Southside
HOUSING ASSOCIATION

Data Protection & Confidentiality of Personal Information

Issued: March 2016
Reviewed: March 2019

1.0 Policy Purpose and Statement

1.1. This Policy describes how the Association will comply with the law on data protection and protect individual rights to privacy and confidentiality. The Policy covers:

- Processing personal information about individuals (our customers[1] and employees);
- How we use personal information and who we may share it with;
- Helping people to access (and if necessary correct) their personal information;
- Making sure information is secure, and does not fall into the wrong hands;
- The standards of confidentiality that customers and employees can expect from us.

1.2. The Association will maintain our registration as a Data Controller under the Data Protection Act 1998 and ensure that our practices comply with the Act. Looking to the future, we will monitor progress in finalising new European Union Data Protection Regulations, expected to be fully in force by 2018[2].

1.3. The Policy and the associated operational procedures will also be used by our subsidiary Southside Factoring and Related Services Ltd.

2.0 Responsibilities for Approval, Implementation and Compliance

2.1. The Management Committee is responsible for approving this Policy, and will receive:

- Reports on complaints received, and
- Immediate notification of any substantive breaches in security or loss of personal data.

2.2. Management responsibilities for data protection will be as follows:

Responsibility	**Officer**
• Overall responsibility for data protection within SHA	Director
• SHA's entry in the Data Protection Register	Corporate Services Manager
• Management oversight of policy implementation and compliance in different business areas	Departmental Managers
• Managing all personnel data, in accordance with Data Protection Act 1998 (DPA) principles	Corporate Services Manager
• Disseminating information about the DPA to all departments and providing advice/support on compliance • Responding to requests from individuals to access personal information we hold about them	Corporate Services Manager
• Co-ordinating action on data security, in consultation with all departments	Head of Finance
• Management of CCTV installations at the Association's residential properties	Concierge Managers

[1] **"Customers" covers prospective (e.g. housing applicants) as well as existing SHA customers**

2.3. We expect all members of staff to comply with this Policy when carrying out their job role, and will provide staff training to support this.

3.0 Policy on Confidentiality of Personal Information

3.1. The Association is committed to protecting the right to confidentiality of our customers and employees. The following requirements on confidentiality must be observed at all times:

Information about customers

- Committee reports or minutes must not contain any means of identifying individual customers (e.g. names, addresses, economic status etc)
- Staff must not divulge personal information about customers to anyone other than fellow staff members or other professionals, and the sharing of the information must be linked to clearly defined legal and professional duties
- Disclosure of sensitive personal information must take account of the Data Protection Act conditions for processing (including the role of consent)
- Data records (both paper and computer) must be kept securely. The Association's committee members have no right to access personal data records.

Information about employees

- Information relating to employment will generally be treated as confidential. This includes selection and recruitment, remuneration, and any grievance or disciplinary action (although information about misconduct will be reported to management).
- Information processing and access to personal information will be managed in accordance with data protection legislation.
- Senior managers, line managers and Corporate Services staff will hold or have access to records relating to current and former staff members.
- Details of individuals' personnel records will not be made available to committee members, other than in the exceptional circumstances where committee decisions are needed at the final stage of any disciplinary matters.

3.2. The requirements on confidentiality stated above do not apply if:

- An individual waives their right to confidentiality (for example, a customer makes personal representations to the Management Committee on a disputed matter)
- The Association has a legal obligation to make information available to a third party (for example, under the data processing exemptions and disclosures required by law stated in the Data Protection Act 1998).

3.3. Any deliberate breach of confidentiality is a serious matter under the Association's codes of conduct. If serious breaches are alleged, these will be investigated. The possible sanctions will include a written warning or dismissal for a member of staff, and a vote to remove a member of the Management Committee.

4.0 The Data Protection Principles

4.1. The Association must implement this Policy in a way that meets the principles set out in the Data Protection Act 1998. This means personal information must be:

- Obtained and processed fairly and lawfully
- Obtained only for specified and lawful purposes, and not used for any other purpose
- Adequate, relevant and not excessive in relation to the purpose for which the information is obtained or kept
- Accurate and up to date
- Held no longer than is necessary for its purpose
- Processed in accordance with the rights of data subjects under the Act
- Kept securely

5.0 Obtaining and Processing Personal Information

5.1. The Association will comply with the conditions for processing in the Data Protection Act (Schedules 2 and 3), including the conditions relating to sensitive personal information. This includes information about a person's ethnic origin, family relationships, gender orientation, health, financial details, religious beliefs, political opinions, sexual life and criminal record.

