



Data Protection Policy

Version Control

Date	Version	Owner	Author
October 2012	Draft 1	Beverley Gallacher	Beverley Gallacher
December	V2	Beverley Gallacher	Beverley Gallacher
November 2018	V3	Sarah Lander	Sarah Lander

DATA PROTECTION

To Be Approved by:	Senior Management Team
Status:	Final
Date:	2018
Review Date:	2021

Supporting Documents:

Data Protection and FOI coordinators – Roles and Responsibilities
Information Sharing Protocol
Southend Borough Council's SAR application form
SBC's Procedure for replying to Subject Access Requests
Corporate information – IT Security Policy
Document Retention Policy
SEH Privacy Notice

DATA PROTECTION

1. Introduction

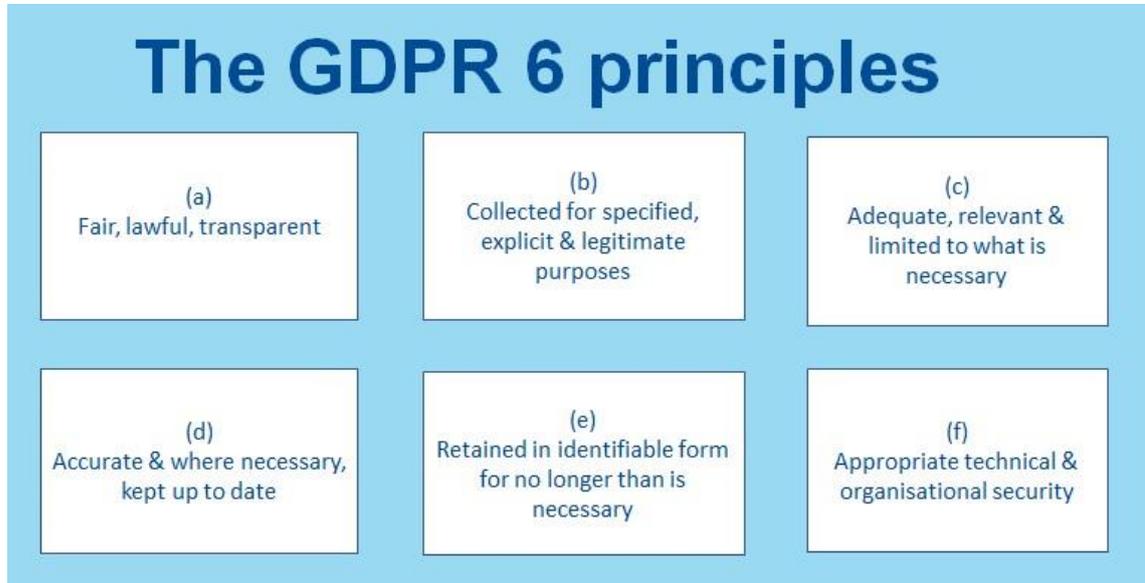
- 1.1 The General Data Protection Regulations (GDPR) and Data Protection Act (DPA) 2018 became law in 2018. The primary aim of this legislation is to enhance legal rights to data subjects in respect of using and storing personal data processed about them by data controllers.
- 1.2 South Essex Homes (the Organisation) needs to collate and handle personal information about individuals, the community, contractors and other organisations on behalf of the Council as a Data Processor and for data relating to past and present employees by South Essex Homes as Data Controller in order to provide a quality service and administer the Organisation efficiently and effectively. It processes information applying at least one of the six lawful reasons for processing data as stipulated by the Information Commissioner's Office;
 - (a) Consent:
 - (b) Contract:
 - (c) Legal obligation:
 - (d) Vital interests:
 - (e) Public task:
 - (f) Legitimate interests:

2. Policy Statement

- 2.1 The lawful, fair and correct processing of personal information by the Organisation is very important to its successful operations and to maintaining confidence.
- 2.2 To this end the Organisation fully endorses and adheres to the principles of data protection as detailed in the DPA.
- 2.3 The DPA consists of 6 enforceable principles of good information handling practice which data controllers are required to comply with.

3. The Six Data Protection Principles are:

3.1 Personal data shall be processed in the following ways;



4. Compliance with the Principles

4.1. The Organisation 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 only to the extent that is needed to fulfill 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
 - The right to be informed
 - The right of access
 - The right to rectification
 - The right to erase
 - The right to restrict processing
 - The right to data portability
 - The right to object
 - Rights in relation to automated decision making and profiling
- Ensure that personal information is not transferred outside the European Economic Area without suitable and adequate protection.
- Ensure that the Organisation's registration with the Information Commissioner's Officer remains up to date and accurate.

5. Management of Data Protection

5.1 The Organisation will ensure that:

- there is someone with specific responsibility for data protection. Currently the nominated persons are the Organisation's Chief Executive who is responsible for managing Data Protection for all employee related information; SEH has a designated Data Protection Officer, the Group Manager of Resources and Business Development. The Council's nominated Privacy Officers are the Director of Transformation and the Director of Digital Services. The Council also has its own Data Protection Officer, the Knowledge and Information Manager. Advice and support is also offered by Southend Borough Council's Data Protection Advisory Service within the Policy, Engagement and Communications Team.
- there is a DP/FOI Coordinators Group in place. This team disseminates best practice across the Council and South Essex Homes and assists with the handling of all Subject Access Requests, in line with the DP/FOI Coordinators 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, and are aware of procedures relating to Subject Access Requests, data breaches and potential data breaches
- 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 are undertaken to ensure compliance with current data legislation.

6. Complaints and Breaches of Data Protection

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

- Managers to ensure that all staff are aware of data protection in line with the terms and conditions of employment. The Human Resources Team will advise and support managers in any disciplinary action that needs to be carried out. The Group Manager for Corporate Services and Income Management will ensure that appropriate training is available.
- All complaints and potential breaches of the Data Protection legislation will be dealt with in accordance with the Organisation's Compliments, Comments and Complaints Procedure.
- Complaints from data subjects in relation to disclosures under Subject Access Requests will be dealt with by the Data Protection Advisory Service with the assistance of South Essex Homes.

- The Data Controller for Southend on Sea Borough Council (SBC) will assist the Organisation in determining how Subject Access Rights may apply, in accordance with the Individuals Rights of Data Subjects Policy and Procedure
- Where a complaint is made to the Information Commissioner's Office (ICO) the Data Controller for SBC will coordinate a response.
- The Data Controller for SBC will apply a fair and consistent approach to the recording and management of all Data Protection incidents and 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 Data Security Incident Management procedure.
- The Data Controller for SBC will consult with the Corporate Services Team at South Essex Homes 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 HR as appropriate, and action may be taken in line with the Organisation's Disciplinary policy.

7. Monitoring of this Policy

- 7.1 The Policy will be monitored by the Group Manager Corporate Resources and Income Management through routine reporting of performance and data incidents and breaches.

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 managed either for Employees of South Essex Homes by the Company as Data Controller and by Southend on Sea Borough Council for all data relating to the management of the housing stock.
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 (i.e. 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. Its website is www.ico.org.uk
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	Information which relates to a living individual who can be identified from that information or that and other information someone may have. 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.
Special Category (Sensitive) Data	Personal data about race or ethnic origin, political opinions, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation. More stringent requirements apply to the disclosure of special category data.
Criminal Offence Data	Personal data revealing details of criminal allegations, criminal proceedings, convictions and sentencing, related security measure and comprehensive register of criminal convictions. More stringent requirements apply to the disclosure of special category 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 one calendar month