Data Protection Policy

COR-POL-08

Version 4.1

Date approved: 16 October 2018

Approved by: Audit and Risk Committee

1. Introduction

1.1 One of Southway's core values is 'Accountability' and we will be responsible and accountable in the way we use personal data.

1.2 This policy sets out Southway's approach to processing personal data, to ensure that Southway complies with the General Data Protection Regulation (GDPR) and other relevant legislation and that customers and staff know their rights and obligations.

1.3 It sets the overarching principles and commitments that underpin Southway's Information Governance Framework. A range of other policies, procedures and guidance set out how these principles and commitments will be delivered in practice.

1.4 All personal data processed in an organised manner by Southway, whether manually or electronically, is covered by the GDPR. Southway processes data about current, past and prospective tenants, leaseholders, service users, employees, and Board and Committee members.

1.5 This policy applies to Southway Housing Trust and all of its subsidiaries. All Southway employees and data processors acting on behalf of Southway must comply with this policy and the related procedures.

1.6 Important terminology used in this policy is defined in a glossary at the end.

2. Legislation and Regulation

2.1 The General Data Protection Regulation (GDPR) is the EU wide regulation that states how personal data should be processed. It aims to protect peoples' right to the protection of personal data. Compliance with the GDPR is the main focus of this policy.

2.2 At the time of producing this policy, a Data Protection Bill is in Parliament. Once this is enacted, the policy will be reviewed to ensure it is compliant.

2.3 The Privacy and Electronic Communication Regulations (PECR) complements the existing data protection regime and sets out more specific privacy rights on electronic communications.

2.4 The Information Commissioner (the ICO) is the regulator responsible for upholding and enforcing the GDPR and PECR. Southway Housing Trust and Southway Plus are registered with the ICO.

2.5 The ICO's website provides a wealth of information and guidance regarding the legislation.

3. Data Protection Principles

3.1 Southway will comply with, and will be able to demonstrate compliance with, the principles set out in the GDPR.

Personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) Accurate and, where necessary, kept up to date;

e) 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; and

f) 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.

4. Lawful Processing

4.1 Southway will only process personal data where:

1. We have identified and recorded the purpose and lawful basis for the processing, and
2. The processing is 'necessary' (it is a targeted and proportionate way of achieving the purpose).

4.2 At least one of these 'legal bases' must apply whenever we process personal data:

a) Consent: the data subject has given clear consent for us to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract we have with the data subject, or because they have asked us to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Special Categories and Criminal Conviction Data

4.3 In addition, one of these conditions must be met for us to process special categories of personal data or personal data relating to criminal convictions and offences:

a) The data subject has given explicit consent to the processing of the data for specified purposes;

b) Processing is necessary to meet the obligations or rights of the data controller or the data subject in the field of employment; or

c) Processing is necessary to protect the vital interests of the data subject.

4.4 Southway will never keep a comprehensive register of criminal conviction information.

4.5 There is supporting guidance on the lawful bases and a procedure for seeking and recording consent appropriately.

5. Data Subjects' Rights

5.1 Southway will facilitate and promote the data subjects' rights provided for in the GDPR:

The right to be informed	Southway must provide people with clear and concise information about what we do with their personal data (see section 6)
The right of access	Individuals can access their personal data and information about how we have processed it
The right to rectification	Individuals can ask us to correct inaccurate data
The right to restrict processing	Individuals can ask us to limit the way we use their data, for example whilst it is being 'rectified'
The right to erasure	Individuals can ask us to erase their data – also known as 'the right to be forgotten'
The right to data portability	Individuals can obtain and reuse data they have provided to us that is held in an automated IT system, for their own use in a different system
The right to object	Individuals can object to: • processing based on legitimate interests or public task (see legal bases above); • direct marketing; and • processing for purposes of scientific/historical research and statistics.
Rights in relation to automated decision making and profiling	We can only make decisions solely by automated means in certain circumstances, and where we do we must: • give individuals information about the processing; • introduce simple ways for them to request human intervention or challenge a decision; • carry out regular checks to make sure that your systems are working as intended.

