Title:	**Data Protection Policy**
Person responsible:	Director of Business Improvement
Customer consultation arrangement:	Consultation required? Yes☐ No☒ If no, please explain why: Insufficient scope for customer input
EIA required:	Yes
EIA completed (date):	October 2025
Approved by:	Audit and Risk Committee
Business Strategy Objective	All Themes
Approval date:	October 2025
Links to other key policies:	Artificial Intelligence (AI) Policy, Cyber Security Policy, Document Retention Policy, ICT Policy, Privacy Notices (Customer, Recruitment & Colleague), Social Media Policy, Procurement & Contract Management Strategy (and Functional Instruction Manual).
Review date:	October 2028

Document management

Version	Date amended	Amendments
1	September 2019	First policy to comply with GDPR
2	October 2022	Refresh and advice from The Data Protection People. Data Breach Reporting Procedure and Records Management Policy have also been updated. No longer taking card payments over the phone (payment security). Also, minor drafting amendments following Audit & Risk Committee review.
3	November 2022	Added Procedure for Handling Information Rights Requests
4	July 2025	DPO updated from Head of Governance and Risk to Director of Business Improvement.
5	October 2025	Updated in line with advice from Data Protection People

1. Introduction

1.1 Organisations processing personal data in the UK are required to comply with the UK data protection legislation framework, namely the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data Use and Access Act 2025. Other laws inter-relate with the above, including but not limited to the Privacy and Electronic Communications Regulations (PECR). In addition, various guidelines, codes of practice and case law contribute to data protection legislation.

1.2 The UK GDPR sets out that everyone has the fundamental right to the protection of their personal data. All customers and other individuals (data subjects) for which South Lakes Housing (SLH) holds personal data have a right to expect SLH to process their data fairly and lawfully.

1.3 This Policy describes SLH's approach to complying with its legal responsibilities regarding data protection and how it enables individual rights to be upheld and exercised.

2. Policy Statement

2.1 It is the policy of SLH to comply with all relevant data protection legislation including the UK General Data Protection Regulation, the Data Protection Act 2018, the Data Use and Access Act 2025 and any subsequent amendments.

2.2 SLH will apply the principles of data protection to all our processing of personal data and undertakes to:

- Process personal data lawfully, fairly and transparently
- Process personal data for specific lawful purposes only
- Collect only the minimum personal data needed for those specific lawful purposes
- Ensure the personal data processed is accurate and up to date
- Keep personal data for only as long as is necessary for the purpose
- Ensure personal data is held securely and protected from unauthorised and unlawful processing
- Maintain records of compliance against these principles

2.3 SLH will maintain a suite of policy and procedural documentation setting out how it intends to implement management controls sufficient to ensure legal compliance with Data Protection Legislation and will ensure these documents are reviewed periodically. See Appendix 1 for an inventory of key procedures relating to data protection.

2.4 SLH will ensure all relevant colleagues have received appropriate and sufficient training in the application of the organisation's policies.

2.5 Management will ensure sufficient and appropriate resources are available to ensure the organisation meets its legal obligations in respect to Data Protection Legislation, and the standards it sets through its policies.

2.6 SLH will uphold the rights and freedoms of data subjects conferred by Data Protection Legislation. SLH will ensure those rights and freedoms are appropriately

taken into account in decisions taken and will ensure sufficient controls are in place to assist people who wish to exercise their rights.

3. Scope

3.1 This policy applies to all personal data processed by South Lakes Housing in any format, whether SLH is processing it in the capacity of Data Controller or Data Processor.

3.2 This policy is applicable to all SLH colleagues, board members, involved residents, contractors and third parties who have access to the personal data SLH processes.

4. Roles and Responsibilities

4.1 All colleagues have responsibilities in relation to this policy and certain roles have additional responsibility as follows:

4.2 Chief Executive Officer

4.2.1 The Chief Executive is the accountable officer responsible for the management of the organisation and ensuring appropriate mechanisms are in place to support service delivery and continuity. Protecting data and thus maintaining confidentiality is pivotal to the organisation being able to operate.

