Data Protection & Data Privacy Policy

Title:	Data Protection & Data Privacy Policy
Person Responsible:	Assistant Director (Quality & Performance)
Customer consultation arrangement:	Tenants' Committee
EIA required:	No
EIA Completed (date):	N/A
Approved by:	Audit and Risk Committee
Business Strategy Objective	4. Improving the running of the business
Approval Date:	April 2019
Links to other Policies:	Records Management Policy, ICT Policies.
Review Date:	April 2022

Document management		
Version	**Date amended**	**Amendments**
1		

1. Purpose

This document outlines South Lakes Housing's (SLH) policy for ensuring compliance with the Data Protection Act 2018 which compliments the EU's General Data Protection Regulations (GDPR). The aim of the policy is to outline how we will safeguard personal data under the six data protection principles and rights under GDPR.

This will be achieved by focussing on the following:

- Information governance arrangements
- Collection, handling and use of data
- IT controls and breach management
- Handling data subject access rights

These are set out in more detail under Section 4 and in the supporting documents.

This policy applies to all employees, board directors, volunteers, contractors and processors in handling personal data. These people are responsible for either/or: *collecting, editing, retaining/storing, disclosing (including sharing), deleting/erasing/destroying, viewing (including images), archiving or listening to (audio recording)*.

2. Regulatory and Legislative Requirements

This policy complies with the UK Data Protection Act 2018, which incorporates the EU GDPR.

Other related legislation includes:

- The Human Rights Act 1998 (Right to Privacy)
- The Payment Card Industry Data Security Standard (PCI DSS)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The ePrivacy Regulations 2019

3. General Principles

The overall aim of this policy is to ensure that SLH will comply with six data protection principles and new rights under GDPR.

6 Data Protection Principles – Personal Data shall be;

1. Processed lawfully, fairly and in a **transparent** manner
2. Collected for specified, **explicit** and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Adequate, relevant and limited to what is **necessary** in relation to the purposes for which they are processed
4. **Accurate** and, where necessary, kept up to date
5. Kept in a form which **permits identification** of data subjects for no longer than is necessary for the purposes for which the personal data are processed
6. 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

Individual Rights under GDPR

The right to be informed
The right of access
The right to rectification
The right to erasure (right to be forgotten)
The right to restrict processing
The right to data portability
The right to object
Rights in relation to automated decision making and profiling

4. Data Protection – Our Approach

This divides in to four areas: Information governance arrangements, Collection, handling and use of data, IT controls and breach management and Handling data subject access rights.

4.1 Information governance arrangements

Management of data protection

Information Security is everyone's business, although responsibility resides ultimately with the Chief Executive this responsibility is discharged through the designated roles of Data Controller (SLH the organisation) and the Data Protection Officer.

The Assistant Director (Quality & Performance) is responsible for information risk and data control within SLH and advises the Board on the effectiveness of information risk management across the organisation. SLH is registered with the UK regulator (the Information Commissioner's Officer or ICO) and has a requirement to update the ICO on any changes. The accountable person is the Assistant Director (Quality & Performance) who is also responsible for reporting compliance to the Audit & Risk Committee. The Data Protection Officer is registered with the ICO and reports to the Assistant Director (Quality & Performance) within the SLH organisational structure.

There are a number of accountable people including the:

- Data Controller (DC) – the organisation (SLH)
- Data Protection Officer (DPO)
- Information Security Officer (ISO).

The DPO and ISO provide training, through management teams, for all staff members who handle personal information and ensure access to further guidance and support. The ISO leads on IT controls and the DPO undertakes regular checks to monitor and assess new processing of personal data and to advice on processing and transfer. The DPO is responsible for the management of data security breaches and reporting 'notifiable incidents' to the Information Commissioner's Office (ICO). The ISO also acts as deputy.

Senior Managers are individually responsible for the security of their physical environments where information/data is processed or stored. Furthermore, they are responsible for:

- Ensuring that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures and user obligations applicable to their area of work.
- Ensuring that all staff, permanent, temporary and contractor, are aware of their personal responsibilities for information security.
- Determining the level of access to be granted to specific individuals
- Ensuring staff have appropriate training for the systems they are using.
- Ensuring staff know how to access advice on information security matters

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance, through appropriate training and responsible management. Failure to do so may result in disciplinary action. A GDPR Champions Group, comprising of representatives from operational teams, will provide advice to teams and will lead on implementing this policy within their respective areas.

