

Appendix 1: Data Protection [UK GDPR] Policy

This statement should be read in conjunction with the policy and the privacy notice. The statement demonstrates how Soha Housing Ltd and its subsidiaries carry out their obligation under the Data Protection Act 2018 and UK GDPR.

CONTENTS

Section	Subject	Page
Part 1	Rights of the Individual	
	1.1 Privacy Notice	3
	1.2 Administration of an Individual's Rights	3
	1.3 Marketing	4
	1.4 Data Subjects	4
Part 2	Lawful Processing	5
Part 3	Disclosure	
	3.1 Information Sharing	6
	3.2 Safeguarding Information	6
	3.3 Exemption	7
Part 4	Management of Personal Information	
	4.1 Information Governance Framework	8
	4.2 Records and Housekeeping	8
	4.3 Data Protection Impact Assessment	9
	4.4 Retention and Disposal of Data	9
	4.5 Personal Data Breach	9
Part 5	Surveillance and Audio	10

Part 1: Rights of the individual

1.1 Privacy Notice

1.1.1 Soha provides information to its data subjects in a privacy notice which resides on the website. We ensure that this privacy notice is included in the following:

- in a dedicated section of contracts of employment
- in our Board packs
- in our shareholder packs
- in our resident's handbooks
- on our web-based marketing site
- in our seller's packs
- in our sign-up packs for new tenants
- in our recruitment packs
- in our tendering and procurement literature

1.1.2 Our privacy notice sets out:

- the eight privacy rights
- how to contact us with a privacy matter
- how to make a complaint
- what we use the information provided for
- what information we hold
- how and when we share information
- our approach to automated decision making
- how we will deal with transfer of data outside the UK
- retaining and storing personal information
- our control around online activity including the use of cookies.

1.2 Administration of an Individual's Rights

The rights are covered in detail in the privacy notice. This section explains how Soha will respond when an individual wishes to exercise a right.

1.2.1 **The right to be informed:** individuals are informed of their rights and how we use their information in our privacy notice which is issued to them at the point where they give us information. Refer to 1.1.1.

1.2.2 **The right of access:** an individual may request their data by submitting a request which initiates a subject access request process. This is administered by the Data Protection Officer (DPO). A log of all requests is maintained and each stage is tracked to ensure adherence to the legislation.

1.2.3 **The right to rectification:** an individual may wish to change part or all their data. This type of request will be dealt with by the relevant business team in line with usual business practice.

- 1.2.4 **The right to erasure:** also known as “the right to be forgotten”; an individual may wish to erase part or all of their data. This is not an absolute right, and we will consider the circumstances of any such request and balance this against our need to continue processing the data, and any legal/regulatory requirements for the data. We will process these types of requests with our “subject erasure request” process. A log of all requests is maintained and each stage is tracked to ensure adherence to the legislation.
- 1.2.5 **The right to restrict processing:** an individual may wish to restrict a process. Requests of this sort will be dealt with by the relevant business team. The individual will be notified if restriction of a process will prevent Soha being able to deliver a service and we may refuse.
- 1.2.6 **The right to object:** an individual may wish to object to how their personal information was collected, what we hold or how we use it. The relevant business team will deal with this type of request in line with usual business practice.
- 1.2.7 **The right to data portability:** an individual may wish to Soha to pass the data it holds to another data controller such as a utility company. This will depend on the nature of the contract we hold with the individual and/or whether there is the need for a data sharing agreement in addition to that contract. The relevant business teams will undertake the requests in line with usual business practice.
- 1.2.8 **Rights in relation to automated decision making and profiling:** an individual can object to a decision being made using an automated process or profiling their information. Soha does not routinely do this. However, it will make every effort to address the request by an alternative method upon request. This will be dealt with by the relevant business team in accordance with their usual business practice. If this is not possible the individual will be provided with a reason.

