

ST JOSEPHS RC PRIMARY DATA PROTECTION POLICY

1. Introduction

1.1 The processing of personal data by Hartlepool Borough Council is essential to many of its services and functions. Compliance with the Data Protection Act 1998 (“the Act”) will ensure that this processing is carried out fairly and lawfully. The Act seeks to strike a balance between, on the one hand, the needs of the organisation to function effectively and efficiently and, on the other, respect for the rights and freedoms of the individual. Hartlepool Borough Council is committed to a policy of processing personal data within the law and ensure that information about individuals is collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Council’s policy statement is attached at Appendix I to this policy

2. Definitions under the Data Protection Act 1998

2.1 In order to have an understanding of this policy it is important that the key definitions in the Act are understood. A list of key definitions are attached at Appendix II

3. Policy Scope

The policy applies to data which is:-

- 3.1 Processed automatically by computer or other equipment capable of operating automatically in response to instructions or which is recorded with the intention of being so processed;
- 3.2 Is recorded in structured and unstructured manual files; and
- 3.3 Forms part of an “accessible record” which is widely defined as a health record, educational record or record held by certain public authorities relating to local authority housing and social services.

4. Who it Concerns

4.1 This policy applies to all staff and elected members of the Council. As a matter of good practice, other agencies, partnerships and individuals working with the Council, and who have access to personal data, will be expected to have read and complied with this policy. It is expected that departments/sections who deal with external agencies will take responsibility for ensuring that such agencies sign an undertaking to abide by this policy.

5. Data Protection Principles

All processing of personal data must be done in accordance with the eight data protection principles.

- 5.1 **Personal Data shall be processed fairly and lawfully**
Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.
- 5.2 **Personal Data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.**
The Council will inform individuals of the purpose(s) for which it processes their personal data and will seek their consent where this is appropriate or required by law. Where data is used for further purposes the individual will be informed of this.
- 5.3 **Personal Data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.**
Information, which is not strictly necessary for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.
- 5.4 **Personal Data shall be accurate and, where necessary, kept up to date.**
Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of the individuals to ensure that data held by the Council are accurate and up-to-date be updated accordingly. It is the responsibility of the Council to ensure that any notification regarding change of circumstances is noted and acted upon.
- 5.5 **Personal Data shall be kept only for as long as necessary.**
The Council will ensure that personal data is securely destroyed when it is no longer needed provided the retention periods required by law have been met.
- 5.6 **Personal Data shall be processed in accordance with the rights of data subjects under the Data Protection Act.**
The Council will respect the rights of individuals who are entitled:
- To ask the authority if it holds personal information about them
 - To ask what it uses the information for
 - To be given a copy of the information (excluding any information exempt from disclosure under the Act)
 - To be given details about the purposes for which the authority uses the information and of other organisations or persons to whom it is disclosed.
 - To ask for incorrect data to be corrected.
- 5.7 **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.**
The Council will maintain procedures and provide training designed to ensure this principle is upheld through the organisation.

5.8 **Personal data shall not be transferred to a country or a 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 must not be transferred outside of the European Economic Area (EEA) – the fifteen EU Member States together with Iceland, Liechtenstein and Norway – without the explicit consent of the individual.

The Council should be particularly aware of this when publishing Information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

6. **Security of Data**

6.1 All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party.

6.2 All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity of the information in question, but always consider keeping personal data:

- in a lockable room with controlled access, or
- in a locked drawer or filing cabinet, or
- if computerised, password protected, or
- kept on disks which are themselves kept securely

6.3 Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed unauthorised personnel.

6.4 Care must be taken to ensure that 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.

6.5 This policy also applies to staff who process personal data at home. Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing personal data at home or in other locations outside the Council.

7. **Rights of Access to Data**

7.1 Any individual who wishes to exercise this right should apply in writing to the Data Protection Officer. The Council reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee.

7.2 In order to respond efficiently to subject access requests the Council needs to have in place appropriate records management practices.

8. **Retention and Disposal of Data**

8.1 The Council discourages the retention of personal data for longer than they are required.

8.2 Departments should regularly review files in accordance with the Council's procedures on disposal and retention.

9. **Disposal of Records**

9.1 Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg shredding, disposal as confidential waste, secure electronic deletion).

10. **Disclosure of Data**

10.1 Personal data should only be disclosed to organisations or individuals specified in the Council's Notification to the Information Commissioner. The list of disclosures could include:

- Council staff
- Elected members
- Other organisations (e.g. other local authorities, health authority). This includes organisations with whom we share and jointly manage personal data.
- Parents and guardians
- Data processors and their staff

10.2 All disclosures should be covered by written documentation, which should include details of the information to be disclosed, the reasons for the disclosure and the need for the recipient to comply with the Data Protection Act in handling the data. The documentation could be in the form of a data sharing agreement, a formal contract or a covering letter.

10.3 There may also be some instances where an organisation asks for disclosure of personal data about a specific individual, for example, in relation to a criminal investigation. Such requests must be in writing, and must specify what information is sought, for what purpose, and the legal powers under which the request is made.

11. **Responsibilities**

11.1 The Council as a corporate body is the Data Controller under the Act.

11.2 **The Data Protection Officer**

11.3 The Data Protection Officer is responsible for day to day data protection matters and for developing specific guidance notes on data protection issues.

11.4 **Staff/Elected Members and third parties**

11.5 Compliance with data protection legislation is the responsibility of all staff, elected members of the Council and third parties with access to personal data held by the Council.

