

1. Scope of Policy

Soha's Data Protection policy sets out our approach to the protection and retention of personal data, in accordance with the Data Protection Act, 2018 (DPA) incorporating GDPR Regulations.

During the course of business, Soha collects and uses personal information. This applies to:

- Tenants, former tenants and housing applicants
- Leaseholders and shared owners
- Employees and applicants for employment
- Board members
- Complainants
- Contractors and suppliers
- Others who may not fall into any of the above categories, but to whom Soha provides services, or with whom Soha contracts

This policy only applies to individuals, and not to limited companies or other corporate entities. Statistical information that does not identify individuals is not subject to this policy.

2. Aims of Policy

Soha recognises that personal information must be processed lawfully under the principles set by the DPA, and that individuals have a right to access the information we hold about them. Soha will comply with all legal requirements transparently. We provide equal access to this service and will not discriminate on protected grounds.

3. Policy Statement

Soha Housing Ltd is registered with the Information Commissioner as a Data Controller and processes personal information in accordance with the eight data protection principles set out by the DPA, which requires all personal data be:

- Obtained and processed fairly and lawfully
- Obtained only for specific and lawful purposes, and not used for any other purposes
- Adequate, relevant, and not excessive in relation to the purpose for which it is processed
- Accurate and up-to-date
- Kept no longer than is necessary
- Processed in line with the individual's rights
- Secure
- Not transferred to a country outside the EU without adequate protection

Soha will ensure that the way we collect and use personal information will be fair, relevant, secure, and transparent. We only share personal information in accordance with law and ensure third parties have the same standard of data protection as Soha. When we send optional information about services to residents, we will ensure we follow the regulations relating to direct marketing, and allow residents to opt out of receiving this material.

Soha will have a clear statement for customers outlining the contents of this policy, including: why we collect data, how we process it and how they may access their personal data.

4. Implementation

4.1 Processing information

Soha processes personal information during the course of business, in order to provide a good service to customers and stakeholders. Personal information is information that relates directly to a living individual who can be identified. The information Soha could process includes, though is not limited to:

- Information about customers – contact information, financial information, data about family circumstances or history, support needs, or medical needs, for example;
- Information about employees and board members – for example, details from employment applications, contract terms, salary, pension, or benefits details;
- Information about other groups or persons – this could include information Soha holds on contractors or complainants, for example.

Soha records calls received by customer services for training and informational purposes. These calls are kept for approximately three months and then erased from the system. No financial details are recorded during the course of these calls.

We may collect information about those who visit our website in the form of ‘cookies’, which send us small amounts of information about how people browse our site. We use this information to improve the browsing experience. You can decline the use of cookies. For more information, please visit: <https://www.soha.co.uk/information/privacy-and-cookies>.

4.1.1 Consent to information processing

Soha will obtain consent from those whose information it processes. By signing a contract of employment or service, or signing a lease or tenancy agreement, consent applies to the processing of personal data required during the usual course of business, unless that data is sensitive personal data.

- Sensitive personal data includes information about racial or ethnic origin, political opinions, religion or other beliefs, trade union membership, health, sexual orientation or identity, and criminal proceedings or conviction. Soha will normally obtain the explicit consent of the individual in advance of disclosure.

Most of the communication that Soha has with its residents is related to its core activities as a social housing provider. Core activities are defined as those in Soha’s business plan. However, as we take the privacy of our residents seriously, we will ensure communication that gives information about services nonetheless complies with direct marketing regulations. Residents will have the option to opt out at the point of data collection. .

4.2 Security

Soha has put in place and will maintain both physical and electronic security measures to ensure only those with a legitimate reason for processing the data have access to it. All employees or involved residents who have access to information are responsible for securing this information, and should not disclose it to third parties, unless in accordance with this policy.

Soha has security measures to protect electronic data, and keep personal information held on paper in secure filing systems. Documents containing personal information should not be left on desks, or on computer screens open to public view.

