

1 Introduction

1.1 This policy is part of SHG's suite of Information Governance (IG) Policies and should be read in conjunction with the wider Information Governance Policy.

1.2 The term 'data subject' refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an identification number (ID), location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

1.3 Personal data is the information by which the data subject may be identified as per in the criteria above. Data subjects (individuals whose personal data is being processed) have a range of specific rights as provided by data protection legislation. This policy sets out how SHG will comply with those rights.

2 Right to be Informed: Privacy Notices

2.1 Data subjects have the right to be informed when and how their personal data is being used by organisations. Compliance with this right is achieved through issuing a privacy policy / notice to describe and explain the processing that is taking place.

2.2 SHG has a Privacy Policy available to all stakeholders on its website [here](#). This provides a broad overview of how SHG processes personal data lawfully, fairly, and transparently.

2.3 This will be kept up to date¹ as SHG and service delivery functions change and evolve. In some instances, data subjects shall be provided with a more specific privacy notice relating to the processing which is taking place.

2.4 Where data subjects do not have access to the internet a copy of the Privacy Policy can be made available upon request and free of charge. This document can be provided by staff within a reasonable time of receiving the request. Documents can be provided in the most suitable format required upon request.

2.5 Teams processing personal data are responsible for the issuing of privacy notices to comply with the right to be informed. These notices should be more specific and relevant to the processing activity and can be issued verbally or in writing. A privacy notice must be concise, transparent, intelligible, and accessible. Further guidance can be obtained from the Assurance Team.

2.6 The most effective and efficient method of delivering privacy notices is through a 'layered approach'. This is where several short information notices are issued to data subjects to avoid one large mass of overwhelming information. SHGs Privacy Policy acts as the overarching layer of the information that is provided to data subjects.

¹ The Assurance Team will ensure that this Policy remains up to date

2.7 Subsequent privacy notices created by teams then act as more detailed and specific layers of privacy information however they need not be overly complex or onerous. A guidance template is below:

- SHG is collecting this information in order to provide a service to you.
- The data will not be shared with any other companies / agencies unless there is a legal reason to do so.
- The data will be stored in line with our retention policies and kept secure at all times.
- More information, including your individual rights, can be found in the Stockport Homes' Privacy Notice which is available [here](#)
- Should you require a paper copy, please ask a member of staff.

3 Right to Access: Subject Access Requests

3.1 A data subject has the right to make a verbal or written request to understand how an organisation is processing its personal data. The right enables data subjects to obtain a copy of their personal data. This is known as the right to access (subject access request or 'SAR'). These requests are coordinated by the Assurance Team and must be responded to within one calendar month².

3.2 The data subject is entitled to be:

- Informed as to whether any personal data is being processed by SHG
- Given a copy of any personal data held, where possible.

3.3 If data subjects have access to the internet, they can access the Subject Access Request³ page on the website in the first instance. This allows customers to make a request online and be guided through the process, enabling them to submit all of the information required to make their request valid.

3.4 Completion of the Subject Access Request form is not mandatory when submitting a SAR, as any request made to the organisation either verbally or in other written form (this includes social media or online) is accepted as a request. The document aims to simplify the process and maximise efficiency.

3.5 SAR forms completed online are directed to the Assurance Team Inbox, where they are recorded and dealt with. Should a SAR be received by another staff member, they are required to ensure the document is complete and send it to the Assurance Team.

² The time limit should be calculated to start from the day of receipt of the request (whether the day after is a working day or not) until the corresponding calendar date in the next month. If the date (e.g. 31st) does not exist in the next month then work to the last day of that month. E.g. a request received on 30th January will need to be responded to by 28th February.

³ <https://www.stockporthomes.org/about-us/open-and-transparent/access-information/subject-access-request-form/#SAR>

3.6 If there is uncertainty regarding the identity of the person making the request, SHG may ask for more information. This is to ensure that a personal data breach does not occur by providing personal data to a person that is not authorised to receive it. ID requests will be made on a proportionate basis, and only when there is no other way to validate who the person is.

3.7 When a third party is acting on behalf of a data subject, it is necessary to ensure that the ID of both parties has been validated appropriately, and that the data subject has given their written consent to the third party acting on their behalf. Any concerns related to third parties will be escalated to the Head of Assurance.

3.8 Where more information is needed to validate a request, SHG will inform the requestor as soon as possible. The period for responding to the request begins when SHG receive the additional information (the request will be placed on hold in between)⁴.

3.9 Where verification is not received within one month if the request shall be closed. Correspondence with the requestor shall make them aware of their relevant rights and the option to submit a new request.