Wherever SLH asks a third party to carry out a service on its behalf, SLH will need to consider the capacity in which that service provider will process any of personal data. If the expectation is that the service provider will act on the SLH's instructions, when processing SLH's personal data, it will be important to ensure that there is a written contract in place with that third party and to ensure that the data processor can produce a sufficient 'guarantee' as to the adequacy of the security arrangements which they will have in place when processing the SLH's personal data. Security is a key consideration when appointing a data processor.

Tenant Involvement

This policy will be communicated and informed by the SLH Tenants' Committee. SLH will explain in what circumstances personal data is being collected, why it is being used and situations where it is provided to third parties. SLH will also describe situations where consent is used and areas where it is not required. The application of this policy will be subject to Tenant Scrutiny activity. Privacy Impact Assessments (PIA's) will also be made available to the scrutiny panel and available to anyone that requests it.

Data Protection Policy Framework

The policy framework includes a number of supporting documents including:

- *Privacy Impact Assessments* – undertaken when there is a significant service or ICT change.
- *Privacy Notices* – providing information about how data is being used (one for staff which is emailed annually, one for customers published on the SLH website and detailed within Tenancy Agreements).
- *Legitimate Impact Assessment* – SLH may have a compelling justification for processing data which is not part of a performance of a contract and neither has the explicit consent from individuals.
- *Data Sharing Agreements/Register* – completed with all suppliers, contractors and third parties documenting the safeguarding of personal data.
- *Data Breach Incident Reporting Template* – used to investigate data breaches (recorded mostly on the Civica Cx system, except reports to ICO).
- *Data Subject Access Request Templates* – a standard set of letters used to respond to subject access requests.
- *Information Asset Register* – documenting information held including owner, location, data held and security controls.

- *Relevant supporting policies* – including: Records Management Policy, Complaints Policy and ICT Policies.

4.2 Collection, handling and use of data

Purposes of data processing activities

The Information Asset Register will document; the purpose/nature of the collection, owner, location, details of security and specified time limit. The register will document the lawful grounds for processing and will have regard to sensitive personal information. The GDPR Champions Group will ensure that the data is kept up-to-date.

SLH is registered with the ICO (ref ZA007139) and has recorded the following purposes for processing information;

- letting, renting and leasing properties
- administering waiting lists
- carrying out research
- administering housing and property grants
- providing associated welfare services, advice and support
- maintaining our accounts and records
- supporting and managing our employees, agents, and contractors
- using CCTV systems to monitor and collect visual images for the purpose of security and the prevention and detection of crime

SLH processes information relevant to the above reasons/purposes;

- personal details
- goods and services
- supplier details
- financial details
- lifestyle and social circumstances
- complaints
- education and employment details
- health, safety and security details
- visual images, personal appearance and behaviour

SLH process the following sensitive classes of information;

- physical or mental health details
- sexual life
- trade union membership
- offences and alleged offences
- criminal proceedings, outcomes and sentences
- racial or ethnic origin
- religious or other beliefs of a similar nature

SLH processes personal information about;

- tenants
- applicants for accommodation which include their families and households

- asylum seekers
- business associates
- landlords
- employees
- probation officers
- social workers
- spiritual and welfare advisers
- consultants and professional advisers
- survey respondents
- employees including self-employed contractors
- offenders and suspected offenders
- complainants and enquirers
- suppliers and service providers
- people captured by CCTV images

Sources of personal data

SLH needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include tenants, employees (present, past and prospective), suppliers and other business contacts. The information includes names, address, email address, date of birth, private and confidential information, sensitive information or certain types of medical information or other vulnerabilities.

In addition, SLH may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or other digital media, on hardcopy, paper or images, including CCTV) this personal information must be dealt with properly to ensure compliance with current acts and regulations, such as the Data Protection Act (DPA) and the incoming General Data Protection Regulations (GDPR).

