with the requirements of government departments. This personal information or data must be dealt with properly however it is collected, recorded and used, whether on paper, stored within a computer, or stored upon other media.

2.2 The Council will endeavour to apply the principles of the Act to **ALL PERSONAL DATA**, regardless of format, and will ensure that all council employees and elected members are aware of their responsibilities under the Act. The rights of individuals, including employees and members of the public, will also be recognised.

2.3 This policy covers all areas of the Council, except schools who are required to provide their own policy and procedures to ensure their full compliance with the requirements of the Act.

2.4 To this end the Council fully endorses and will adhere to the Principles of the Act.

3.0 The purpose of the Data Protection Act 1998

3.1 The Act covers the collection, storage, processing and distribution of personal data. It gives rights to individuals about whom information is recorded (data subjects). They may find out what information is held about them, challenge it if appropriate and claim compensation in certain circumstances.

3.2 The Act places obligations on those who record and use personal data (data controllers and data processors):

- They must be open about the use of personal data through notification (previously referred to as registration) to the Information Commissioner.
- They must be open with data subjects about the use of personal data through fair processing notices (explaining how the data controllers and data processors plan to use the personal data).
- They must follow sound and proper practices by applying the data protection principles.

4.0 The principles of the Data Protection Act 1998

4.1 The Act establishes eight principles, which 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.

4.2 Therefore, the 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. 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 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, 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 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 Council adhere to appropriate controls.

4.3 In addition, the Council will ensure that:-

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

ii. All subject access requests will, in the first instance, be referred to a Contact Officer in the relevant Service Grouping, who will take reasonable steps to ensure that the request is processed within that Service Grouping, unless the requested information is held exclusively by the Children, Education and Social Care service group or Council

Tax. These latter requests are to be directed, in the first instance, to the relevant Corporate Director, who will take reasonable steps to ensure that they are processed appropriately.

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

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

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

vi. Everyone managing and handling personal information is aware of and has reference to data sharing guarantee guidance provided by the Ministry of Justice;

vii. Methods of handling personal information are clearly described;

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

ix. 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 services 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.

Definition of Personal Data

4.4 Personal data is defined as data that relates to a living identifiable individual which is in the possession of, or which is likely to come into the possession of, the data controller. This 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

4.5 The Act also defines 'sensitive personal data'. Sensitive personal data is information about an individual's:

- Racial or ethnic origin;
- Political opinions;
- Religious beliefs (or beliefs of a similar nature);
- Membership of a trade union;
- Physical or mental health condition;
- Sexual life;
- Criminal offences, or criminal proceedings and convictions

4.6 The processing of sensitive personal data is more strictly controlled than for other types of personal information.

Individuals' Rights

4.7 The Act give rights to individuals in respect of personal data held about them by others. This applies to all individuals whether they are an employee, elected member or a member of the public. Each individual has the right to:

- Access personal data;
- Prevent processing likely to cause damage or distress
- Prevent processing for the purposes of direct marketing;
- Question automated decision-making processes;
- Take action for compensation if they suffer damage by any contravention of the Act by the data controller;
- Rectify, block, erase or destroy inaccurate data; and
- Make a request to the Information Commissioner for an assessment to be made of the data controller if they feel that the Act has been contravened.

Accessing Personal Data

4.8 Any individual wishing to access their personal data must put their request in writing to the Data Protection Officer and provide suitable proof of identification and pay a fee of £10 at the data controller's discretion.

4.9 The request will be dealt with within forty calendar days and the response will consist of a copy of the personal data, the purposes for which it is being processed and to whom it may be disclosed. Third party personal data will be redacted to protect that individual's data protection rights.

Security

4.10 The seventh principle of the Act refers to the security of personal data. The data controller must introduce measures that ensure a level of security appropriate to the nature of the data and the harm that might result from a breach of security, including loss of that data.

4.11 Reasonable steps must be taken to ensure the reliability of any employees who have access to personal data and that appropriate clauses in written contracts clearly state the employee's responsibilities under the Act when accessing and processing personal data.

5.0 The Council's responsibility

5.1 As a data controller, the Council will:-

- Ensure that all employees are aware of their responsibilities under the Act by providing them with a copy of this policy and relevant guidance notes and by ensuring that any personal data they deal with is relevant, processed fairly and handled in accordance with security guidelines specified by the Council.

- Provide awareness training to Council employees to ensure that they understand their responsibilities and that non-compliance could result in disciplinary action against them under the Council's Disciplinary Procedure.

- Provide secure information systems, both manual and computerised, so that all employees dealing with such data are required to take appropriate security measures.

- Ensure that the Council's notification with the Information Commissioner is kept up to date.

- Ensure that all Council partners understand their responsibilities and are made aware of the Council's Data Protection Policy and use it as

a benchmark for devising local arrangements governing personal data in their partnership.

6.0 Individual Responsibilities and Roles

6.1 The Act is "an Act to make provision for the regulation of the processing of information relating to individuals including the obtaining, holding, use or disclosure of such information. It places obligations on those who record and use personal data". The Authority will endeavour to apply the spirit of the Act to ALL data operations.

6.2 The overall responsibility for the notification of the Council as a data controller and for ensuring compliance with the Act rests with the Monitoring Officer in liaison with the Chief Executive.

6.3 All employees are instructed to provide for the attention of their Service Group Director, or Chief Officer, details of any proposal to create a system, paper or automated, which contains personal data, for approval and notification before implementation. Privacy impact assessments will be conducted prior to any implementation to ensure the uses of personal data do not contravene the Act.

6.4 An individual is entitled, on making a written request using the approved Data Subject Access Request Form (obtainable on request by telephoning 527060 or at http://www.stockton.gov.uk/documents/stocktoncouncil/832215/datasubjectaccessrequest.pdf), to be supplied by any data user with a copy of all the information, which forms the personal data held about him or her. A request for subject access must be responded to within 40 days. If it is not, the data subject is entitled to complain to the Information Commissioner at the following internet address www.ico.org.uk/concerns . Reasonable steps must be taken to ensure that the appropriate Officer or Officers within the relevant Service Group process all requests. If the request relates specifically to information held by Children, Education and Social Care or Council Tax, you must forward the request to the relevant Corporate Director, in the first instance.

6.5 All subject access requestors have the right to complain if they feel the information provided is incorrect, information has been provided outside of the specified time periods or they are dissatisfied with the service. The complaint should be presented in writing and forwarded to the complaints department at

Municipal Buildings, Church Road, Stockton-on-Tees, TS18 1LD or **Telephone** 01642 393939 **Fax** 01642 524800 email customer.comments@stockton.gov.uk

6.6 With regard to information requests from the Police, the Act permits the disclosure of personal information without consent, under Section 29 of the Act. Section 29 allows information to be disclosed when required for the:-

- Prevention or detection of crime
- Apprehension or prosecution of offenders

6.7 Under the above circumstances, client information can be disclosed to the Police without consent from the client.

6.8 All employees are advised that any wilful non-compliance with the data protection principles will be regarded as a serious disciplinary matter and may lead to dismissal.

6.9 This policy will form part of the Authority's Handbook of Personnel Policies and Procedures.

7.0 Monitoring and Review

7.1 This policy will be monitored and reviewed regularly to ensure that it remains up to date and relevant.