Information Security Policy

1 Policy information

Date of issue	March 2024
Replacing/Updating	Information Security Policy 2022
Review Date	March 2026
Drafted by	Head of ICT
Contributors	ICT
Responsible Director	Executive Director of Culture & Communications
Circulation List	Available on SharePoint

3 Policy statement

Information, as a critical business asset, must be adequately protected. As users of personal information, South Liverpool Homes and our colleagues are required by law to ensure data is protected. Much of the processed information is confidential to customers, clients and other parties. As such, South Liverpool Homes takes the security of the data entrusted with it seriously. The provisions of this document are the minimum standards that are expected of colleagues and Board and Committee members. This policy details how South Liverpool Homes will protect the information that we hold.

As an organisation, South Liverpool Homes recognises the importance of information security and the need to ensure that policies and procedures that maintain the three essential security components of confidentiality, integrity, and availability are in place and controlled. Under the legislation, South Liverpool Homes must ensure that information and communication technology (ICT) systems (including paper-based systems) are not misused. The information within them is held securely and protected from accidental loss or damage. This document aims to clarify information security issues and define the standards to which staff must work to create a secure working environment.

4 Policy aims

The aims of this policy are to:

- Ensure colleagues, Board and Committee members are aware of their responsibilities and accountability for information security
- Ensure business continuity and minimise business damage by preventing and minimising the impact of information security incidents
- Share information whilst ensuring its protection and that of ICT assets
- Ensure compliance with relevant legislation
- Protect sensitive information from unauthorised disclosure or intelligible interception
- Safeguard the accuracy and completeness of the information and computer software
- Ensure that information and vital services are available to colleagues and customers when required
- Comply with British Standards ISO27001 (information security techniques and management systems requirements) and ISO27002 (code of practice for information security management)

5 Information Security Policy

5.1 Legislation

There are various pieces of legislation governing the use of computers and the information held within them, and legislation that, although not explicitly drafted with computers in mind, applies to the use, transmission or publication of information.

They place obligations on all colleagues, Board and Committee members who use or have access to information and have the facilities to transmit it. Potential liabilities could arise from the misuse of the information held by South Liverpool Homes or its systems, which could result in legal action against South Liverpool Homes and/or individuals. This could include claims for breach of contract, unwanted contracts, increased vulnerability to computer crime, libel, slander, defamation, discrimination claims, bullying and harassment.

5.2 Data subject access request (DSAR)

Under data protection legislation, data subjects have the right of access (DSAR – data subject access request) to personal data relating to them and the right to have inaccurate data corrected or erased. Requests for information should be referred to the Data Protection Officer (Innovation Manager) before taking any action. South Liverpool Homes has a procedure for DSAR's that complies with the legislation.

5.3 Information sharing/exchange of data

South Liverpool Homes has a requirement to share information with key partners and agencies. Such organisations must complete and sign South Liverpool Homes' Information Sharing Protocol document before sharing information. To provide a robust degree of assurance and to minimise the risk of data loss, copies of their information security policy must be obtained and shared with the Data Protection Officer before information will be shared. Information Sharing register can be found on SLH's SharePoint.

Requests of this nature and any other requests from third parties for information about customers, colleagues or other parties with which South Liverpool Homes carry out business should be referred to SLH's registered Data Protection Officer - Innovation Manager.

5.4 Third-Party Risk Framework

Pre-contractual due diligence should be carried out for new contracts to South Liverpool Homes, confirming contracts and agreement include security clauses. Checks should be made by the use of a self-assessment, which will capture the third-parties responsibilities on data management.

Periodic audits are carried out to ensure compliance on security controls which third-party conform to.

Data Protection Impact Assessment should be undertaken on data sensitivity against service criticality.

5.5 Paper records & clear desk

The legislation detailed in section 10 also applies to information in paper records. Information contained within paper records generated and related to South Liverpool Homes' business activities remains the property of South Liverpool Homes.

South Liverpool Homes has guidelines and procedures to manage paper-based information, detailed in the electronic document management handling procedures, summarised below.

Desks, both in the office and working remotely should remain clear of paper-based customer information at all times. At the end of the working day, documents containing customer-related information must be locked away.

As soon as they are not needed, Confidential and Secret classified documents in paper medium must be disposed of using the appropriate disposal bins located in the Parklands office.

Meeting rooms must be cleaned and cleared when leaving, including any papers.