The types of sources of information include;

- Housing application form
- Pre-tenancy assessment forms
- Tenancy agreement
- Equality and diversity monitoring forms
- Income and expenditure / financial assessments
- Direct debit forms
- Electronic systems – Cx, handheld devices, computer desktops, databases
- Case notes and opinions on tenant behaviour

SLH also collects other documentation, including;

- Universal Credit and other benefit information
- Proof of income
- Bank statements
- ID and proof of residence documents

- Housing benefit information
- Letters from DWP, Money Advice etc
- Medical letters
- Information for social services, police, health professionals etc

Information processing systems, flows and information assets

Email is used throughout the organisation and confidential information is sent to recipients via encryption utilising 7zip or winrar tools (guidance is available from Service Desk). SLH has an agreement with the Ministry of Justice (Criminal Justice Secure Email Service) service which allows data to be transferred in a secure format to other organisations that are registered. SLH has established a mechanism for logging requests for data portability via the IT Service Desk. They ensure the secure execution of any transfers of data.

All external media devices are defaulted to be blocked with all SLH owned equipment.

Consents

There may be occasions where SLH may wish to re-use personal data for another purpose (where it is not strictly needed for the tenancy or employment reasons) – such as obtaining grant or offering additional services. In these cases, SLH will issue Consent Forms which includes a space for the individual to indicate his or her explicit consent to the processing of the personal data for this new purpose. Consent cannot be assumed (even where it is for their benefit) if there is no response (apart from a 'life or death' situation). Explicit consent will need to be.

Where third parties are involved then SLH will consider the capacity in which that service provider will process any of data and why it is needed. A written contract will need to be in place to ensure that the data processor can produce a significant 'guarantee' as to the adequacy of the security arrangements that they will have in place.

SLH does not allow individuals to obtain or disclose personal data held by SLH without the consent of the organisation. Where this has been obtained without permission (e.g. an employee accessing personal data of a tenant without line manager approval) then the matter will be investigating in line with the Disciplinary Policy and Code of Conduct. As this is also a criminal offence, details will be passed to the Police for investigation. Directors can also be prosecuted if it is due to 'neglect, connivance or consent'.

Guidance can be provided by the DPO or ISO.

Data sharing and use of data processors

SLH is able to share individual personal data with third parties if this is essential to carrying out our legal responsibilities or protecting a tenant from harm. This may include;

- local authorities, the police and other public bodies for the purposes of crime prevention/reduction
- HMRC for the assessment and collection of tax in relation to SLH's employees and contractors, for example for the purposes of repairs to the housing stock
- debt collection agencies and tracing agents, for the purposes of collecting unpaid rent from former tenants who have vacated the property without paying rent due
- Department of Work and Pensions (DWP) and local authorities for the purposes of universal credit claims
- local Safeguarding Authorities, for the purposes of making a safeguarding alert where there is a concern regarding the safety of a child or vulnerable adult

SLH is legally responsible for its own breaches or breaches caused by the actions (or inactions) of data processors.

Personal data passed to other organisations will need to be tightly controlled. SLH will ensure that a Contract will be in place to ensure companies have adequate technical and organisational security measures in place to ensure that the risk of any data breach is minimised. Data Sharing Agreements (for regular sharing) and or appropriate sections in Contracts with external contractors that allow access to the organisation's information systems must be in operation before access is allowed. These agreements/contracts will ensure that the staff or sub-contractors of the external organisation comply with all appropriate SLH security policies. This will include examples including; external researchers, independent tenant advisors, maintenance contractors, debt collection agencies, external auditors and managing agents.

For elected officials covered by the Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 (i.e. MP's and Local Authority Councillors), SLH will check to ensure that they have the implied consent of residents. Where highly sensitive data processing is required (e.g. beliefs/preferences, vulnerabilities, financial commitments, trade union member, safeguarding) then an explicit consent form will need to be signed by the resident. Other forms of elected members (e.g. Town and Parish Councillors) are not covered by the same Order so that a signed consent form will be required from the individual whose data is being shared.

There may be other instances where SLH faces a mandatory legal disclosure e.g. court order, safeguarding of vulnerable people (Care Act 2014), HMRC requirement or to protect national security. There are also discretionary disclosures, including;

- under the Crime and Disorder Act 1998, to provide personal data to public bodies (linked to crime reduction strategies)
- under the Welfare Reform Act 2012 where sharing of personal data for the purposes of universal credit claims are possible
- Disclosures to the Police as part of investigations and SLH will not need to inform data subjects (exempt data protection principal). Subjects would not be able to exercise their 'subject access' right to obtain details of what was

passed to police if this might prejudice the police investigation. Tenants cannot object to this processing
- 'Life and death' situations – for example, providing personal tenant data where a tenant has collapsed and information needs to be relayed to the emergency services.