5.2 Note that some of the rights only apply in certain circumstances. There is further guidance on this.

6. Privacy Information

6.1 Southway will provide information about the following matters to data subjects:

a) Identity and contact details of Southway's Data Protection Officer;
b) Processing undertaken, purpose and legal bases;
c) Categories of personal data processed;
d) Anyone that Southway will share the data with;
e) Details of any transfer of data to third countries and safeguards to ensure it remains secure;
f) Retention periods;
g) The existence of data subjects' rights;
h) The right to withdraw consent for processing, where relevant;
i) The right to complain and how to do so;
j) The source of personal data (where it is not supplied by the data subject);
k) Whether providing personal data is part of a contractual obligation and the consequences of not providing it; and
l) The existence of any automated decision making or profiling.

6.2 We will use a layered approach to ensure data subjects know the relevant information at the right time. A generic privacy statement will be published on our websites and privacy notices will be provided whenever we collect personal data.

6.3 The information we provide will be clear and concise, written in Plain English and easily accessible.

6.4 Click here to read our Data Protection & Privacy Statement

7. Data Quality, Minimisation and Retention

7.1 Before we collect personal data and on an on going basis, we will consider:

1. What data we really need in order to fulfil the intended purpose;
2. Whether and how we can ensure it is accurate and kept up-to-date;
3. How long it will need to be retained.

7.2 Data will be destroyed when it is no longer required for the intended purpose. Southway maintains a Data Retention Schedule, to guide employees about how long particular types of data should be retained. All

employees are responsible for using their judgement and discretion to ensure this Schedule is applied and reviewed regularly.

7.3 Where we need to retain information but it is not necessary for the subject to be identifiable, anonymisation will be considered.

8. Data Security and Personal Data Breaches

8.1 There is a separate Data Security Policy.

8.2 Southway's DPO will inform the ICO of any personal data breach within 72 hours of the breach becoming apparent.

8.3 Employees, Board/Committee Members and data processors (including consultants and contractors) must inform the Head of Governance and Performance immediately of any personal data breach, including the loss or theft of any ICT hardware or paper documentation that may contain personal data.

8.4 The procedure for dealing with a data breach will be highlighted as part of inductions and awareness raising campaigns.

9. Data Protection by Design

9.1 Southway will ensure that data protection and data subjects' rights are taken into account wherever a service change is underway, to ensure data subjects' rights are given due prominence in decisions and Southway remains compliant with the GDPR following changes.

9.2 There will be a Data Protection Impact Assessment (DPIA) Procedure. A DPIA is required where processing is likely to result in a high risk to individuals and their rights.

9.3 The need to consider data protection will be incorporated into procedural documents to be used during strategy setting, policy review and project planning, to ensure data protection is considered along with other issues such as equality and diversity and value for money.

10. Marketing and Electronic Communications

10.1 Southway will ensure that it is compliant with PECR, which covers:

a) Marketing by electronic means, including marketing calls, texts and emails.

b) The use of cookies or similar technologies that track information about people accessing a website or other electronic service.

c) Security of public electronic communications services.

d) Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services and directory listings.

11. Transparency and Freedom of Information

11.1 Southway is not obliged to comply with the Freedom of Information Act 2000 and does not have to respond to any requests made under the Act. However, we will operate within the spirit of the Act and be as open and transparent as possible. We will publish important information on our website and will make available any non confidential documents requested by our customers or any third party with a legitimate interest.

12. Use of Data Processors

12.1 Wherever Southway uses a data processor we will have a contract in place and will provide clear written instructions regarding the processing of personal data, to ensure both parties understand their obligations, responsibilities and liabilities.

12.2 Southway we will undertake due diligence prior to awarding a contract, to ensure data processors can meet the requirements of the GDPR, and will conduct audits and inspections during contracts as appropriate.

12.3 Contracts must set out:

a) The subject matter and duration of the processing;
b) The nature and purpose of the processing;
c) The type of personal data and categories of data subjects; and
d) The obligations and rights of the controller.

12.4 Contracts must include as a minimum the following terms, requiring the processor to:

a) Only act on Southway's written instructions;

b) Ensure that people processing the data are subject to a duty of confidence;
c) Take appropriate measures to ensure the security of processing;
d) Only engage sub-processors with Southway's prior consent and under a written contract;
e) Assist Southway in providing subject access and allowing data subjects to exercise their rights under the GDPR;
f) Assist Southway in meeting our GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
g) Delete or return all personal data to Southway as requested at the end of the contract; and
h) Submit to audits and inspections, provide Southway with whatever information we need to ensure that we are both meeting our Article 28 obligations, and tell Southway immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or the UK.