ICT makes checks each month to make sure printers and desks are clear of paper containing sensitive information. Paper will be destroyed using one of the sensitive waste bins in the Parklands office. ICT also makes checks on storage cupboards to confirm they are locked and unable to be accessed without key.

5.6 Clear Screen

Colleagues and contractors must always be aware of their surroundings and ensure that no unauthorised individuals can see or hear sensitive information. All mobile and laptop devices must be locked when unoccupied. Session time-outs of 10 minutes and lockouts are enforced through technical controls for all systems containing information.

All devices containing sensitive information, including mobile devices, shall be configured to automatically lock after a period of inactivity (e.g., screen saver).

The following actions must be taken to ensure the security of information displayed on a computer or device screen:

- Screens must be locked when unattended so that classified information is not displayed, and no access is available to restricted systems.
- Care must be taken that screens are not sited so unauthorised people can easily see the information displayed. Privacy screens can be requested from ICT.
- Users must remain aware of situations where unauthorised people, including visitors, may overlook their screens.
- Cameras or other recording devices (including mobile devices with a camera) must not be used in the vicinity of screens which may display classified information.

5.7 Electronic document management (EDM)

South Liverpool Homes has implemented electronic document management (EDM) system for the processing and storage of the following documents:

- Tenancy – any documents relating to a tenancy
- Property – any documents associated with any of South Liverpool Homes properties
- Application – any documents relating to an application for housing
- Person – any documents relating to customers

Invoices – all invoices from clients are processed by the Finance team. All documents relating to tenancy, property, application and person are processed through the Orchard Housing document management system. Controls and procedures are in place to scan the information immediately and destroy the paper-based copy within one month. Access to electronic documents of a sensitive nature, such as anti-social behaviour cases, is controlled by the relevant user access permissions of Orchard.

Invoices are processed through the eBIS financial document management system and are subject to similar controls outlined in the operating financial procedures.

Documents are retained on both Orchard, E-Bis and Cascade HR for a length of time as outlined in the South Liverpool Homes document retention schedule, which has been developed by the National Housing Federation (NHF) 2018 document retention guidelines.

5.8 Physical security

South Liverpool Homes operate a set of access controls where possible to prevent unauthorised access to its physical assets. Physical barriers are installed to ensure access with the correct authorisation level. These should prevent tailgating i.e. an unauthorised person following an authorised person through the front or side entrances to the Parklands building. This includes monitoring and recording electronic door entry access to Parklands and visual monitoring through CCTV. Physical access to the data centre located on the first floor at Parklands is subject to a different set of access controls. The ICT team monitors the environment within the room on a 24/7 basis. All visitors must be signed in at reception and record details of their identity and date/time of entry and departure using SwipedON. Privacy legislation is displayed during the sign in process.

Third-party visitor access to the secure area must be requested in advance, and an authorised staff member must always supervise such visitors.

All colleagues of secure areas (including visitors) must wear a visible and current ID badge, and be aware to be challenged if ID badge is not on display.

ICT equipment is asset tagged and recorded in the ICT Helpdesk inventory and organisational asset register. Laptop hard drives are encrypted by default.

To mitigate against the risk of unauthorised systems access, we operate a policy of automatic locking of computer screens after ten minutes of inactivity.

USB ports on company laptops are blocked from accessing removable storage to prevent keyloggers and company data transfer.

South Liverpool Homes regard the defacement, destruction, and removal of any hardware, software or electronic files, without the express authority of the Executive Director of Culture & Communications, a violation of this policy that may render current and former employees liable to disciplinary or legal action.

As outlined in the Waste Electrical and Electronic Equipment (WEEE) Disposal Policy, we dispose of any redundant or obsolete equipment via an approved third-party supplier.

5.9 Passwords

- All passwords are to be treated as sensitive and confidential information.
- Any system that handles valuable information must be protected with a password-based access control system.
- Every colleague must use a separate password for each system.
- Each password must have a strong, private, alphanumeric password to be able to access any service. They should be at least 12 characters long.
- The same password may not be used again for at least one year.
- The password for some special identities will not expire. In those cases, the password must be at least 18 characters long.
- It is discouraged to use administrative credentials for non-administrative work. ICT members must have two sets of credentials: one for administrative work and the other for common work.
- Sharing of passwords is forbidden. Password should not be revealed to anyone.
- All passwords will be governed by password lock-out control (3 Times) where possible.
- Whenever a password is deemed to have been compromised, it must be changed immediately. ICT must be informed immediately.
- Digital certificates (encryption) and multiple-factor authentication using smart cards should be used whenever possible for critical applications.
- All users must not use the “Remember Password” feature; it should be manually changed.
- Passwords shall not be stored in any insecure location (e.g., purse, wallet, notepad).