Whenever data is shared, the following principles will be followed to ensure that the data is;

- accurate
- up-to-date
- not excessive accurate (the company should only be given the data with which they need to undertake a function on behalf of SLH – based upon the principle of '*need to know*')

SLH will establish Data Sharing Agreements and the GDPR Champions Group will maintain a Data Sharing Register.

Data transfer protocols

SLH has adopted a secure data transfer policy which means that data sent electronically should be in the form of Sharepoint links. If other file types such as word, excel and email are to be used then these documents should be password protected and encrypted. Other such software such as 7Zip or WInrar should be used to encrypt documents and the password supplied to the other individual to be sent via another method other than email such as telephone, Skype or in person. Dropbox and other unsecure filing sharing platforms are not permitted as a general rule but can be available in isolated occasions where named individuals can be allowed to use them e.g. for sending photography/large files containing no personal data (along as this is password protected and sent via an alternative email). Service Desk will enable file sharing and then disabled it after use. The employee will sign a disclaimer to ensure that the data that is being shared does not contain personal data.

Data quality & accuracy

SLH operates a Data Quality Policy which ensures that information is maintained accurately. This includes; employees updating personal data and communication preferences on Cx, tenants updating their details on the 'My Account' (portal), updating contact details on survey responses and employees completing annual declarations etc.

This will be monitored by the GDPR Champions Group and subject to compliance audits by the DPO.

Data minimisation

SLH will ensures that data collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance to support data privacy. This means using data that is

- Adequate
- Relevant
- Limited to what is necessary for the purposes for which they are processed.

This will ensure that SLH maintains customer trust and reduces the risk of unauthorised access and other security threats. SLH will ensure the future ICT system developments include GDPR compliance e.g. compliant modules.

Anonymised data

Personal data must relate to a living individual and that living individual must be identifiable from the information. There are situations where the data protection regulations do not apply at the point at which the personal data is anonymised and is therefore no longer personal data. This is used for example, in tenant scrutiny activities where information relating to customer feedback (such as complaints) is anonymised (names, addresses and other personal information that can be linked to the person is removed).

However, it is not always possible in every scenario to guarantee 100% anonymisation. Difficulties arise where there is some degree of risk of re-identification from a set of data. If there is information on the Internet for example, which would allow reidentification of a living individual, then the data may fall within the definition of 'personal data' under the regulations.

Before anonymisation takes place, a Privacy Impact Assessment must be completed. This should include an assessment of;

- the risk of a 'jigsaw' attack i.e. piecing different bits of information together from difference sources (the SLH source, the internet e.g. electoral roll/newspapers, social media e.g. date of birth)
- whether the same code numbers are used in each dataset (the anonymised and non-anonymised)
- other 'linkable' information available in the public domain or easily sourced
- whether the data could be identified through technical measures

Where possible, anonymisation will be applied via the IT system in place to anonymise that data.

Data retention

SLH has a Records Management Policy which sets out the minimum retention periods for each area of the business. It contains details on how information should be securely stored and then appropriately destroyed. The policy is informed by sector best practice including reference to the National Housing Federation.

SLH has a contract with Paper Waste Confidential Business Services to securely shred confidential paper records. This company is accredited with the British Security Industry Association (BSIA) and destroy the contents properly. The company also supplies certification each collection to document the appropriate disposal which is also signed by an SLH employee. Shredding devices are used in

satellite offices which conform to the required standards. SLH will ensure that any future contracts comply with the security standards and affiliated with BSIA.

4.3 IT controls and breach management

ICT Policy

The ICT Policy details the organisation's policy and internal controls around; access to and acceptable us of IT systems, information security, clear desk protocols, document management and retention, information classification, use of the internet, wireless communication, use of emails, encryption, use of phones and portable devices.