4.3 Data Protection Officer

4.3.1 The Data Protection Officer is responsible for monitoring and ensuring compliance with this policy and overseeing the lawful processing of all personal data processed by SLH.

4.3.2 It is the Data Protection Officer's responsibility to fulfil the following tasks set out in the UK GDPR Article 39:

- To inform and advise SLH of data protection responsibilities as a controller and processor of personal data
- To monitor compliance with data protection legislation and this policy
- To provide advice where requested on Data Protection Impact Assessments (DPIAs)
- To cooperate with and act as a point of contact for the ICO
- To be the contact point for data subjects with regard to all issues related to the processing of their data

4.3.3 The Data Protection Officer for SLH is John Mansergh, Director of Business Improvement, and can be contacted at governanceteam@southlakeshousing.co.uk / 0300 303 8540.

4.3.4 The Data Protection Officer is also responsible for seeking guidance from the Systems and Change Lead where data security concerns arise and shall provide advice and guidance to the organisation regarding the lawful and appropriate processing of special category data.

4.4 Information Security Officer

4.4.1 The Information Security Officer for SLH is the Systems and Change Lead. They will provide technical support and guidance around the secure and confidential

processing of personal data within the organisation and shall be responsible for addressing any data security concerns.

4.4.2 The Information Security Officer is responsible for providing training to new starters within 3 months of them starting.

4.5 Governance and Risk Manager

The Governance and Risk Manager is responsible for the day to day administration of processes relating to Data Protection, including responding to information rights requests, ensuring appropriate reporting to Board, supporting colleagues to complete DPIAs and maintaining appropriate documentation and registers relating to SLH's Record of Processing Activity (ROPA), Data Sharing/Processing Agreements and Legitimate Interest Assessments.

4.6 Process Owners

4.6.1 Process ownership is assigned to each of SLH's business operations. The Process Owner has primary operational responsibility for compliance with data protection legislation and good practice in respect to processing activities within their area of responsibility.

4.6.2 Process Owners are responsible for understanding what personal data is used in their business area, how it is used, who has access to it and why.

4.6.3 Process Owners may delegate day-to-day responsibility for compliance within their management hierarchies, subject to other People & Culture policies and ensuring that all staff are appropriately trained.

4.7 All Colleagues, Contractors, Involved Residents and Board Members

4.7.1 All colleagues, contractors, and Board Members must:

- Adhere to this policy, associated procedures and data protection legislation
- Only process personal data as authorised and necessary for the completion of their duties.
- Report any actual or suspected non-compliance or concerns regarding the processing of personal data to the Data Protection Officer without delay.
- Attend data protection training as required.
- Report all actual and suspected personal data breaches in accordance with SLH's Personal Data Breach Reporting Procedure.
- Respect data subjects' rights to confidentiality.

5. Policy Detail

5.1 Special Category Data/ Criminal Conviction and Offense Data

5.1.1 Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

5.1.2 Where the processing of special categories of personal data is necessary, the Data Protection Officer shall ensure that the lawful grounds for such processing are documented and shall maintain a periodic review of the necessity to processing the special categories of personal data.

5.1.3 SLH will take appropriate care in processing any personal data relating to criminal convictions and offences. It shall implement suitable measures are in place including identification of the appropriate condition for processing criminal offense data outlined in Schedule 1 of the Data Protection Act 2018. Appropriate policy documentation will be maintained where required.

5.2 Data Protection Principles

5.2.1 SLH will ensure any processing of personal data is carried out in compliance with the Data Protection Principles as detailed below:

5.2.2 **Fairness:** SLH shall ensure personal data is processed fairly and in compliance with legislation at all times.

5.2.3 **Lawfulness:** SLH will ensure there is an applicable lawful basis to facilitate all processing of personal data and special category data.

