Data Protection Policy

Version Control

Date	Version	Reason	Owner	Author
06/08/2014	Version 8	Amendments after review	Lysanne Eddy	Indi Viknaraja

DATA PROTECTION

Status:	Final
Date:	August 2014
Review Date:	August 2016
Consultation:	SIRO Head of Legal Head of Support Services

Supporting Documents:

Data Protection Policy
Information Sharing Protocol
Principle 6 and Subject Access Request Procedures
Principle 7 – IT Security Policy
Data Security Breach Management Procedure
How to Process a Section 29 Request
Records Management Policy
Information Asset Register
Privacy Vs Data Sharing
Project Management Guidance

DATA PROTECTION

1 Introduction

1.1 The Data Protection Act (DPA) 1998 became law in March 2000. The primary aim of the Act is to give legal rights to data subjects in respect of personal data processed about them by data controllers. (**Appendix 1**)

1.2 Southend on Sea Borough Council (the 'Council') needs to collate and handle personal information about individuals, the community, past and present employees, contractors and other organisations to provide a quality service and administer the Council efficiently and effectively. The personal information must be dealt with properly, whether it is collected, recorded and processed on paper, electronically or recorded in other material. The DPA prescribes how the Council must look after that information.

2 Policy Statement

2.1 The lawful, fair and correct processing of personal information by the Council is very important to successful operations and to maintaining confidence.

2.2 To this end the Council fully endorses and adheres to the principles of data protection as detailed in the DPA.

2.3 The DPA consists of 8 enforceable principles of good information handling practice which data controllers are required to comply with.

3 The Eight Data Protection Principles are:

Personal data shall:

- be processed fairly and lawfully, and in particular, shall not be processed unless specific conditions are met;
- 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;
- be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- be accurate and, where necessary kept up to date;
- not be kept for longer than is necessary for that purpose or those purposes;
- be processed in line with the rights of the data subjects under the Act;
- 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;
- not be transferred to a country outside the European Economic Area, unless

that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

4 Compliance with the Principles

The Council will, through strict application of criteria and controls:

- Adhere fully to conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used; including specific requirements that must be met to ensure fair and lawful sharing of personal data both internally and externally in line with the Whole Essex Information Sharing Framework and the Information Sharing Protocol for Southend-on- Sea.
- Collate and process relevant personal information, and only to the extent that is needed to fulfil operational requirements or to comply with any legal or statutory obligation.
- Ensure the quality of information used.
- Apply stringent checks to determine the length of time information is held.
- Ensure that people are able to fully exercise their rights under the Act. These include having the right of access to their personal information, the right to be informed that processing is undertaken, the right to be able to correct, block, remove or destroy information which is inaccurate or contains expressions of opinion based on inaccurate information and in certain circumstances prevent processing or disclosure of information.
- Ensure that personal information is not transferred outside the European Economic Area without suitable and adequate protection.
- Ensure that the Council's Notification to the Information Commissioner's Office remains up to date and accurate.

5 Management of Data Protection

The Council will ensure that:

- there is someone with specific responsibility for data protection. Currently the nominated persons are the Head of Legal and Head of Customer Services. The Policy, Engagement & Communications Team in Corporate Services is corporately responsible for managing DP and to provide advice on aspects of this policy to data owners in the Council;
- there is a DP/FOI Co-ordinators Group in place. This team disseminates best practice across all Directorates and assists with the handling of all Subject Access Requests, in line with the DP/FOI Co-ordinators' Roles and Responsibilities Guidance;

- all staff who manage and handle personal information are responsible for adhering to good data protection practice;
- all staff managing and handling personal information are adequately and appropriately trained and supervised;
- all queries on handling personal information are dealt with promptly and courteously;
- methods and documentation for handling personal information are clear and readily available;
- methods of handling personal information are regularly assessed and evaluated;
- performance of handling personal information is regularly assessed and evaluated;
- the way personal information is managed is reviewed and audited regularly to test compliance with each Principle;
- Risk assessments should be undertaken to ensure compliance with the DPA.