Cloud Services

SLH operate most IT systems in its own datacentre located at Bridge Mills Business Centre, Kendal but also have other systems which are located in the cloud. The following systems are hosted external to SLH:

- Microsoft SharePoint- This stores the organisations filing system
- Microsoft OneDrive- This works alongside SharePoint to sync such files offline
- Cloud Dialogs Service Connect- Repairs mobile and scheduling sytem
- Microsoft Exchange- Email System
- Microsoft Skype for Business- Instant messaging software
- Mobysoft Rentsense- Prediction of arrears software
- ProcurePlus- Tender system for asset management
- CJSM- Secure Email Function (part of the justice system)
- Survey Monkey – customer and staff survey tool

Physical security of premises

All SLH IT equipment is located in a secure server room which is located in Bridge Mills, Kendal. The server room is secured via ID Card recognition for authorised personnel. This is limited down to only the IT team. If anyone needs to access the room for other purposes such as air conditioning checking, they are occupied by a member of the IT Team. All other access to rooms\offices in Bridge Mills are also operated via ID Card recognition on each door.

Penetration\Vulnerability Testing

SLH perform annual penetration against all external facing IT systems and internal scanning against all equipment\systems located in the internal network. Both tests are performed by an external company who are experts in the field of security testing.

Storage

All storage is operated in NetApp technology using Storage Area Network (SAN). A SAN moves storage off the common user network and reorganises them into an

independent, high performance network. This allows all SLH data/software to be secure without the data being exposed.

Two Factor Authentications (2FA)

Two Factor Authentication (2FA), adds an additional layer to SLH software protection. 2FA creates two layers of authentication when logging into systems (e.g. password plus text message). This involves additional licence costs (as 2FA licence is required per user). The SLH high risk systems (off site exposure and containing personal data) are in the process of being 2FA compliant.

All future ICT system developments and procurement will ensure 2FA compliance.

Payment Card Industry Data Security Standard Compliance (PCI / DSS)

SLH allow customers to make card payments via various methods such as touch tone payments, internet payments and in person transactions using payment card devices. Such transactions must be compliant with the Payment Card Industry Data Security Standards (PCI DSS) including; processing, storing and transmitting cardholder data.

SLH ensures that this is secured with PCI Compliant hosting providers. SLH use Capita to store this information in the cloud. SLH have completed the PCI DSS SAQ A & PCI DSS SAQ B self-assessment questionnaires to the PCI Council for the website and payment card devices. This includes the following processes:

- All staff are trained on the PCI where relevant and the Payment Card Security Awareness & Procedure is given to all staff to sign to make sure card machines are checked daily for any tampering.
- The website is quarterly scanned to be PCI compliant to make sure the redirect to Capita 360 is secure.
- Card receipts are blacked out where the card numbers shows and is immediately placed in the safe by finance staff
- Receipts stored are safely shredded every 6 months by finance staff
- No staff will communicate card details via any messaging services
- Capita 360 provide us with annual AOC's for PCI assurance
- Piranha our website hosting provider annually provides us with written agreements to maintain PCI Compliance such as starter and leavers information.

Formally document Joiners/Movers/Leavers policy

All documents related to staff joining, moving and leaving the organisation are stored within the useful IT section on SharePoint for the manager of the staff member to complete. Once complete, this document is approved by HR and then passed through to the IT Manager to make the necessary access changes.

Disposing of redundant IT equipment

When devices become broken or redundant, IT will drill holes in the hard drives where applicable and then dispose of the remaining parts. The hard drives get kept in the secure server room therefore eliminating any data loss.

Control of access to data

All data is controlled through the IT Service Desk system where staff will request access to data or software and the IT Manager will grant the access once the relevant approval has been given from the manager or owner of that area.

Bring Your Own Device (BYOD)

SLH allows staff to access systems and data on devices not owned by SLH e.g. mobile phone, tablet, laptops. There is a separate policy for BYOD (ICTP021 Mobile Phone Policy) which ensures that the staff member must obtain approval from their line manager, IT Manager and Director. The maximum amount of email storage is two months.

Use of portable media

All portable media is recommended not to be used in the organisation. All devices such as USB drives and CD's are blocked if staff try to plug them into devices. If data devices are required then this is available through the IT Service Desk.