3.10 All requests should be directed to the Assurance Team where they will be recorded on a SAR register and coordinated / complied with centrally. Requests can be directed to the mailbox: assurance@stockporthomes.org

3.11 Other teams that are required to provide information for the request should do so without undue delay. Timescales will be agreed to ensure SAR deadlines are complied with.

3.12 The Assurance Team will consider whether any exemptions apply or whether any other GDPR / DPA 2018 terms apply. They will also coordinate the release of the information to the requestor in a secure format.

4 Right to Rectification

4.1 Data subjects have the right to have any inaccurate information that is held by an organisation rectified or completed if it is incomplete. An individual can make a request verbally or in writing and the inaccuracy must be amended within one month of receipt of the request.

4.2 This right applies when information held on record is incorrect or misleading as to any matter of fact.

4.3 The right does not apply to information that is a record of a mistake as the information itself is not misleading and the record's sole function is to record the mistake.

⁴ The Data Use and Access Act 2025 provides more information about the "stop the clock" function

- For example, a customer may have been misdiagnosed with an ailment that affected their Disabled Facilities Grant. This information was recorded electronically, and the customer would now like the reference to it deleting. In this case the right would not apply as the customer was given such a diagnosis at that point in time.

4.4 The request can be refused if it is manifestly unfounded, unreasonable, or excessive. This assessment shall consider the frequency of requests and whether they are of a repetitive or debilitating nature.

4.5 All requests for rectification should be dealt with by the relevant staff member using a common-sense approach. More complex requests for rectification should be directed to the Assurance Team where they will be recorded on a register and coordinated / complied with centrally.

5 Right to Erasure

5.1 Data subjects have the right to request the deletion of their personal data. This is often known as the “right to be forgotten”. This is not an absolute right and is only applicable in certain circumstances⁵ and so records are not to be deleted without the request being considered by the Assurance Team and a full assessment made.

5.2 This right is applicable when:

- The personal data is no longer necessary for the purpose it was originally collected / processed for (unless there is a new purpose which enables the information to be retained, e.g. to respond to a court case)
- When the processing is reliant on consent as the lawful basis, and the data subject withdraws that consent
- When the processing is reliant on legitimate interests as the lawful basis, and the data subject objects to the processing, and, there is no overriding legitimate interest
- When the processing is for direct marketing purposes and the individual objects to the processing
- When the processing is deemed to be unlawful
- When the processing is to offer information society services to a child

5.3 Where any of the above apply the data subject has the right to have the relevant pieces of personal data deleted.

5.4 All requests should be directed to the Assurance Team. Request for deletion will be recorded on a register and coordinated / complied with centrally.

⁵ The Head of Assurance will determine whether the circumstances have been met

6 Right to Restrict Processing

6.1 Data subjects have the right to request the restriction or suppression of the processing of their personal data. This is not an absolute right and therefore only applies in certain circumstances⁶.

6.2 Individuals can make the request verbally or in writing and are entitled to receive a response within one month from receipt of the request.

6.3 Data subjects may request the restriction of their processing when:

- The accuracy of the data is being contested
- The data has or is being unlawfully processed and the data subject requests restriction in place of erasure
- SHG no longer require the personal data, but it is needed in order to establish, exercise, or defend a legal claim
- The individual has objected to the processing and SHG are considering whether there is an overriding legitimate interest.

6.4 When an individual makes a request for erasure (as per Section 5asn such as request is refused, it may be the case that the scope of the processing could be instead restricted to ensure it is adequate, relevant, and limited to what is needed. This is a matter which can be discussed and agreed with the requestor.

6.5 All requests should be directed to the Assurance Team where they will be recorded on a register and coordinated / complied with centrally.

7 Right to Data Portability

7.1 Data subjects have the right to have their personal data transported from one IT environment to another in a structured, commonly used, machine-readable format. This is not an absolute right which means it is only applicable in certain circumstances.

7.2 This right is applicable when:

- The lawful basis for processing is consent or for the performance of a contract, and
- The processing is being carried out by automated means (i.e. does not use physical paper files).

7.3 If both of these criteria are met then the right will apply, and data subjects can request for information to be ported. The information that can be ported is limited to the data subjects personal data that the data subject

⁶ The Head of Assurance will determine whether the circumstances have been met

themselves provided (issued to SHG as a Data Controller) and will be ported in a secure manner at all times.

7.4 All requests should be directed to the Assurance Team where they will be recorded on a register and coordinated / complied with centrally.