5.2. When external contractors create or have access to records about our customers (e.g. repairs contractors or customer survey contractors), we will establish data protection compliance responsibilities and requirements, normally as a condition of the contract.

5.3. In exceptional circumstances, the Association may rely on the exemptions stated in Part IV of the Data Protection Act to set aside the normal conditions for processing. The exemptions include matters such as preventing or detecting crime, disclosures required by law, and information required for the purposes of regulatory activity.

6.0 How We Will Use Personal Information

6.1. The Association will provide customers with a **Privacy Notice,** explaining:

- What personal information the Association collects and why;
- The main ways we will use information; and
- When we are likely to share information, for example with service delivery partners.

6.2. The Association will use the Privacy Notice as part of our sign-up routines for new customers For existing customers the Association will use the quarterly newsletter to publicise how we will use personal information. We will also use summary versions of the full privacy notice where appropriate (for example, on our website).

6.3. The Association will produce tailored guides for different services where required, for example housing support services. We may also adapt or supplement our forms for employment and service delivery, if we need to collect sensitive personal information and a customised privacy notice is needed.

7.0 Access Rights to Personal Information

7.1. The Association wishes to make it easy for people to have access to their personal information. We will always seek to be open in providing access to the information we hold, and individuals will also be able to exercise their rights to:

- Know what information the Association is processing
- Ask why the information is being processed, the source of the data (if known) and whether we will give it to any other organisations or people
- Challenge the accuracy of any non-confidential information we make available, and ask for information to be corrected.

7.2. Wherever possible, we will deal with simple information requests on the spot rather than as a formal subject access request. In responding to formal requests, we will adopt the following features of the framework set out in the Data Protection Act:

Responding to Subject Access Requests

- Requests must be made in writing, and the identity of the requester must be verified
- We will normally charge a fee of £10.00, as permitted by the Act
- We will respond within a period not exceeding 40 days (the timescale specified in the Act), and sooner than this where possible
- In general we will not make available:
  - Information relating to, or identifying, another person unless that person has given their written permission for us to do so
  - Confidential information given to the Association by third parties such as doctors, social work and the police, unless the third party has given their written permission for us to disclose it
  - Information relating to contemplated or actual legal proceedings or commercial negotiations and transactions
  - Personal information that is subject to the exemptions set out in Part IV of the Act

7.3. The Association will provide a copy of the information requested in a permanent form (for example, a written statement or photocopies), unless the individual prefers to view their personal file at our offices. If it is not feasible to provide information in a permanent form, we will offer the opportunity to inspect files/data at our office.

7.4. The Association will establish procedures to review personal information that is challenged or disputed by the person to whom the information relates. We will amend records where there are agreed errors of fact, and make sure any disputed information that cannot be verified is explained on the individual's file.

8.0 External Requests for Access to Personal Information

8.1. The Association's general policy is that only information that can or must be legally disclosed under the Data Protection Act will be shared with a third party, unless we have the individual's consent.

- Our operational procedures restrict what information can be released without the individual's consent, and who it can be provided to;
- If a request involves sensitive information (for example, about an individual's health), we will always seek to obtain explicit consent;
- We will provide the individual with information about the information requested, the purpose of the request and how the information may be used.

8.2. In exceptional circumstances in which the Data Protection Act allows us to disclose personal information without consent. For example, disclosures required by law; information relating to the prevention or detection of crime; and disclosure to protect the vital interests of an individual where their consent cannot be given or obtained.

9.0 Disclosure of Personal Information by the Association

9.1. If the Association itself considers it necessary to disclose or share information about an individual with a third party, we will:

- Do this wherever possible with the individual's consent, and
- Advise the individual of the extent and nature of the information being given.

9.2. In exceptional circumstances, the Association may provide information where consent has not been given. For example, if the Association is under a statutory obligation to provide information, or if withholding information may put the welfare of vulnerable individuals at risk. The Association has a duty of care that may require information to be passed on to colleagues, relatives or other professionals. In such cases, we will only make information available to those who need to know it.

9.3. If information is disclosed to a third party without the individual's consent, this will be recorded in a file note which will be counter-signed by a departmental manager.

10.0 Keeping Personal Information Safe and Secure

10.1. The Association will be vigilant in safeguarding personal information. We will implement a range of measures, as summarised below, to help minimise and manage the risks of data loss or unintended disclosure.

