
# Data Protection and Information Sharing Policy

**COR-POL-08**

**Version 3.0**

**Date approved: 30 July 2013**

**Approved by: Board**

## 1. Purpose of the Policy

- To ensure compliance with the Data Protection Act 1998 (the Act).
- To ensure customers and staff know their rights and obligations under the Act.
- To ensure that Southway staff incorporate the principles of the Act into their daily work.
- To establish a framework for the sharing of information with third parties when it is appropriate to do so.

## 2. General Principles

2.1 In order to operate efficiently, Southway has to collect, store and use personal information about a wide range of people. This includes current, past and prospective tenants and other service users, current, past and prospective staff members, Board members, and contractors, consultants and suppliers.

2.2 All data held ("processed") in an organised manner by Southway, whether manually or electronically, is covered by the Act.

2.3 Southway is committed to collecting, using, storing and disposing of this data in a sensitive and responsible manner. We will at all times abide by and comply with the eight Principles of Data Collection, contained within the Act.

2.4 Southway will:

(1) Collect, use, store and dispose of (‘process’) personal data in a fair and lawful manner.

(2) Inform people why we collect information about them and only use the information for these specified purposes.

(3) Only process personal information which is adequate, relevant and necessary in relation to the purposes for which it was collected.

(4) Ensure personal data held is accurate and kept up-to-date.

(5) Only hold personal data for as long as is necessary in relation to the purposes for which it was collected, and dispose of all data in a timely manner.

(6) Ensure the people about whom data is held can access information about themselves where appropriate and exercise other rights in accordance with the Data Protection Act.

(7) Take appropriate technical and organisational security measures to safeguard personal data against loss or damage and inappropriate or unlawful use.

(8) Not transfer personal data outside of the European Union without appropriate safeguards.

## 3. Freedom of Information Act 2000

3.1 As a Registered Provider Southway Housing Trust 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, as a responsible landlord, we will operate within the spirit of the Act and be as open and transparent as possible. We will make available upon request any non confidential documents requested by our customers or any third party with a legitimate interest.

## 4. Responsibilities

4.1 The Governance Team have overall responsibility for the effective management and operation of data protection policies and procedures at Southway. On behalf of the Trust, the Governance Manager will:

(a) Notify the Information Commissioner of Southway's processing of personal data annually and within 28 days of any significant change.

(b) Notify the Information Commissioner of any breaches of the Act.

(c) Ensure Southway's data protection policy and practices are kept up-to-date with legislative changes and the latest best practice, and that staff and contractors are aware of these.

(d) Ensure information about Southway's data protection policy and procedures is made available to customers on Southway's website and at Reception.

(e) Ensure Southway's Privacy Statement is kept up-to-date and is made available to customers, staff, contractors and others.

(f) Ensure staff and contractors have access only to the personal data which they require for the effective performance of their duties.

(g) Monitor Southway's handling and use of personal data to ensure that this is effective and the Act is complied with.

(h) Ensure all staff members with access to personal data are appropriately trained.

(i) Provide advice and guidance on data protection to Southway staff, contractors, customers and others.

(j) Coordinate responses to requests for information from the subjects of data and others.

4.2 All staff will be made aware at their induction of their contractual responsibility for handling personal data in line with this policy and with good data protection practice.

4.3 Any accidental loss or sharing of personal data should be notified to the Governance Manager as soon as possible.

## 5. Data Collection

5.1 Southway has a Privacy Statement, which it will make available on its website, at Aspen House Reception and upon request.

5.2 The Privacy Statement reads as follows:

> To undertake the functions of Southway Housing Trust in providing effective housing, we have to obtain, process and store personal information about our applicants, tenants and suppliers.
>
> We will only request personal information that is appropriate for our business functions, and you may refuse to provide information if you deem any requests to be inappropriate.
>
> Any personal information you give to us will always be processed in accordance with the UK Data Protection Act 1998.
>
> We will only use the personal information you provide to deliver the services you have requested, or for our lawful, disclosed purposes.
>
> We will not make your personal details available outside our organisation without your consent, unless obliged to by law or to enable us to deliver, or services or by operation of law.

You are entitled to see a copy of the personal data we hold on you.

5.3 All requests for personal information should be accompanied by an explanation of the purposes for which the data will be used.

## 6. Sensitive Personal Data

6.1 The Act prohibits the processing of sensitive data except in specified circumstances, for example diversity monitoring. Explicit and informed consent of the Data Subject should be obtained for the processing of information that may include sensitive personal data.

6.2 Sensitive Personal Data is classed as the following:

- The Data Subject's:
  - Racial or ethnic origin
  - Political opinions
  - Religious beliefs or other of a similar nature
  - Physical or mental health or condition
  - Sexual life
- Whether the Data Subject is a member of a trade union
- The commission or alleged commission by the Data Subject of any offence, or any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

## 7. Data Retention

7.1 In accordance with the Data Protection Act, all staff should securely dispose of any personal data held once it is no longer needed for the purpose for which it was collected. Staff should use their personal judgement about what information is no longer needed and refer to the Governance Manager for advice and guidance.

