# Data Protection Policy

## COR-POL-08

## Version 4.3

**Date approved: 26 April 2022**

**Approved by: Audit and Risk Committee**

## 1. Introduction

1.1 This policy sets out Southway's approach to processing personal data, to ensure that Southway complies with r relevant legislation and that customers and staff know their rights and obligations.

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

1.3 All personal data processed in an organised manner by Southway, whether manually or electronically, is covered by this policy

1.4 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.

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

## 2. 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 | acts 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 |

## 3. Legislation and Regulation

3.1 The Data Protection Act 2018 (DPA 2018) is the legislation that states how personal data should be processed. It was influenced by the General Data

Protection Regulation (GDPR) which was an EU wide regulation enacted around the same time. Compliance with the GDPR is the main focus of this policy. Policy.

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

3.3 The Regulation and Investigatory Powers Act (RIPA)-Governs the use of covert surveillance by public authorities.

3.4 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.

## 4. Data Protection Principles

4.1 Southway will comply with, and will be able to demonstrate compliance with, the 6 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.

## 5. Lawful Processing

5.1 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).

5.2 There are 6 'legal bases' for processing data. We will identify and record the appropriate at least one of these prior to processing any 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.

**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. Special Categories and Criminal Conviction Data**

5.3 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.

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

**Record of Processing Activities**

5.5 Southway will keep a record of its processing activities (ROPA)_ including the legal bases for processing.

5.6 This ROPA will be updated at least annually, or when there is a significant change to processing such as

A new activity that requires data to be processed, or

A change in the legal basis for processing data.

5.7 All Managers and Heads of Service who are responsible for activities where personal data is processed will update the ROPA with the support of the Data Protection Officer.There is supporting guidance on the lawful bases and a procedure for seeking and recording consent appropriately.

**Data Quality, Minimisation and Retention**

5.8 Before we collect personal data and on an ongoing 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.

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

**Data Protection by Design**

5.10 Southway will ensure that data protection and data subjects' rights are taken into account wherever a service change, strategy or policy review, or relevant

project is underway, to ensure data subjects' rights are given due prominence in decisions and Southway remains compliant with the GDPR following changes.

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

**Surveillance and RIPA**

5.12 Southway will comply with RIPA and also carry out a DPIA prior to carrying out surveillance through the use of CCTV.

5.13 Southway may occasionally provide tenants with surveillance or sound monitoring equipment to assist with gathering evidence in Anti-Social Behaviour cases. In these instances the responsibilities and any liability for Data Protection will be explained to the tenant in advance. More information is provided in the privacy statement,

## 6. Data Subjects' Rights

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

| | |
|---|---|
| The right to be informed | Southway will be clear and transparent about how people's personal data is used through Privacy Statements (see section 6) |
| The right of access | Individuals can access their personal data and information about how we have processed it by submitting a Data Subject Access Request (DSAR). Southway has a separate DSAR procedure |
| The right to rectification | Southway will rectify inaccurate data once we are made aware of it. |
| 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'. Southway will erase data providing there are no grounds preventing deletion |
| 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.<br><br>This right only applies where the individual has provided the personal data themselves (by consent) and entered it into an automated system (such as a website form). |
| The right to object | Individuals can object to:<br>• processing based on legitimate interests or public task (see legal bases above);<br>• direct marketing; and<br>• 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:<br>• give individuals information about the processing;<br>• introduce simple ways for them to request human intervention or challenge a decision;<br>• carry out regular checks to make sure that your systems are working as intended. |

6.2 Some of the rights only apply in certain circumstances. Further guidance is provided in Southway's Privacy Notice

## 7. Privacy Information

7.1 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.

7.2 A generic privacy statement will be published on our websites and privacy notices will be provided whenever we collect personal data.

7.3 A separate Privacy Statement will be maintained that relates solely to how employees data is used by Southway. This will be available on the Staff Intranet, or on request from the Data Protection Officer, or the Human Resources Team.

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

## 8. Data Security and Personal Data Breaches

8.1 There is a separate Information Security Policy.

8.2 Southway's DPO will inform the ICO of any personal data breach within 72 hours of the breach becoming apparent. A procedure is in place to inform staff what to do in the event of a breach.

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.

## 9. Marketing and Electronic Communications

9.1 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.

## 10. Transparency and Freedom of Information

10.1 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 make available any non-confidential documents to our customers or any third party with a legitimate interest, providing the request is not deemed excessive.

## 11. Use of Data Processors

11.1 Wherever Southway uses a third party to process data 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.

11.2 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.

11.3 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.

11.4 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.

11.5 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.

## 12. Information Sharing

12.1 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).

12.2 All instances of data sharing must be recorded, with detail of the purpose and legal basis for doing so.

12.3 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.

**Use of e-mail** 13.1 Southway will avoid the use of e-mail for sharing personal data or sensitive personal data. If personal data is shared via e-mail, other security measures must be considered (encryption, or password protection) 13.2 Emails may need to be considered when we handle information requests under the right of access. Emails should be drafted carefully (ie be brief, factual and polite) and time should be taken to review the content of an email before it is sent.

13.3 All Southway Staff will receive periodic reminders about the potential for data breaches due to use of e-mail. Staff who wilfully or negligently caused data breaches due to improper use of e-mail can be subject to disciplinary action

## 13.3 14Data Protection Officer (DPO)

14.1 Southway will have a Data Protection Officer. This is currently the Head of Governance and Performance (HGP). The tasks and responsibilities of the DPO are replicated in the Job Description of the HGP.

14.2 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**

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

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

14.5 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**

14.6 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.

14.7 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 must have the requisite skills and knowledge or must immediately be provided with appropriate training.

## 15 Staff Induction, Training and Awareness

15.1 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.

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

15.3 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.

## 16 Performance Management1

16.1 Southway will record performance on key aspects of Data Protection, including, but not limited to; time taken to respond to Data Subject Access Requests and Signed Agreements in place for Data Sharing.

## 17. Related Documents

- Other documents that form the Information Governance Framework include the Data Retention Schedule, Privacy Notices, Records Management Policy 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).<br>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:<br>• Health,<br>• A person's sex life or sexual orientation<br>• Racial or ethnic origin,<br>• Religious or philosophical beliefs,<br>• Political opinions,<br>• 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. |
| ***Data Subject Access Request*** | Means by which someone can obtain personal information about themselves which is held by Southway |
| *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**<br>(version number – approved by – approval date – title if different)<br><br>V1 - Board – 03/11/2009<br>V2 - Board – 29/08/2012 – Data Protection Policy<br>V3 – Board – 30/07/2013 – Data Protection and Information Sharing Policy<br>V3.1 – Audit and Risk Committee – 02/11/2016<br>V4-Audit and Risk Committee 17/04/2018<br>V4.1-Audit and Risk Committee 16/10/2018<br>V4.2-Audit and Risk Committee 25/2/2020 | |
| **Date of last EIA:** | February 2022 |
| **Review lead by:** | Matthew Maouati, Head of Governance and Performance |

| **Main points or amendments made and reasons** | |
|---|---|
| V4.3<br>3.3-Inclusion of explanation of RIPA<br>5.6-5.7-Further explanation of the purpose and obligations on RIPA<br>5.12-5.13-Inclusion of explanation on use of Surveillance Equipment<br>7.3-Specific reference to Employee Privacy Notice<br>13.1-13.3-Specific section on use of e-mail. | |
| **Next review due:** | **Q3 2023/24** |
| **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