Standards for protecting personal information

- **Forms/data collection:** Ensure only essential information is collected.
- **Data security:** Information accessible only to those who need to know it in order to carry out their duties. Computers and individual systems password-protected. Paper files and records kept secure at all times.
- **Use of personal data out of the office**: Staff accessing SHA emails externally should use SHA devices wherever possible. Staff may also access emails via their own devices but should be aware of the necessity for data protection on their own

device. Staff accessing SHA servers and directories must only use SHA devices. SHA mobile devices shall be password protected and encrypted where possible.

- **Discussion of personal or confidential matters:** Discussions with customers must take place in a private space. Caution required if discussing customers with colleagues out of the office (e.g. when using public transport).

Corporate actions to enhance security

- **Staff training:** on data management and security
- Corporate Services Manager will have lead responsibility for information security, including investigation and remedying of any breaches; co-ordination between departments; and audits of security measures
- **Business continuity plan:** Including provision for protecting/recovering personal information held
- **Paper records and obsolete ICT hardware** will be disposed of securely through a private company for professional data deletion where appropriate.
- **Security procedures:** authenticate the identity of a person asking for personal information to be disclosed by phone or e-mail
- **Security procedures:** control access to SHA business premises, supervise visitors
- **Corporate data security measures:** Systems are protected by firewall and virus checking software. Sensitive and confidential information will only be through secure email. All data held on servers is backed up daily and maintained offsite.

10.2. If any loss or unintended disclosure of personal information occurs, we will take immediate action to limit any damages. We will also notify the individual(s) affected, the Association's Management Committee and any third parties as required (for example, the local authority, banks, the Police).

10.3. Having taken any immediate action needed, we will evaluate the circumstances that led to any breach or failure and revise our policy and procedures accordingly.

11.0 Retention and Disposal of Personal Information

11.1. The Association must ensure that we do not retain personal information any longer than is necessary for the purpose for which the information was provided. We must also update the information we hold, if this is required (for example, service usage by existing customers, housing application reviews for potential customers).

11.2. Each department will be responsible for implementing housekeeping arrangements to dispose of information that is no longer needed. This should take account of the Association's guidelines for document/data retention, which take account of statutory requirements and the possibility of any future claims against the Association.

12.0 CCTV Images

12.1. The Association operates CCTV in a number of our neighbourhoods, to help reduce anti-social behaviour, prevent crime and create safer environments for our customers.

12.2. The Data Protection Act 1998 covers the collection and processing of images of individuals using CCTV cameras. The Association has measures in place to:

- Provide appropriate signage where CCTV is in operation (this responsibility is currently contracted out to the approved contractor, Video Watchman Systems Ltd.).
- Ensure that cameras are in operation at all times.
- Conduct regular checks to make sure images are correctly date- and time-stamped and are securely stored. This is done on a monthly basis by connecting to each CCTV server remotely.
- Restrict who can view CCTV images (The Association has a written procedure regarding how to request a copy/viewing of CCTV footage. This is on display at all Concierge sites)
- Provide individuals with access to their personal information, upon request.
- Consider stopping or preventing processing that is causing damage or distress to an individual.
- Delete images within 21 days when there is no longer a reason to keep them.
- Record the details of any disclosure of CCTV data to third parties (e.g. the Police and Community Safety Glasgow), including the date of disclosure, the name of the third party organisation and the purpose for which the disclosure was made.
- The Association has a written protocol on information sharing with the Police and Glasgow Community Safety (see attached)

13.0 Appeals and Complaints

13.1. Customers may use the Association's Complaints Procedure if they are dissatisfied with how we have kept, used or provided access to their personal information, for example:

- If there is a dispute as to whether information held on file is factually correct or not;
- If a customer believes we are continuing to process information that is out of date or no longer relevant;
- If we have refused access to documents (except those containing information supplied in confidence by third parties that are not prepared to allow disclosure, or any information covered by legal exemptions from disclosure).

13.2. The Association's Director will be responsible for deciding appeals or complaints, with details noted on the relevant file. Thereafter, if matters have not been resolved to the customer's satisfaction, they may refer their concerns to:

- The Scottish Public Services Ombudsman, or
- The Information Commissioner's Office, under section 42 of the Data Protection Act.

14.0 Publishing the Data Protection and Confidentiality Policy

14.1. The Association will make copies of this Policy available at each of our offices, as well as an information leaflet in English, translated into Urdu, Punjabi, Arabic and Hindi, and any other community languages on demand. Languages specified are as per current SHA Policy.

14.2. Tenants/Residents receiving a Housing Support service from Southside Housing Association will be made aware of this Policy when commencing the service.