Disaster recovery and business continuity

The SLH Business Continuity Plan (BCP) and Disaster Recovery (DR) systems are reviewed annually. The BCP acts as a general framework for guiding decision making rather than containing a contemporaneous account of how SLH will respond to a specific incident, including use in the loss of data or security incident.

Security incidents and breach management

Investigations are conducted in line with the SLH Data Protection Incident Reporting Procedure. This also includes '*near miss*' reporting. Investigations are conducted using the approved Data Breach Reporting Template and completed within 24 hours where this involves personal identifiable information.

Incidents that are 'notifiable' are required to be reported to the ICO within 72 hours of the organisation becoming aware of it. The DPO is responsible for reporting breaches but may wish to involve the Assistant Director (Quality & Performance), if available, to obtain a 'second opinion'. Further detail about the data breach procedure and reporting form is included in a separate procedure.

The test for a notifying the ICO includes an impact assessment on the actual or potential effects on the individuals concerned, including

- *Emotional distress* (e.g. risk of increases in anxiety and other mental health conditions)
- *Physical damage* (e.g. risk of identity stolen or vulnerabilities exploited)
- *Financial damage* (e.g. risk of money being stolen)

SLH will undertake a risk assessment to assess whether there has been 'significant' actual or potential detriment as a result of the breach, whether because of the volume of data, its sensitivity or a combination of the two. SLH will have regard to the advice contained on the ICO website and European Protection Board Guidelines regarding reporting 'thresholds'.

4.4 Handling data subject access requests

Right to information and transparency

Individuals will have the right to information to be supplied within 30 calendar days. This includes;

- Contact details of the data controller and DPO
- Purpose of the processing and the lawful basis for the processing
- Legitimate interests of the controller or third party
- Categories of personal data
- Any recipients or categories of recipients of the personal data
- Details of transfers to third country and safeguards
- Retention periods and criteria
- The existence of each of the data subjects' rights
- The right to withdraw consent at any time (where relevant)
- The right to lodge a complaint with a supervisory authority
- The source of the personal data originates from and whether it came from publicly accessible sources
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation
- The existence of automated decision making, including profiling and information about how decisions are made

Right of access

Data subjects have the right to make a request in writing (including via email, social media, webchat) to obtain a copy of all of their personal data or to find out how the personal data is being processed and what third parties it is being shared with. This is called a '*subject access request*'. SLH has developed a suite of Standards Letters covering how requests will be acknowledged, verified, released or refused.

SLH provides no charge for this service and will respond, supplying the information requested, within 30 calendar days of the date of receipt of the request. If further information is required from the data subject (e.g. timeline of data requested, what information is wanted) then the 30 day 'clock' would then start upon receipt of this further information.

SLH will accept 'subject access requests' from third parties where, there is evidence of signed authority from the person in question authorising the third party to seek the

information on their behalf (and this is then checked with the data subject before information is processed and shared). Where there is doubt about mental capacity then SLH will request an original or certified copy of a power of attorney or Court of Protection Deputyship Order which clearly provides authority for the third party to make such a request on the subjects' behalf.

There may also be situations where SLH wish to withhold certain personal data e.g. 'legal professional privilege' which protects the communications between lawyer and client Legal advice should be sought if there are any areas which SLH wishes to withhold (this must be done within the 30-day target period).

Disclosures to the Police as part of investigations and SLH will not need to inform data subjects (exempt data protection principal). Subjects would not be able to exercise their 'subject access' right to obtain details of what was passed to police if this might prejudice the police investigation. Tenants cannot object to this processing.

Data Subject Access Requests will be investigated by the DPO or ISO and logged on Civica Cx.

Right to object to processing (the right to say 'no and stop')

People have the right to object to processing and SLH will log such objections. People can write to explain clearly which particular processing is objected to and why it is causing or likely to cause substantial damage and/or distress to them and why that processing would be unwarranted. Upon receipt of notice (known as a 'section 10 notice'), SLH has 21 days to respond and explain whether they agree with the objection and if so, set out what steps that are going to be taken to comply with the request within a reasonable time.

If the personal data collected is for legitimate and lawful interests (checked against the Data Purposes Register) then the rights of the data subjects may be overridden. The following examples are legitimate reasons to decline a request;

- personal data that is essential to the granting and continuation of the tenancy and/or essential to enable SLH fulfil their obligations in relation to the continuation of the tenancy
- personal data processed by SLH to protect a tenant's 'vital interests'(i.e. a life/death matter), or
- personal data which SLH must process in accordance with a legal requirement.