1.3 Direct Marketing

Soha routinely markets properties for sale. Personal data of potential home buyers is collected with their consent. Only the data of those who go onto to purchase from us is retained under contract. Details of unsuccessful applications may be retained for other schemes when they become available but only with the consent of the individual.

As a social landlord it is in our legitimate interests to communicate with service users about products and services which relate to services we already provide, and to keep users up to date with news and events which meet our objectives around social inclusion and helping to build communities. We will use the most appropriate and preferred contact details to do this. If we need to market something we do not normally do as a landlord; we will obtain consent before we make contact. An individual may withdraw consent where previously given or update their marketing preferences at any time.

1.4 Data Subjects

Employees	Personal data for current and former employees is retained under their employment contract.
Job Applicants	Personal data is obtained via the recruitment process with their consent and disposed of if they are unsuccessful.
Board Members	Personal data for existing Board members is retained for the duration of their office with their consent under a deed of service.
Shareholders	Personal data for shareholders is held under their share certificate.
Leaseholders and Shared Owners	Personal data for current and former leaseholders and shared owners is held under contract in their lease.
Potential Home Buyers	Personal data is obtained via the application process with their consent and disposed of if they are unsuccessful unless they have given us consent to hold it for future schemes.
Tenants	Personal data for current and former tenants is held under contract in their tenancy agreement. Information additional to this may be held for those who receive support or care, and this will be obtained at the point of setting up a plan.
Housing Applicants	Personal data is obtained via the application process with their consent and disposed of if they are unsuccessful.
Contractors and Suppliers (including professionals)	Personal data may be held under their contracts, agreements and letters of instruction.

Part 2: Lawful Processing

- 2.1 Soha sets out its lawful processing in our privacy notice and we comply with the six legal bases stipulated by the UK GDPR.
- We will obtain express consent where we are required to do so.
 - We will only use the personal data supplied to perform under a contract.
 - We will comply with legislation.
 - We will protect the vital interests of a data subject.
 - We will only use the personal data supplied for tasks carried out in the public interest.
 - We will ensure we have a legitimate interest to process and ensure at all times that we work to ensure the fundamental rights and freedom of an individual are protected.
- 2.2 We will comply with the special protection given to certain kinds of personal information that is particularly sensitive. We will only use it where:
- We have a legal obligation to do so (e.g. to protect vulnerable people);
 - In order to protect a vital interest (e.g. in cases of severe and immediate medical need);
 - It is in the substantial public interest;
 - It is necessary for the prevention or detection of crime;
 - It is necessary for insurance purposes; or
 - We have specific consent to use it.
- 2.3 Soha is a social landlord which provides and builds homes. It has a Board and employs staff. Our lawful processing is covered in detail in our privacy notice; both in terms of what we do and what information we may need to undertake it. In summary:
- **We manage the tenancies of the people we house.** The information we need is in relation to housing applicants, our tenants, their household members, and the communities they reside in.
 - **We support our vulnerable customers.** The information we need is in relation to their health and wellbeing.
 - **We provide a leasehold service.** The information we need is in relation to their leases and sublessees.
 - **We sell homes.** The information we need is in relation to the buyers and their ability to purchase.
 - **We are accountable to a Board and shareholding Members.** The information we need is in relation to its membership and shares.
 - **We are an employer.** The information we need is in relation to job applications, management of staff and their personal development and wellbeing.
 - **We must meet our obligations to the housing and financial regulators.** The information we need is in relation to demonstrating our compliance.
 - **We must meet our obligations to our contractors, suppliers and stakeholders.** The information we need is in relation to meeting these obligations.