11.6 **The Corporate Management Group (CMG)**

11.7 The Corporate Management Group are responsible for approving and overseeing a corporate framework for the management of data protection issues

11.8 **Departmental Management Teams (DMT) are:**

11.8.1 Responsible for ensuring that any policies, procedures or protocols agreed by Corporate Management Group are implemented within the department/service;

11.8.2 Responsible for ensuring that appropriate employees are designated to assist with the implementation of this policy;

11.8.3 Responsible for ensuring that employees and elected members are supported in terms of training and development in adhering to this policy and procedures.

11.8.4 Responsible for ensuring that concerns are brought to the attention of Corporate Management Group at the earliest opportunity.

11.9 **Information Security Group**

11.10 A cross council group has been established to develop and implement appropriate policies and procedures for information security and as such will be an appropriate forum for reviewing this policy and related policies and procedures on data protection and freedom of information.

11.11 Responsible for agreeing method of training for employees and councillors

11.12 Report to respective DMTs and CMG on progress.

12. **Notification**

12.1 Hartlepool Borough Council must notify the information commissioner of all personal data being processed which is subject to the Act.

12.2 Notification is the responsibility of the Data Protection Officer. Details of the Council's Notification are published on the Information Commissioner's website www.informationcommissioner.gov.uk . Anyone who is, or intends, processing data for purposes not included in the Council's Notification should seek advice from the Data Protection Officer.

13. **Implementation**

13.1 The policy will be related to new employees as part of the induction process. Appropriate departmental representatives and line managers will inform existing employees. This policy will be published on the Councils Intranet and updated accordingly.

14. **Monitoring and Review**

14.1 This policy will be monitored by the Data Protection Officer in collaboration with the Departmental Data Protection Officers, and will be reviewed annually to ensure that it remains up to date and relevant.

15. **Appendices**

Appendix I – Policy Statement

Appendix II – Definitions under Data Protection Act

Appendix III – Relation Legislation, Standards and Policies

APPENDIX I: POLICY STATEMENT

Policy Statement

We will comply with all requirements of the Data Protection Act 1998.

We will keep individuals informed of the purposes for which we are processing personal data, and will seek their consent where possible and appropriate. Where data is used for another purpose, individuals will be informed of this. We will also provide general information to the public on their rights under data protection legislation.

We will hold the minimum personal data necessary to carry out the Council's functions and every effort will be made to ensure its accuracy. Data which is no longer required will be securely destroyed.

Processing will comply with the Council's Information Security Policies and will follow the Code of Practice contained in the standard ISO17779 (Information Security Management) where appropriate.

We aim to respond to all requests from individuals to access their personal data within the timescales set down in the Data Protection Act 1998. Requests must be in writing, provide proof of ID, provide adequate information to be able to locate the data requested and be accompanied by the statutory maximum fee of £10.

The Data Protection Act allows exemptions from subject access, providing information to Individuals and non disclosure of information, in specific and limited circumstances. We will normally only invoke an exemption where it is deemed necessary to the effective operation of the Council, for the prevention and detection of crime, to protect the individual, or is required by law.

Elected members and staff will be trained to an appropriate level in the use and control of personal data.

APPENDIX II: DEFINITIONS UNDER DATA PROTECTION ACT

Personal Data

Personal data includes any information relating to a living individual who can be identified from the data either alone or in combination with other information relating to that person. This can include not only personal details, details of family and social circumstances, education, employment, business and financial details, but also goods or services received, expressions of opinions or intentions, and images such as those recorded on CCTV.

Sensitive Personal Data

The Act gives this category of personal data additional safeguards in relation to its processing. Sensitive personal data consist of information relation to:-

- race or ethnic origin;
- political opinions;
- religious or similar beliefs;
- membership of trade unions;
- physical or mental health;
- sexual life;
- commission or alleged commission of any offence; or
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Processing of personal data

Processing is defined very widely in the Data Protection Act. The term processing includes obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data. It includes any of the following: organisation, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, alignment, combination, blocking, erasure or destruction. As such, most if not all operations involving personal data will be covered by the definition.

Data subject

A Data subject is any individual who is the subject of personal data. The definition excludes corporate entities, but will include individual employees and representatives of corporations.

Data Controller

A data controller is any person who determines the purposes for and the manner in which any personal data are or will be processed. Hartlepool Borough Council is a data controller holding data on its employees and members of the public.

APPENDIX III: RELATED LEGISLATION, STANDARDS AND POLICIES

Main Legislation

- i) Freedom of information Act 2000 (providing overarching right of access to all information held by a public authority).
- ii) Human Rights Act 1998 (brings much of European Convention on Human Rights into UK law).

Professional Standards

- i) BS4783 Storage, transportation and maintenance of media for use in data processing and information storage.
- ii) ISO 17799 Standard on Information Security Management.
- iii) ISO 15489 Standard on Best Practice in Records Management.
- iv) BSI DISC PD 0008:1999 Code of practice for legal admissibility and evidential weight of information stored electronically.
- v) BSI DISC PD 0010:1997 the principles of good practice for information management.
- vi) BSI DISC PD 0012: Guide to the practical implications of the Data Protection Act.

Internal Policy

- i) Best Value Performance Plan.
- ii) Freedom of Information Policy.
- iii) Information Security Policy.

Created September 2006

Reviewed Autumn 2008 MMH / AH