12.5 Southway has a set of standard contract templates and clauses, accompanied by guidance, to enable employees to ensure each contract is appropriate for the purpose.

13. Information Sharing

13.1 There will be occasions where Southway shares data with third parties (other data controllers, rather than data processors acting on Southway's behalf). This might be a routine arrangement (e.g. involvement in a safeguarding board) or a one off arrangement (e.g. where information is requested from the Police as part of a criminal investigation).

13.2 As with all processing, the purpose and legal basis for the data sharing must be established and recorded and Southway must comply with the data protection principles.

13.3 All instances of data sharing must be recorded.

13.4 For routine, systematic data sharing, there must be a written data sharing agreement in place, which must document as a minimum:

a) The purpose of the sharing;
b) The potential recipients or types of recipient and the circumstances in which they will have access;
c) The data to be shared;

d) Data security requirements and arrangements;
e) Data retention arrangements;
f) Procedures for dealing with access requests and fulfilling data subjects' rights;
g) The process for review of the effectiveness / termination of the sharing agreement;
h) Sanctions for failure to comply with the agreement or breaches by individual staff.

14. Responsibility and Accountability

The Audit and Risk Committee	sets and oversees the Information Governance Framework.
The Chief Executive	is ultimately accountable for ensuring that Southway complies with the GDPR and other data protection law.
The Head of Governance and Performance	will act as Southway's DPO (see section 14).
The Head of ICT	is responsible for the policies and technical measures necessary to maintain information security and otherwise apply the Information Governance Framework.
All Southway employees and data processors	must complete the required training and ensure they understand and comply with this policy and the related procedures

15. Data Protection Officer (DPO)

15.1 Southway will have a Data Protection Officer. This will be the Head of Governance and Performance. The tasks and responsibilities of the DPO are shown below and will be replicated in the Job Description of the Head of Governance and Performance.

Role
The DPO plays a key role in Southway's data protection governance structure and helps to improve accountability. They help Southway to operate within the law by advising and helping to monitor compliance.

Tasks
The DPO will:

1. Inform and advise the Board, the Executive Group, officers and data processors about Southway's obligations to comply with the GDPR and other data protection laws.
2. Produce and review Southway's data protection policies and seek the Audit and Risk Committee's approval for these.
3. Monitor compliance with the GDPR and other data protection laws, and with Southway's data protection polices. This will include:
    - Managing internal data protection activities;
    - Maintaining records of processing operations; and
    - Conducting internal audits.
4. Ensure staff receive appropriate training on GDPR and other data protection laws and raise awareness of data protection issues.
5. Advise on, and monitor, data protection impact assessments.
6. Assess and consider the risks associated with processing activities (taking into account the nature, scope, context and purposes of the processing) and provide risk-based advice to the organisation.
7. Be the first point of contact for and cooperate with the Information Commissioner's Office.
8. Notify the Information Commissioner's Office of any personal data breach within 72 hours of the breach becoming apparent.
9. Be the first point of contact for individuals whose data is processed (employees, customers etc).

Accountability and Reporting
The DPO reports directly to the Chief Executive and to the Parent Board (including via the Audit and Risk Committee).
It should be noted that the DPO is not personally liable for data protection compliance.

15.2 Southway will take account of the DPO's advice and the information they provide on our data protection obligations. If a decision is taken not to follow advice given by the DPO, the reasons for this will be recorded.

Accessibility

15.3 The DPO will be easily accessible to Southway's Board, Executive, employees, customers, other data subjects, and the ICO.

15.4 The DPO will ensure that there are effective arrangements in place should they be absent. The Governance Officer will act as deputy in most instances.

15.5 The DPO's contact details will be:

a) Published on the Southway and Gecko websites;
b) Included in all privacy notices;
c) Provided to employees on SID and as part of data protection procedures;
d) Provided to the ICO (including when consulting them about a DPIA); and
e) Provided to the ICO and to the individuals affected in the case of a personal data breach.