Part 3: Disclosure

3.1 Information sharing

- 3.1.1 Soha will ensure that personal data is not disclosed to unauthorised third parties. This includes family members, friends, government bodies and in certain circumstances the police. Our employees have been trained to exercise caution when asked to disclose personal data held on an individual to a third party.
- 3.1.2 Where we work with the police, councils and other agencies; we have information sharing agreements in place.
- 3.1.3 Our contractors and suppliers provide services on our behalf and need access to personal data of our residents. We will ensure their data protection status is known before we employ them. This is covered in our procurement processes. A successful contractor will enter into a Data Processing Agreement with us which protects the information we will need to share with them. Older agreements will be reviewed, and a non-disclosure agreement attached.
- 3.1.4 We will only share personal information with our Board and shareholding Members with the individual's written permission, except as is necessary in the course of their duties in which case it will be marked "private and confidential".
- 3.1.5 We may withhold information where it would identify someone else who has not given consent to the disclosure unless it can be edited out (redaction). Joint tenants will be asked if they agree to their data being disclosed to the 'other' tenant if only one makes the request. Otherwise, all the references to the other joint tenant will have to be redacted. There may be other exemptions specifically relating to health information.
- 3.1.6 If there are concerns that the data protection legislation would be breached, a court order requiring the release will be requested and the DPO will advise on this.
- 3.1.7 In order to protect employees and contractors from risk when working in residents' homes, Soha has a system to identify people who may threaten their safety. This information is confidential and will not be disclosed outside Soha. It should be subject to review and be treated in accordance with the record keeping section of this policy.
- 3.1.8 Our privacy notice states who we need to share information with and for what purpose.

3.2 Safeguarding Information

Soha actively works to safeguard children, young people and vulnerable adults from harm. We have a duty to tell Social Services where an individual's safety is at risk and share information with them, whether reported directly or indirectly to staff. This will be undertaken in line with local safeguarding information sharing protocols.

3.3 Exemptions

3.3.1 The legislation allows us to make disclosures without consent in the following circumstances:

- to safeguard national security
- prevention or detection of crime including the apprehension or prosecution of offenders
- assessment or collection of tax duty
- discharge of regulatory duties (including health, safety and welfare of persons at work)
- to prevent serious harm to a third party
- to protect the vital interests of the individual, e.g. emergency medical situations.

3.3.2 We will approach exemptions using a verification framework:

- a) Disclosure must be for one of the reasons in 3.3.1.
- b) The request must be supported by appropriate paperwork to justify the decision.
- c) If we need more information, we will ask for it.
- d) We will check the identity of the person requesting the information.
- e) We will consider whether an investigation will be significantly impeded if we do not release the information.
- f) We will only provide the minimum amount of information to enable them to do their job.

3.3.3 Such disclosures will be specifically authorised by our DPO.

4.1 Information Governance Framework

We are committed to an information governance framework which:

- Defines the data we hold
- Defines our priorities in terms of compliance, integrity, quality, and security of our data
- Encompasses this UK GDPR compliance statement
- Lists the relevant policies and procedures which drive the framework
- Outlines how we will share wider information with others
- Details the performance indicators we will use to measure our success
- Routine reviews and audits as part of the compliance framework
- Overseen by the Chief Executive and regularly reported to the Board and shareholding Members.

4.2 Records and Housekeeping

4.2.1 Data Processing

Soha has listed the processing it undertakes routinely within its privacy notice which also encompasses our fair processing notice(s):

- purpose of the processing
- the various steps involved in the processing
- what data is being processed
- who the data relates to
- where the data is held
- technical and organisational measures taken to secure the data
- how consent is given, and the lawful processing basis used.

4.2.2 Data Security Statement

Our IT Security Policy contains a data security statement which explains how we secure our data.

4.2.3 Data Map

We have mapped all our electronic and manual personal information into a data map. This means we know where all our personal information is held and how it can be safely deleted when it is no longer needed for the purpose for which it was collected. The data map is held and maintained by the DPO. Where a full data protection impact assessment is undertaken the map will be updated accordingly.

4.2.4 Encryption

If we need to share personal information with one of our third parties, it will be protected with suitable encryption software.