8 Right to Object

8.1 Data subjects have an absolute right to object to processing that is being carried out for direct marketing purposes. This objection must result in the cessation of that processing activity. Objections to direct marketing shall be directed towards The Assurance Team who will liaise with the Marketing and Communications Team (and any other relevant teams) as required.

8.2 Data subjects may also object, and the organisation will consider the request in full, when the processing is for:

- A task carried out in the public interest
- The exercise of official authority vested in the organisation; or
- The legitimate interests of the organisation (or a third party)

8.3 Any objections should be directed to the Assurance Team where they will be recorded on a register and coordinated / complied with centrally.

9 Rights Related to Automated Decision Making

9.1 Data subjects have the right to not be subject to a decision that is made solely by automated means, including profiling, so long as the decision produces a legal effect. Where relevant, the data subject has the right to obtain human intervention in that decision in place of automated decision making.

9.2 All requests should be directed to the Assurance Team where they will be recorded on a register and coordinated / complied with centrally.

10 Rights to Lodge a Complaint

10.1 Data subjects have the right to make a complaint if they believe their personal data has been mishandled. This could include:

- Failure to respond to a SAR
- Inaccurate or excessive data retention
- Unlawful disclosure or use of personal data
- Failure to uphold data subjects' rights.

10.2 More information on SHG's complaints process is available on the SHG website⁷.

⁷ [Stockport Homes | Complaints - Stockport Homes](#)



Data Subject Rights Policy

10.3 Individuals also have the right to lodge a complaint with the supervisory authority: the Information Commissioners Office (ICO) by visiting: www.ico.org.uk/make-a-complaint/.

11 Internal Controls

1	Version control	Version number will change every three years or at major review	
	Version No.	Date	Change/s and reasons for change
	1	August 2025	Review of existing policy

2	Policy Owner i.e. Director	Director of Corporate Services/Deputy Chief Executive
	Policy Author/s i.e. Head of Service	Head of Assurance
	Approved by/date	Director of Corporate Services/Deputy Chief Executive – 6 th November 2025 – Decision
	Communication	Team Meeting
	Effective Date - the date of sign-off	6 th November 2025
	Next Full Review Date i.e. 3 years after effective date, with an annual light touch review	5 th November 2028 or sooner should there be legislative / regulatory changes in this area.

3	Regulatory Standards	Please list the Consumer, Governance, Viability standards and outcomes this policy meets
	Standard/s	Required outcome
	Legislation	<ul style="list-style-type: none"> • Data Protection Act (DPA) 2018 • UK General Data Protection Regulation (UKGDPR) • Privacy and Electronic Communications Regulation (PECR) 2003 • Freedom of Information Act (FOIA) 2000 • Data Use and Access Act 2025

4	Linked policies/strategies	<ul style="list-style-type: none"> • Information Governance Policy • Privacy Policy • Information Governance Charging Policy • Records Management Policy • Data Incident Procedure • ICT Security Policy • Acceptable Use Policy • Employee Code of Conduct
----------	-----------------------------------	---

5	Equality, diversity and inclusion	<p>Describe how different experiences, characteristics, and approaches were considered during the formulation of the policy, e.g. neurodiversity, age, religion, sex/gender, financial/digital inclusion.</p> <p>Anyone can make requests to access either their own information, or corporate information. There are legislative requirements which relate to information requests and SHG has a Vulnerability Policy which it will utilise to ensure fair access to the request process. Customers will be supported to make requests as required or signposted to other organisations which can provide such support and assistance.</p>
6	Customer/Colleague Voice	<p>Describe how the customer and/or colleague voice shapes and influences the policy and services</p> <p>Customer / colleague voice has not specifically shaped this policy although as noted above, this policy relates to the collection and use of personal data, which can often include sensitive or confidential data. Any feedback received on the policy / working practices will be considered in future policy reviews.</p> <p>There is a customer privacy notice, a colleague privacy notice and a job applicant privacy notice which exist.</p>
7	Risk management	<p>This policy helps to mitigate the following risks identified on the Corporate Risk Register</p> <p>Corporate Risk 2 Stockport Homes is not adequately prepared for a proactive inspection of the Consumer Standards by the Regulator of Social Housing</p> <p>Corporate Risk 3 Stockport Homes does not maintain a strong, positive reputation where stakeholders have trust and confidence in SHG</p> <p>Corporate Risk 7 Stockport Homes does not respond to and learn from complaints effectively and does not listen to the customer voice</p>
8	Performance monitoring	<p>Please list the relevant government TSMs (Tenant Satisfaction Measures)</p> <p>N/A</p>