No portable digital media containing personal information should be removed from the office unless in accordance with Soha’s Information Security policy (SP33). Furthermore, Soha will not

send electronic information from its computers unless the process complies with our procedures on the transfer of data to third parties.

4.3 Access to personal information

Soha has agreed procedures for dealing with access to personal information, and has trained staff to deal with these requests.

- Soha has a Data Protection Officer (DPO) who keeps a record of all Data Subject Access Requests (DSAR).
- Soha will not charge a fee to deal with a request for information. However where requests are 'manifestly unfounded' or 'excessive' it is permissible to charge a reasonable fee.
- When a DSAR is received Soha must respond within one month unless where the request is complex in which case Soha will have a further two months to comply with notification sent to the data subject that this is the case.

A DSAR should be made on the appropriate form that can be downloaded from the Soha website at: <https://www.soha.co.uk/information/data-protection/> we can assist those with learning disabilities to access this service, or assist their support worker in doing so. We will provide copies of the relevant documents unless this would be excessive or unreasonable. Additionally, we will explain technical terms to the individual.

Soha will change or delete information which we discover is clearly wrong. If we cannot agree a dispute about the accuracy of information, we will add a note to reflect this dispute.

Certain information is exempt (DPA 2018) from Soha's policy on access to personal information and will not be available for individuals to view through this policy. This includes:

- Information relating to a third party, unless the third party has given written consent;
- Information from third parties or other agencies which could be reasonably expected to be confidential (i.e. lawyers);
- Information subject to legal professional privilege or statutory requirement, or information that is likely to lead to legal proceedings being taken;
- Information that is prejudicial to the commercial or financial interests of Soha.

When Soha refuses a request for information, we will give the individual reasons for this.

4.4 Disclosure of information to third parties

Personal information may only be disclosed to third parties in accordance with the principles in the DPA. Where Soha discloses information to third parties, we will ensure they have adequate security and data protection measures in place, and provide written guarantees to this effect.

Soha may disclose personal information (including sensitive personal information when absolutely necessary) to third parties without the consent of the individual, only in the following circumstances:

- In connection with the assessment or collection of tax or duty (i.e. Council Tax)
- For the detection or prevention of crime (i.e. a police investigation)
- Where disclosure is necessary to protect the vital interests of the individual (i.e. medical emergency)
- To comply with prevailing health and safety legislation
- Where a court orders the disclosure

Soha will train all staff on the contents of this policy and associated regulations in accordance with their role in the organisation.

5. Resident Involvement

This is an internal policy that deals directly with the way Soha complies with the DPA 2018 & GDPR, so consultation with residents when drafting the document is minimal. However, as with all policies, it will be scrutinised and approved by our involved tenants in the Members' Forum. We will also consult with tenants about our data protection practices to inform policy changes and best practices.

6. Further details

Further details can be found at: <https://www.soha.co.uk/information/data-protection/> or from the Information Commissioners Office <https://www.ico.org.uk> or upon request to:

Data Protection Officer
Soha Housing Limited
99 Station Road
Didcot
Oxfordshire
OX11 7NN

Tel No: 01235-515-900 / Freephone: 0800-014-15-45

Email: dpo@soha.co.uk

7. Monitoring / Responsibility

The Director of Finance & Resources has overall responsibility over access to personal information. The Data Protection Officer is responsible for data protection issues. The relevant Service Manager will process requests by tenants to view their personal information. The HR Manager will process requests by Staff and Board Members to view their personal information.

This policy is regularly monitored and updated, in line with changing legislation and best practice.

Context

Data Protection Act 2018
General Data Protection Regulations 2018
Equalities Act 2010
Human Rights Act 1998
Limitations Act, 1980
CCTV Code of Practice, 2008
SP35 Social Media

Computer Misuse Act 1990
NHF Document Retention for Housing Associations guidelines, 2018 (revised)

SP33 Information Security, Email, and Internet

| | | | |
|-------------------------|-----------------|----------------|-----------------|
| Members' Forum Approved | 24 January 2019 | Board Approved | 31 January 2019 |
| EIA Completed | | Review Date | By January 2023 |