Support for the DPO

15.6 Southway will ensure that:

a) The DPO is involved, closely and in a timely manner, in all data protection matters;

b) The DPO operates independently and is not dismissed or penalised for performing their tasks;

c) Adequate resources are provided (sufficient time, financial, infrastructure, and, where appropriate, staff) to enable the DPO to meet their GDPR obligations, and to maintain their expert level of knowledge;

d) The DPO is given appropriate access to personal data and processing activities;

e) The DPO is given appropriate access to other services within Southway so that they can receive essential support, input or information;

f) The DPO's advice is sought when carrying out a DPIA; and

g) Any other tasks or duties assigned to the DPO do not result in a conflict of interests with their role as a DPO.

15.7 The DPO must have an expert knowledge of data protection law and practices (proportionate to the type of processing carried out by Southway). Any individual appointed to the role of Head of Governance and Performance must have the requisite skills and knowledge or must immediately be provided with appropriate training.

16. Staff Induction, Training and Awareness

16.1 At induction all staff will be introduced to data protection and Southway's Information Governance Framework, and informed of their responsibility for handling personal data in line with this policy.

16.2 There is a Data Protection Training Plan, specifying the level of expertise and the training required by each team or role.

16.3 The DPO, in partnership with the HR and ICT Teams, is responsible for ensuring that this Training Plan is delivered and there is regular awareness raising.

17. Related Documents

- Other documents that form the Information Governance Framework include the Data Retention Schedule, Privacy Notices and the Information Security Policy, as well as procedures and guidance
- ICT Policies and Procedures
- Codes of Conduct
- HR Policies and Procedures
- Single Equality Scheme and Customer Care Framework

18. Glossary of Important Terms

Personal Data	Any information relating to a person who can be identified directly or indirectly (i.e. by reference to other information). A wide range of information types can constitute personal data, including name, address, online identifier, payroll number, a rent payment, a vulnerability indicator on the housing management system, or a photograph or voice recording.
Special Categories of Personal Data	Personal data revealing or concerning: • Health, • A person's sex life or sexual orientation • Racial or ethnic origin, • Religious or philosophical beliefs, • Political opinions, • Trade union membership, • Genetic and biometric data

Data Subject	The person to whom personal data relates (e.g. the tenant or employee whose bank details Southway holds)
Data Controller	The organisation that determines the purposes and means of processing personal data. Southway is a data controller.
Data Processor	An organisation or individual that processes personal data on behalf of a data controller. Contractors, consultants and service providers appointed by Southway are data processors. There may also be cases where Southway acts as a data processor for another organisation.
Processing	Any operation performed on personal data, such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, disclosure (sending or publishing), or deletion.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

POLICY REVIEW HISTORY	
To be completed during each review	
Previous versions (version number – approved by – approval date – title if different) V1 - Board – 03/11/2009 V2 - Board – 29/08/2012 – Data Protection Policy V3 – Board – 30/07/2013 – Data Protection and Information Sharing Policy V3.1 – Audit and Risk Committee – 02/11/2016	
Date of last EIA:	April 2018
Review lead by:	Matthew Maouati, Head of Governance and Performance

Main points or amendments made and reasons

V4.1
Data Protection by Design section added

V4.0
A new policy was produced to reflect the new GDPR and encompass the Privacy and Electronic Communication Regulations (PECR). It is structured in line with the data protection principles. It is made clear that this policy will form part of a wider information governance framework, with some matters dealt with in different policies, procedures and guidance

- The lawful bases for processing and the full list of data subjects' rights have been included.
- The difference between using data processors and sharing information is made explicit.
- Detail of the circumstances in which data sharing will be undertaken has been removed.
- Based on ICO guidance, specific information is provided about what must be included in:
  - Privacy information for data subjects,
  - Contracts with data processors, and
  - Data sharing agreements.
- Detail regarding data retention and subject access has been removed – these are amongst the matters that will be covered by procedures.
- The policy regarding data quality and minimisation has been added.
- The 72 hour reporting period for subject data breaches has been added and highlighted, and the definition of a breach is included to make it clear that this includes things other than loss of data.
- Reference to the PECR and to marketing has been added.
- The Data Protection Officer is introduced and the Role Description for this role (which is based on ICO Guidance) replaces the previous list of the Head of Governance's responsibilities.
- Reference to the responsibilities of other parties have been added.

Next review due:	**Q1 2019/20**
Approval level:	**Audit and Risk Committee**

Southway's Data Protection Officer is:
Matthew Maouati, Head of Governance and Performance
Email: m.maouati@southwayhousing.co.uk
Telephone via the Southway Hub on 0161 448 4200