4.3 Data Protection Impact Assessment

We will assess the impact to the personal data where:

- We undertake a new project
- We significantly change one of our services
- We introduce or change a strategy
- We introduce or change a policy

- We consider CCTV or other surveillance equipment

Our Data Protection Impact Assessment (DPIA) framework includes guidance, a checklist to determine whether a full impact assessment is required which must be authorised by the DPO and a full impact assessment template which must be authorised by the DPO and may also require a report to the ICO if there is a significant change to our lawful processing. A register of DPIAs is maintained.

4.4 Retention and disposal of data

4.4.1 We will only keep the data we hold for as long as we need it; after which it will be safely deleted.

4.4.2 We have adopted the retention schedule recommended by the National Housing Federation. Within the schedule we have:

- Provided guidance on use of the schedule
- Assigned business owners for each area of record keeping
- Set a retention period for entry in the schedule
- Sign posted the reader on what to do if they need the data longer

4.4.3 There are three processes which work alongside the retention schedule:

- **Annual data review process:** coordinated by the DPO its purpose is to routinely delete anything that has reached its retention period end.
- **Subject erasure process:** administered by the DPO where an individual exercise's their right to be forgotten.
- **Archiving process:** administered by facilities management this will dovetail with both of the above processes to move manual records to safe storage for the duration of their retention period.

4.4.4 We may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. It will remain subject to all the security measures required to safeguard the rights and freedoms of the data subject.

4.4.5 We will dispose of personal data in a way that protects the “rights and freedoms” of data subjects such as shredding, disposal as confidential waste, secure electronic deletion.

4.5 Personal Data Breach

We have a “breach management process” which is activated where we are informed of an alleged breach, or we detect one ourselves. The breach is managed by the DPO. Any employee who suspects a data protection breach must report it immediately commencing with reading the process and completing a breach incident form. Breaches posing a risk to the rights and freedom of data subjects will be reported to the ICO. The highest level of scrutiny will be applied to breaches. Deliberate breaches are considered a serious disciplinary offence and may result in disciplinary action and/or legal action and are covered in our staff code of conduct. We will maintain a log of all breaches and routinely report them to our Board.

Part 5: Surveillance and Audio

- 5.1 The ICO has issued a CCTV Code of Practice 2019. The code was developed to explain the legal requirements operators of surveillance cameras are required to meet under the Data Protection Act 2018 and promote best practice. This code works in connection with the wider framework governing the use of surveillance and recording equipment. Soha will only use equipment of this nature in accordance with the principles set out in this code.
- 5.2 The code of practice covers the use of camera related surveillance equipment including:
- Automatic Number Plate Recognition (ANPR)
 - body worn video (BWV)
 - unmanned aerial systems (UAS)
 - other systems which capture personal information
- 5.3 Soha complies with the twelve principles in relation to the use of surveillance equipment which are:
- 1) Will always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
 - 2) We will assess the impact on the privacy before use of CCTV and ensure its use remains justified.
 - 3) We will ensure notices are on clear display where CCTV is in use with contact details should someone wish to complain.
 - 4) We will ensure footage is held and used responsibly.
 - 5) Our staff will receive the appropriate training.
 - 6) Footage will be held for express purpose for which it was collected and deleted once this purpose is discharged.
 - 7) Access to footage will be subject to the subject access request process or for law enforcement purposes.
 - 8) We will ensure we meet technical and competency standards.
 - 9) Footage will be held securely as with our other electronic data.
 - 10) We will review CCTV use in order to meet legal compliance.
 - 11) We will ensure our policies and procedures are reviewed in relation to CCTV.
 - 12) Any surveillance or recording practice will be subject to scrutiny at the highest level.
- 5.4 Soha has adopted the ICO checklist for use of surveillance and recording equipment.
- 5.5 Soha routinely records telephone conversations for business purposes. We ensure the recording stops if bank details need to be captured. We may also record the environment during an investigation of a noise complaint. In all circumstances advance warning is given and consent is obtained. Audio media files will be checked in relation to an individual exercising one of their rights under the UK GDPR.