Where the processing of a tenant's personal data is based upon the tenant's consent, the tenant may withdraw their consent if at any point afterwards they object to the processing.

Right to object to direct marketing

People can 'opt out' of direct marketing communications from SLH or other third parties e.g. surveys, promotional material, engagement event and research. 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. The 2019 ePrivacy Regulations also apply to cookies, opt-outs and online services and prevents the communication of direct marketing to recipients.

Direct marketing should only take place when the person has consented to receiving it. Individuals can write to SLH asking for the processing of direct marketing to cease (without necessarily providing a reason for it). SLH will then stop within a reasonable time (the ICO recommends electronic marketing to stop within 28 days and postal marketing within 2 months).

SLH will continue to provide direct marketing material relating to communications from the landlord in connection with the tenancy (tenant annual reports, rent statements, newsletters for example) as they will fulfil an obligation in connection with the tenancy agreement (e.g. Right to Consultation and Right to Information).

Right not to be subject to automated decision making

SLH can use automatic systems to make decisions but people do have the right to require SLH to have the decision reviewed by a human being rather than by a computer.

The Information Asset Register will be tested against automated decision-making rules. Where automated decision-making solutions are in place (e.g. Mobysoft RentSense which is a predictive analytics tool for managing rent arrears and cashflow) then fair processing notices will be created to notify tenants that profiling is currently occurring.

Tenants have the right not to be subject to automated decision making or profiling. SLH will also create log objections to profiling or automated processing and will remove this data from the predictive analytical tools.

Right to data portability

Individuals may request their personal data from SLH's systems and this will be provided in a structured, commonly used and machine readable form e.g. CSV files. This will enables the individual to use the data for other purposes.

The information will be provided free of charge and without undue delay, and within one month.

This can be extended by two months where the request is complex or there have been a number of requests. SLH will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Right to the restriction of processing

SLH will restrict the processing of personal data in the following circumstances;

- Where an individual contests the accuracy of the personal data, SLH will restrict the processing until the accuracy of the personal data has been verified.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and SLH is considering whether the organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If SLH no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

SLH will inform individuals when it decides to lift a restriction on processing.

Right to correction/erasure of data (Right to be forgotten)

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances;

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

SLH will refuse to comply with a request for erasure where the personal data is processed for the following reasons;

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.

SLH will pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is

because a child may not have been fully aware of the risks involved in the processing at the time of consent (Recital 65).

Right to complain

Tenants have the right to complain via the SLH Complaints Policy and Procedures if they feel that SLH has failed to meet any of its duties or obligations under the data protection laws and regulations. The policy will also be utilised for other data subjects, including staff.

People can also complain to the ICO and request an investigation – this should be done when the complainant has not had their complaint resolved to their satisfaction following the SLH Complaints Policy.

People can commence legal proceedings through the Civil Courts for compensation. In these instances, SLH will commission legal advice.

Right to compensation

Where damage or distress has been suffered by the tenant as a result of SLH breaching any requirements of the Data Protection Act or GDPR, the tenant can request compensation. The SLH Complaints Policy contains the policy framework for considering compensation amounts.

The Civil Courts also has the power to make an order requiring landlords to rectify, block, erase or destroy inaccurate data. Tenants and other data subjects can also ask the Courts to consider compensation.

5. Monitoring & Review

Adherence to this policy will be monitored by the SLH Data Protection Team, comprising of the DPO, ISO and Assistant Director (Quality & Performance).

The DPO is responsible for conducting quality assurance audits, conducting data subject access requests and incident reporting. The ISO is responsible for checking and monitoring compliance with IT controls and data transfer.

Data protection performance will form part of the Compliance Report, reported quarterly to the Audit & Risk Committee. This includes reporting on KPIs, including: data breaches, data subject access requests, data sharing agreements and privacy impact assessments. It is also listed on the Strategic Risk Summary report to Board and forms part of the Internal Audit three-year plan.

The SLH Board Chair will be notified of reports to the ICO.

This policy will be reviewed by the Audit & Risk Committee 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.