6 Complaints and Breaches of Data Protection

The Council will take the following steps to enforce this Policy and deal with any notified Data Protection related complaints and/or breaches both via internal and external sources including:

- Managers to ensure that all staff are aware of DP in line with the terms and conditions of employment. The People & Policy Team in Corporate Services will advise and support managers in any disciplinary action that needs to be carried out. The Data Governance Advisor will ensure that appropriate training is available.
- All complaints and potential breaches of the DP legislation will be dealt with in accordance with the Council's Compliments, Comments and Complaint's and Breach Management Procedures.
- Complaints from data subjects, in relation to disclosures under Subject Access Requests will be dealt with by the Information Commissioner's Office (ICO), in line with Principle 6 of the DPA and led by the Data Governance Advisor.
- The Council's Policy, Engagement & Communications Team in Corporate Services will apply a fair and consistent approach to the recording and management of all data protection breaches, including notification of breaches to affected individuals (the data subjects). In each case, a risk assessment of the consequences of the breach, conducted in line with guidance from the ICO will be carried out in line with the existing investigation procedures.
- Separate procedures for notifying affected individuals of data security breaches (Principle 7) will be followed in line with the Council's security of information and encryption guidance and advice from the ICO.

- The Policy, Engagement & Communications Team will consult with People & Policy Team on each breach where a member of staff or department representative is found to be accountable for the breach of this policy. Responsibility may then transfer to the relevant manager to investigate, with support from People & Policy Team as appropriate, and action may be taken in line with the People & Policy Disciplinary policy.

7 Monitoring of this Policy

The Policy will be monitored by the Data Governance Advisor through routine reporting of performance and data breaches to Corporate Services DMT.

Appendix 1
Terms used in this document – Jargon Buster

Data	Information which is processed by means of equipment operating automatically in response to instructions given for that purpose/ or recorded with the intention that it should be processed/or is recorded as part of a 'relevant filing system' or with the intention that it should form part of a relevant filing system/it does not fall within the above but forms part of an 'accessible record'.
Data Controller	The person or organisation that decides the purposes for which, and the manner in which personal information is to be processed.
Data Subject	The person whose personal information is held by a Data Controller.
Data Subject's Consent	Means freely given, specific and information of his/her wishes by which the data subject signifies his/her agreement to personal data relating to him/her being processed.
Disclosure//Recipient	Other parties to whom the personal data can be disclosed
Information Commissioner	An independent office-holder appointed by the Crown (ie the Government) to administer and enforce the Data Protection Act, the Freedom of Information Act 2000 and other legislation governing the use of and access to Information. The Information Commissioner is independent of the government and reports directly to Parliament. www.ico.gov.uk
Notification	The process by which data controllers register their details on the statutory register maintained by the Information Commissioner. They must register the types of information they hold, and the purposes for which they hold it.
Processing	The processing of personal data includes obtaining, recording, holding or carrying out any operation on the data.
Relevant Filing System(manual records)	Means any set of information relating to individuals to the extent that although the information is not automatically processed, the set is structured, either by reference to individuals or by reference to criteria to individuals, in such a way that specific information relating to a particular individual is readily accessible.
Personal data	Data which relates 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 possession of the **Data Controller,** 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.
Sensitive Personal Data	Personal data about racial or ethnic origin, political opinions, religion, trade union membership, physical or mental health, sexual life, crime offences or proceedings. More stringent requirements apply to the disclosure of sensitive data.
Subject Access Request (SAR)	The right of data subjects to receive a copy of the information held about them, a description of why their information is being processed, and details of anyone who may see a copy of their data, to whom it may be transferred, and the logic involved in any automated decisions taken on the basis of that data. SARs must as far as possible be dealt with within 40 calendar days