Privacy & Data Protection Policy

Summary	This Policy sets out Southern Housing Group's (SHG) approach to protecting personal data and complying with data protection legislation.
Who to Contact	Data Protection Manager
Effective from	25th May 2018
Planned review date	25th May 2019
Version Number	Version 1

Contents

1. Policy
    a. Scope
    b. Definitions
    c. Objectives
2. Roles & Responsibilities
3. Related Documents
4. Contact Details

1. Policy

Southern Housing Group (The Group) is a registered social landlord (RSL) with social objectives. We provide high quality housing across a range of tenures, from supported living and affordable homes to shared ownership and outright sales, and we also provide a range of services to support our customers and the community.

In order to fulfil our landlord duties and our social objectives we collect, use, hold and process personal information (including special categories of personal data) about individuals, including our customers, members of the public, service users, applicants and employees, contractors, suppliers, partner organisations, and other stakeholders.

The Group respects the privacy of individuals and is committed to upholding the principles of data protection legislation to ensure that we protect and manage personal information lawfully and properly.

a) Scope

The policy governs the Group's conduct in processing of personal data and special categories of personal data as defined by data protection legislation (see section B).

This Policy applies to all employees of Southern Housing Group Ltd and all its subsidiaries, including volunteers, temporary, permanent and contracted workers.

b) Definitions

Data Protection Terms	Definition
Personal Data	Personal data is information relating to an identified or identifiable living individual.
Identifiable individual	An identifiable individual is one who can be identified, directly or indirectly by reference to: • A name, photo, job title, email address. • An identification number like an employee number. • Location data such as a home address or tracing location of a mobile phone. • An online identifier via IP address, internet cookies, social media account. • One or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of the individual such as a medical file.
Special Categories of Personal Data	This is considered to be a special category of personal data and under GDPR it will need an additional measure of protection. Under the new law this relates to data that reveals an individual's: • Racial or ethnic origin. • Political opinions. • Religious or philosophical beliefs. • Trade union membership. • Processing or genetic data. • Biometric data for uniquely identifying an individual. • Data concerning health. • Data concerning an individual's sex life or sexual orientation.
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly determines the purposes and means of the processing of personal data.
Data Processor	The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

c) Objectives

The Group understands the importance of the six data protection principles and upholds these as follows;

Principle 1: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals (data subjects).

- The Group ensures it has a legal basis (also known as 'conditions of processing' or 'legitimising conditions' as defined by the legislation) for the processing any personal information (including the collection, use, storage, and sharing of information)
- The Group clearly communicates to individuals about the way it processes their personal data, the purpose of the processing and the extent it is or will be processed,
- The Group ensures individuals are easily able to understand how their personal data is processed, including the risks, procedures and safeguards to protect it.
- The Group informs individuals about their rights in relation to the processing of their information and how to exercise their rights.
- The Group processes information in a way that is fair and consistent to the individual.

Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Purpose Limitation).

- The Group will only process and use personal data for the reason it was intended to be used as communicated to the individual (or a similar reason).
- Before processing any personal data for a similar or different purpose than it was originally intended, the Group will take into account the reasonable expectations of the individual, the consequences and any risks and effect it may have on the individual.

Principle 3: Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Data Minimisation)

- The Group will collect the minimum amount of personal information that is necessary to carry out its business activities, functions and obligations
- The Group will not collect, use, process or store information that is not relevant to carry out its business activities unless it is at the request of the individual.

Principle 4: Data is Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (Accuracy).

- The Group will take reasonable steps to verify the accuracy of personal information it holds with individuals.
- Where relevant the Group will apply corrections to the data held about an individual when they inform the Group of inaccuracies.

Principle 5: Personal Data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (Storage Limitation)

- The Group endeavours to retain personal data for the minimum length of time required to fulfil its legal and business purposes in accordance with its document and data retention schedule.
- Where personal data is no longer required, it will be securely destroyed in a timely and appropriate manner.

Principle 6: Personal data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Integrity and Confidentiality)

- The Group maintains policies and procedures to ensure information is secure when stored and used internally, or when sharing data with a third party, including our information security policy, data breach procedure, and procurement and contracting procedures.
- Personal data will only be passed to other organisations or agencies on a under approved Data Sharing Agreements or contractual arrangements or with an individual's consent unless there are exceptional circumstances.
- The Group will regularly train all employees in their responsibilities in relation to data protection and security of data, to ensure high levels of awareness and understanding amongst staff.
- The Group verifies the identity of all customers and their designated representatives when they contact us.
- We have a clear procedure to follow if a data breach is suspected or occurs, which ensures the appropriate steps to notify the ICO, inform the data subject and work to manage the consequences of any breach can take place in a timely way.
- We will require third parties to have adequate organisational and technology security measures in place to ensure integrity and confidentiality.

2. Roles and Responsibilities

Group Directors - The Group's Directors (Group Strategy Team) are accountable for this policy.

Data Protection Officer - The DPO is responsible for monitoring internal compliance, informing and advising Group Directors on data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for individuals and the supervisory authority.

Employees - Employees (including temporary and contractors) are responsible for acting in accordance with this policy. We will train all relevant employees as appropriate. Any breach of responsibility under this policy may be investigated under the Group's disciplinary policy.

3. Related Documents

Privacy Notices
Subject Access Request Form

Data Privacy Impact Assessment Procedure
Disciplinary Policy & Procedure
Data Breach Procedure
Document & Data Retention Schedule

4. Contact Details

For any concerns, queries in relation to this policy please contact the Data Protection Manager at data.protection@shgroup.org.uk.

Author	Melina Phillip, Data Protection Officer
Approval date	22nd May 2018
Approved by	GST (Group Steering Board)
Policy Owner	Kat Worth, Company Secretary