Where the lawful grounds are legitimate interests, a legitimate interests assessment (LIA) will be undertaken and documented. Where the lawful grounds are a task carried out in the public interest or in the exercise of official authority vested in the organisation, a public interests assessment (PIA) will be undertaken and documented. Where the lawful grounds are a legal obligation, the relevant legislation shall be cited and appropriately documented.

Where the lawful basis is consent or explicit consent the organisation shall ensure the consent is valid and that the data subject is able to withdraw their consent should they choose to. Consent shall not be valid unless:

- there is a genuine choice of whether or not to consent;
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of personal data relating to them;
- the consent was given through statement made by the data subject or by a clear affirmative action undertaken by them;
- SLH can demonstrate that the data subject has been fully informed about the data processing to which they have consented and is able to prove that it has obtained valid consent lawfully; and
- a mechanism is provided to data subjects to enable them to withdraw consent and which makes the withdrawal of consent in effect as easy as it was to give and that the data subject has been informed about how to exercise their right to withdraw consent.

SLH recognises consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject. Where consent is the lawful basis for processing, the Data Protection Officer shall ensure that consent is properly obtained in accordance with the conditions above.

5.2.4 **Transparency**: SLH shall ensure transparency is engrained the processing undertaken. Before any processing of personal data begins, the privacy information provided to data subjects will be considered and will be updated where necessary to ensure it accurately reflects the processing being undertaken.

5.2.5 **Purpose Limitation:** SLH shall ensure personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

5.2.6 **Data Minimisation:** SLH shall ensure personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. SLH will strive to use a minimum of personal data in its data processing activities and will periodically review the relevance of the information that is collects.

5.2.7 **Accuracy:** SLH will use its reasonable endeavours to maintain data as accurate and up-to-date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date.

5.2.8 **Storage Limitation:** SLH will ensure that it does not retain personal data for any longer than is necessary for the purposes for which they were collected and will apply appropriate measures at the end of data's useful life such as erasure or anonymisation.

5.2.9 **Security:** SLH will ensure that any personal data that it processes or commissions the processing of is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. In particular, a Cyber Security Policy will be maintained setting out specific policies in relation to ensuring the confidentiality, availability and integrity of personal data.

5.2.10 **Accountability:** SLH will implement sufficient controls to ensure it is able to demonstrate compliance with the Data Protection Legislation including the keeping of sufficient records of data processing activities, risk assessments and relevant decisions relating to data processing activities.

5.3 Rights

5.3.1 SLH will ensure any processing undertaken does not infringe people's rights and ensure appropriate policies and procedures are in place to effectively manage any individual rights requests.

5.3.2 SLH will take appropriate steps to advise individuals of their rights and to ensure colleagues are able to recognise information rights requests and handle them appropriately when received.

5.3.3 These rights include:

- Right to information about data processing operations
- Right of access to personal data
- Right to portability of personal data
- Right of rectification of personal data
- Right of erasure of personal data
- Right to restriction of processing
- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right of complaint about the organisation's processing of personal data and the right to a judicial remedy and compensation

5.3.4 The Data Protection Officer shall maintain a procedure setting out how information rights requests are to be handled and ensure that all relevant people are made aware of it.

5.4 Personal Data Breaches

5.4.1 SLH will maintain a Personal Data Breach Reporting Procedure and ensure all colleagues and those with access to personal data are aware of it.

5.4.2 All colleagues and individuals with access to personal data for which the organisation is either data controller or processor must report all personal data breaches to an appropriate individual as set out in the Personal Data Breach Reporting Procedure as soon as they become aware of the breach (whether this is actual or suspected).

5.4.3 SLH will log all personal data breaches and will investigate each incident without delay. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data protection near misses will also be recorded and investigated in the same manner as data protection breaches. The Personal Data Breach Reporting Procedure sets out responsibilities, decision-making criteria and timescales for notifying data subjects, the Information Commissioner and the media about a personal data breach.

5.4.4 The Data Protection Officer shall be responsible for maintaining the Personal Data Breach Reporting Procedure and for ensuring that all relevant people are made aware of it.