5.10 Systems access

It is a criminal offence for an unauthorised person to attempt to access a system or information within systems or to exceed the computer facilities or privileges granted to them. South Liverpool Homes will prosecute those committing an offence under the Misuse of Computers Act 1990.

The ICT team has a robust set of internal controls and procedures to monitor system access, and levels of system access are subject to regular audits.

Sharing logins and passwords is strictly prohibited and may render employee(s) liable to disciplinary action.

ICT creates uniquely designed accounts to make them identifiable to the employee. Shared accounts are not permitted.

Requests for privileged access to other information will not be granted without written authorisation from a manager or above to the Head of ICT.

Process for new user accounts on how passwords are provided.

All customer data is held in the Orchard Housing database, and access to this is controlled using the mechanisms above. South Liverpool Homes also operate a system of alerts (or user-defined characteristics - UDC's) that enables the early identification of those customers with alternative communication or service requirements.

Access to systems outside the United Kingdom is prevented to lower the risk of unauthorised login attempts. Request for access outside of United Kingdom is through SLH ICT Helpdesk.

User accounts are disabled immediately at the point of employee's termination.

Accounts which have not been used for 90 days are disabled

5.11 Unauthorised software

Only software legally licensed for South Liverpool Homes is installed on ICT equipment. By implementing user administrative rights, the installation of unauthorised software is not possible. Requests for new software installations are managed through internal controls within the ICT Team. All software licenses are managed through an online portal provided by the preferred software supplier, Phoenix Software.

5.12 Network and file-level security

A Ubiquiti UDM Pro protects South Liverpool Homes' network and infrastructure located at Parklands, which is managed internally by the ICT Team. Microsoft Defender secures Computers and servers, and Microsoft security updates are applied via Microsoft Intune. Internet access is controlled through Microsoft Defender, and Microsoft Exchange Online Protection scans all inbound and outbound e-mails. We operate a series of network drives to provide secure access to and share documents. As detailed in the Backup policy, these are backed up overnight to Azure Backup.

South Liverpool Homes has infrastructure based in Microsoft Azure's UK South datacentre. Data is backed up to geo-redundant storage daily.

5.13 Remote access

Contractors and approved partners can access South Liverpool Homes systems remotely through a secure Awingu appliance. To protect organisational assets, remote access is secured by multi-factor authentication. Any user wishing to access the SLH network remotely must have enrolled their smartphone or email address to obtain a 6-digit passcode.

Any South Liverpool Homes issued device used to access company applications, systems, infrastructure, or data must be used only by the authorised colleague or contractor of such device.

If you are in a public space, ensure your sightlines are blocked and do not have a tenant or other confidential conversation. If someone is close to you, assume they can see and hear everything. Connecting directly to a public wireless network that doesn't employ, at minimum, WPA-2 or an equivalent wireless protocol is prohibited.

While working at home, colleagues and applicable contractors should be mindful when visitors are at their property, as visitors could become privy to sensitive information left up on computer screens.

Access is provided to ICT suppliers using a BeyondTrust Privileged Remote Access system. This access is recorded on the appliance to review any changes that have impacted system performance. Recordings are removed after 30 days.

Third-party suppliers who require continuous access to systems, such as the primary partner contractors and out of hours provider, will be continually monitored and subject to regular audit. A signed information sharing protocol exists in all cases, and stored on SharePoint

5.14 Internet

We provide controlled Internet access to all employees. Usage is continuously monitored through the Microsoft Defender. Access to unauthorised or explicit sites is permanently blocked, and requests for access to such sites are reported to the ICT team.

Reasonable personal use of South Liverpool Homes Internet facilities by staff, Board and committee members are permitted. However, we reserve the right to withdraw the facility if excessive misuse is suspected. This may also result in disciplinary action being taken against the employee.

Access to personal email accounts on South Liverpool Homes devices is prohibited. This is to prevent data loss.

5.15 Malware & Software Vulnerabilities

Malware detected on SLH provided laptops are picked up by Microsoft Defender. Malware remediation occurs automatically and any manual intervention is emailed to ICT Helpdesk for assistance in the event malware cannot be removed.