7.2 Southway has a Document Retention Schedule which concerns various types of information, including personal information. For each document type the Schedule sets out the period of time for which it should be retained, and after which therefore t should be securely destroyed. It also identifies a staff member who 'owns' each document type and this individual will be responsible for the secure retention and disposal of the document(s). The

Governance Team will have oversight of the Schedule and will monitor compliance with it.

7.3 It is vital that any personal information no longer needed by Southway is disposed of securely, using secure recycling bins and shredders as appropriate. This includes informal notes as well as information stored in organised systems, and is the responsibility of all staff.

## 8. Access to Personal Information

8.1 Staff, customers and other individuals have the right to access personal information that Southway holds about them. Southway has a Subject Access Request Procedure, which provides details of how a request should be made and dealt with.

8.2 It is the responsibility of the Governance Team to coordinate the response to a request for information.

8.3 Southway will not usually agree to process subject access requests make make personal information about a subject available to third parties without the written consent of the subject. However there may be occasions when we will share information without consent and these are listed below.

## 9. Information Sharing

9.1 During the course of Southway's operations it may become necessary to share information about customers and others with third parties. In order to comply with the principals of the Act, information should only be shared in very limited circumstances or where consent has been given.

9.2 We may disclose information to a third party without consent in the following circumstances:

(a) Where disclosure to another organisation may be justified in the individual's best interests. This includes if the individual is likely to be a victim of crime, or at serious risk of harm, or causing harm.

(b) To comply with the law

(c) To assist in the prevention or detection of crime

(d) In connection with legal proceedings

(e) Where disclosure is necessary to provide services for our tenants and we can justify sharing data for this reason. In these cases it is essential that the data is used only for the purposes agreed (for example, to target under occupiers as identified by the City Council)

9.3 Southway may wish at certain times to participate in information sharing schemes that further the interests of its tenants or communities. Before setting up or agreeing to participate in any such scheme, the advice of the Governance Manager should be sought.

9.4 The Governance Manager will assess the desirability of Southway participating in an information sharing scheme based on the following criteria:

- Whether participation will improve the position of our tenants and/or communities
- Whether participation will aid the prevention or detection of crime
- Whether a Data Sharing Agreement / Protocol is needed / is in place
- Whether consent from the subject is needed before information is shared

9.5 It is good practice for a Data Sharing Agreement to be in place before any arrangement which will involve the transfer of large amounts of tenant data between Southway and another organisation. It is the responsibility of the officer leading on the information sharing scheme to arrange this agreement, but they should then pass the document to the Governance Team to store.

9.6 It is important to remember that even where Southway has an agreement to share information with another organisation, it may not be appropriate to do so in all circumstances.

## 10. Contractors and Third Parties

10.1 All contractors, consultants, partners or other servants or agents of Southway who are users of personal information supplied by Southway will be required to confirm that they will abide by the requirements of the Act.

10.2 Southway will require that they enter into a contract which will oblige them to:

(a) Ensure that they and all of their staff who have access to personal information held or processed for us or on our behalf, are aware of

this policy and are fully trained in and are aware of their duties and responsibilities under the Act.

(b) Ensure that they only act on our instructions with regard to the processing of personal information we supply to them.

(c) Ensure that they have adequate security measures in place regarding personal information supplied to them and, in particular, will take appropriate organisational and technical steps to ensure that there is no loss, damage or destruction of such information.

(d) Allow data protection audits by Southway, of information held on its behalf (if requested).

(e) Indemnify Southway against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation arising out of any breach of the Act by them.

10.3 Any breach of any provision of the Act will be deemed as being a breach of any contract between Southway and that individual, company, partner or firm.

## 11. Links to Other Policies

- Staff Code of Conduct
- ICT Network Security Policy
- ICT Internet & Email Usage Policy
- ICT Remote Access / Mobile Computing Policy
- Secure Disposal of ICT Equipment Policy
- ICT Information Security Policy

## 12. Supporting Documents

- Subject Access Request Procedure
- Data Retention Schedule

| **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 – Data Protection Policy<br>V2 - Board – 29/08/2012 – Data Protection Policy | |
| **Date of last EIA:** | N/A |
| **Review lead by:** | Matthew Maouati, Governance Manager |
| **Main points or amendments made and reasons**<br><br>▪ Simplified, reduced in length and put in a more logical order<br>▪ Some procedural detail removed<br>▪ Merged the Data Protection and Information Sharing policies, due to their inter-related nature<br>▪ Added detail about data retention<br>▪ The intention is to make the policy more readable for staff and customers | |
| **Next review due:** | **Q2 2015/16** |
| **Approval level:** | **A – Board** |