5.5 Data Sharing and Data Processors

5.5.1 SLH will only share personal data where an appropriate lawful basis has been identified. SLH shall carry out appropriate due diligence and ensure there is an adequate Data Sharing Agreement, Data Processing Agreement or contractual clauses relating to data protection in place prior to any sharing of personal data with third parties.

5.5.2 The Data Protection Officer shall maintain a record of all parties with whom data is shared and all data processors, and is responsible for ensuring that appropriate agreements are in place.

5.6 Restricted Transfers

5.6.1 SLH will only transfer data outside of the UK where it is strictly necessary to do so. Prior to transferring any personal data outside of the UK (referred to as a restricted transfer) SLH will take steps to ensure there are appropriate data transfer mechanisms in place to safeguard the data.

5.7 Children's Data

5.7.1 Special measures will be taken by SLH in the limited instances it processes personal data relating to children under the age of 13. This includes consideration of the nature of privacy information provided and approach to handling information rights requests.

5.8 Data Protection Impact Assessments

5.8.1 SLH will adopt a risk-based approach to processing personal data ensuring it assesses any risks to privacy or to the rights and freedoms of people before commencing, commissioning or changing data processing activities.

5.8.2 Where necessary SLH shall, as a minimum, ensure that a DPIA is undertaken where required by Data Protection Legislation and/or when one is deemed to be desirable by the Data Protection Officer.

5.8.3 The Data Protection Officer shall be responsible for maintaining the SLH's DPIA Procedure and for ensuring that all relevant people are made aware of it.

5.9 Electronic Marketing

5.9.1 Customers can 'opt out' of direct marketing communications from SLH or other third parties e.g., surveys, promotional material, engagement event and research.

5.9.2 Where such material is made by email, text message, telephone, or social media then the rules relating to direct marketing under other regulations (Privacy and Electronic Communications Regulations 2003) will also apply.

5.9.3 Direct marketing should only take place when the person has consented to receiving it. Individuals can contact SLH asking for the processing of direct marketing to cease (without necessarily providing a reason for it). SLH will then cease marketing immediately.

5.9.4 SLH will continue to provide direct contact and materials relating to communications from the landlord in connection with the tenancy (resident annual reports, rent statements, newsletters for example) as this is required fulfil an obligation in connection with the tenancy agreement (e.g. Right to Consultation and Right to Information) and a requirement under the RSH Consumer Standards (communication information about landlord services and performance information).

5.10 Privacy By Design and Default

5.10.1 SLH shall consider privacy by design and by default when processing personal data. Privacy by design and by default is a legal obligation. Privacy by design and by default requires organisations to consider data protection issues at the design stage of the processing and throughout its cycle.

5.11 Training and Awareness

5.11.1 The Information Security Officer will provide training to new starters to the business within 3 months of them starting. Annual e-learning training is provided to all colleagues and is mandated.

5.11.2 SLH will undertake data protection awareness raising activities from time to time to keep data protection front of colleagues minds. All training and awareness raising activities will be logged. Refresher training will be provided periodically.

6. Monitoring & Review

6.1 The Data Protection Officer owns this policy and is responsible for ensuring it is reviewed on a regular basis.

6.2 This policy will be reviewed every three years, or where there have been significant changes to regulation or legislation to warrant a further policy review. The Policy may also be reviewed sooner where there is a need to address operational issues, or where best practice has evolved and there is a need to incorporate this.

Appendix A: Inventory of Key Procedures relating to Data Protection

Procedure	Review Frequency
Acceptable Use Procedure	Every 3 years
Document Management Procedure	Every 3 years
Encryption Procedure	Every 3 years
Bring your own devise (BYOD) Procedure	Every 3 years
Handling Information Rights Requests Procedure	Every 3 years
Personal Data Breach and Near Miss Reporting Procedure	Annual
Guidance for colleagues on the use of Whatsapp	Annual
Photo Consent FAQs for colleagues	Annual
Data Protection Impact Assessment Procedure	Every 3 years