Laptops provided by SLH are covered with ManageEngine Vulnerability software. This software reports all installed software to a central server. Any software deemed to have a vulnerability will be automatically patched between Wednesday and Friday every week. Colleagues will receive requests on their laptops to restart their laptops to force any updates. ICT reviews exception reports on a weekly basis.

The Vulnerability Manager software reports at a high level, which is reported to the Executive Leadership Team within the compliance checks.

ICT meets monthly to discuss any known threats regarding the suite of applications SLH manages and review the Microsoft updates released on the second Tuesday of each month.

5.16 Social media

We operate a few social media sites, such as Facebook and X(Formally known as Twitter). We understand that many of our staff use these sites to communicate with friends and colleagues. We want to empower colleagues to be good ambassadors of our brand and recognise that social media is a route to doing this. If colleagues do choose to post or upload content about South Liverpool Homes on social media sites, the organisation must be reflected positively.

Only the Marketing & Communications Team are permitted to create new social media accounts in the company's name.

Staff publishing confidential corporate information relating to South Liverpool Homes using personal social media accounts may be subject to disciplinary action.

5.17 Wireless access (WiFi) & bring your own device (BYOD)

South Liverpool Homes operate three Ubiquiti wireless networks within Parklands for secure and Guest wireless access. Network traffic across the two devices is constantly monitored. Approved corporate devices that are part of the internal network domain will only be allowed access to the secure network. As such, users of those devices are subject to the various security controls detailed elsewhere in this policy.

The reception area has guest WiFi, which operates separately from the SLH network, and access is gained by the person 'Liking' the SLH Facebook page to gain access. This network is heavily locked down, with the bandwidth restricted.

Colleagues, Board and Committee members, and trusted partners may connect devices to the unsecured wireless network with the provision of a network key.

This is a direct feed out to the Internet and does not touch the internal network, eliminating the risk of compromise.

South Liverpool Homes provides staff with the necessary equipment to carry out their duties. Access to corporate facilities such as e-mail is not permitted on an unsupplied device, commonly known as BYOD (bring your own device). An exception is Board and Committee members who may use their device to access the secure, cloud-based Convene.

5.18 Cloud computing

Cloud computing is defined as running services over the Internet, and can fall into one of two categories, public or private cloud. South Liverpool Homes has access to a private cloud whereby sensitive data can be managed.

The use of a public cloud is not permitted for data that is classified as financial, intellectual or personal. The use of public cloud solutions will require a risk assessment to be undertaken by the Head of ICT.

Servers based within Azure are continually scanned for vulnerabilities using Qualys. This provides

In order to comply with the requirements of the General Data Protection Regulation (GDPR), datacentres for either public or private cloud solutions or products must reside in the United Kingdom.

5.19 E-mail

E-mail messages, mainly when containing customer information, are subject to the provisions of the GDPR and will be treated accordingly.

Outbound and inbound emails are scanned for viruses to protect both the SLH and recipient systems.

Email is not a secure method to transfer data, so it must not be used to send passwords, account numbers, person records without the email being encrypted. Emails received classified as sensitive or confidential are not to be forwarded to external e-mail addresses outside of South Liverpool Homes.

We provide industry strength level encryption for transmitting information relating to customers. South Liverpool Homes also subscribe to a secure e-mail

facility via the Criminal Justice System (CJSM) to facilitate the exchange of information between trusted partners.

The transmitting of any electronic communication containing defamatory or derogatory information or containing offensive language will render an employee liable to disciplinary action. To protect the assets of South Liverpool Homes, all incoming, outgoing, and internal e-mail is recorded using a forensic strength appliance, Cryoserver. In accordance with the Document Retention Policy, archived emails are kept for 72 months.

5.2 Logging and Monitoring

South Liverpool Homes collects & monitors audit logs and alerts on critical events from production systems, applications, databases, servers, message queues, critical services, and user and admin activities. ICT manages the logging solution and Microsoft SIEM tool to collect event information on the systems and activities.

Logs are securely stored and archived for at least one year to assist with potential forensic efforts.

Relevant team members have access to logs for troubleshooting, auditing, and capacity planning activities. System and user activity logs may also be used to assess the causes of incidents and problems. ICT uses access control to prevent unauthorized access, deletion, or tampering with logging facilities and log information.

When events and alerts are generated from monitoring solutions and mechanisms, ICT correlates those events and alerts across all sources to identify root causes and formally declare incidents, as necessary, by the Security Incident Response Policy.

Additionally, SLH utilises threat detection solution(s) to actively monitor and alert network and application-based threats.

5.3 Phishing Emails

In improving colleague awareness of the threat to the business via suspicious emails, ICT runs a regular phishing campaign. This is a targeted email to specific departments or the whole business on a monthly basis. The emails portray to be suspicious, but if a colleague is to open, it would present online training to be completed to increase awareness to avoid and report future suspicious emails.

5.4 Vendor Management

South Liverpool Homes requires a vendor security assessment before third-party products or services are used, confirming that the provider can maintain appropriate security and privacy controls. The review may include gathering applicable compliance audits (SOC 1, SOC 2, PCI DSS, CyberEssentials, ISO 27001, etc.) or other security compliance evidence. Agreements will be updated and amended as necessary when business, laws, and regulatory requirements change.

Provisions

The contract that exists with each supplier and the goods or services provided will generally determine the information security requirements.

However, the following will generally apply.

- A written contract that may be an addition to the primary commercial contract or part of it must expressly state the information security requirements and controls.
- Where a more detailed level of control over secrecy is required, several non-disclosure agreements must be implemented.

- Before contracts are agreed upon, new suppliers must be selected and approved using the proper due diligence.
- It is crucial to comprehend and, if necessary, enhance the information security policies in place at current suppliers (where due diligence was not carried out as part of initial selection).
- Suppliers must use authorised remote access techniques that adhere to our information security regulations.
- Wherever possible, access to SLH information must be restricted in accordance with business needs.
- Less privilege, segregation of roles, and defence in depth are fundamental information security principles that must be followed.
- In order to deliver goods or services to SLH, the supplier will be required to exercise adequate control over the information security policies and practises followed by subcontractors.
- South Liverpool Homes will have the right to examine the supplier's and, if necessary, the subcontractor's information security procedures.
- A Supplier self-assessment must be used to establish incident management and backup plans.
- Both parties to the agreement will conduct security awareness training based on the established processes and procedures.

5.5 Reporting a Breach

Under the GDPR, SLH will have an obligation to report serious data protection breaches to the Information Commissioner's Office (ICO). However, please refer to the 'Breach Reporting Procedure' in all instances. Breaches of a more severe nature may invoke Business Continuity Planning.

6 Customer Standards & Performance Monitoring

By implementing this policy (and associated policies) and the robust controls and procedures that are in place, South Liverpool Homes can effectively manage its systems and incorporate information. A reporting mechanism and procedure also exists for instances of security breaches, and these are reported quarterly to Audit & Risk Committee.

7 Auditing and Compliance Checking

SLH will undertake or commission as appropriate internal and/or external audit of the Information Security Policy at least on a bi-annual basis and make any revisions as required to any processes falling under the scope of the Policy.

Compliance checking is the only way to provide assurance that policies are being followed and that understanding has been gained. To this end, SLH will conduct a regular programme of IT compliance checks. These may include a physical compliance check of a specific area or an electronic audit of the usage of systems.

8 Information Asset Register

To ensure compliance with the GDPR, SLH will maintain an accurate and up to date Information Asset Register.

9 Information Risk Management

SLH will apply a risk assessment process to any significant decisions it is considering that affect the data it is processing (e.g. changing supplier or primary platform functionality).

Where appropriate, it will carry out a Data Privacy Impact Assessment (DPIA) of that processing activity. SLH will also maintain a log of all completed DPIAs.

10 Training and support

SLH will implement processes and procedures to enable staff to confidently handle and process data using the systems and network in place. In practice this will mean;

Ensuring that appropriate training is accessible and available

- Ensuring staff have access and passwords for the systems they must use to complete their duties.
- Providing support in the form of a management structure and advice network (namely IT helpdesk and a selection of policies and procedures specialising in specific criteria).

11 Statutory and Legislative Framework

The following applies to this policy:

Protection of Children Act 1978: Criminal Justice Act 1988
Data Protection Act 2018
General Data Protection Regulations 2018
The Copyright, Designs and Patents Act 1988
Communications Act 2003
Obscene Publications Act 1959
Digital Economy Act 2010
Electronic Communications Act 2000
Malicious Communications Act 1988
Privacy & electronic communications regulations 2003
Computers Misuse Act 1990
Waste Electronic and Electrical Equipment Regulations 2013