SOUTHSIDE
housing association

SHA IT Policy

Issued: September 2022

Next Review Date: September 2025

1.0 Scope

1.1 This policy applies to all System Users. System Users are staff, volunteers (including Management Committee members), casual workers, agency staff, students, trainees, contractors and Consultants accessing any Southside Housing Association IT systems, servers or applications or using any Southside Housing Association devices.

1.2 This policy replaces and combines the previous IT Password and Security Policy and the Email and Internet Policy. It refers to:

- All Email and Internet resources at the Association, irrespective of where that email use takes place: on association premises, while working off site, while travelling for business or while working from home.
- Use of SHA email on any device, no matter whether owned by the association or employee
- User ID and Password Protocols

2.0 New Starts/System Users

2.1 New starts are initiated by submitting a New Start Form, **APPENDIX 1**, to the IT & Digital Manager, who will make necessary arrangements to set up a new system user

2.2 This information should be provided at the earliest opportunity, for example, when an appointment is made.

3.0 Email

3.1 Any person (System User) who uses Southside Housing Association email facilities consents to all of the provisions of this policy and agrees to comply with all of its terms and conditions and with all applicable laws and regulations.

3.2 Any user of the email system, whose actions violate this policy, or any other Southside Housing Association policy or regulation, may be subject to limitations or elimination of email or internet privileges as well as disciplinary actions.

3.3 The policy aims to establish basic guidelines for appropriate use of the resources and ensure that use of email among Southside Housing

Association system users is consistent with its own internal policies, all applicable laws, and the individual user's job responsibilities.

3.4 The policy also aims to establish basic guidelines for appropriate use of the resources.

3.5 Email is used as a standard form of communication and the association makes email available to all system users where it is relevant and useful for their roles. This policy describes the rules surrounding email use at the association. It also details how system users are expected to conduct themselves whist using email.

3.6 Only those who have been authorised to use email at SHA may do so. Authorisation is provided by an employee’s line manager or the IT department. It is typically granted when a new employee joins the company and is assigned their login details for the associations IT systems. Unauthorised use of the associations email system is prohibited. Employees who use association email without Authorisation or who provide access to unauthorised people may have disciplinary action taken against them.

3.7 Occasional and incidental personal communications using email are not disallowed by this policy and are permitted so long as this does not interfere with the performance of expected duties.

3.8 Used inappropriately, email can be a source of security problems for the company. Users of the Association email system must not:

- Open email attachments from unknown sources, in case they contain a virus, Trojan, spyware, ransomware or other malware.
- Forward any suspicious emails to our IT support desk using abuse@tecnica.co.uk
- Disable security or email scanning software. These tools are essential to protect from security problems.
- Send confidential company or personal data via email. The IT department can advise on appropriate tools to use instead in line with the GDPR policy.
- Access another user’s company email account without relevant permission. If they require access to a specific message (for instance, while an employee is off sick), they should approach their line manager or the IT department.

3.9 Staff members must always consider the security of the Associations’ systems and data when using email. If required, help and guidance is available from the IT department.

4.0 Proper Use

4.1 The Proper Use Protocol is intended to guide users on the Southside Housing Association's standards and is attached as **APPENDIX 2**

4.2 A manager concerned about a system user's potential breach of Southside Housing Association's Proper Use Protocol (for example, excessive use of email or internet access for personal use) should NOT unilaterally seek to gain access to an user's electronic communications. Instead, the manager should:

- Review whether or not expectations and standards in this area have been well communicated and made clear to the user.
- Pursue direct communication with the user regarding the issue.
- Proceed as one would handle any personnel-related disciplinary action.

4.3 Since Southside Housing Association's resources are being used to create and store files, system users should understand that Southside Housing Association must assign certain individuals responsibility for maintaining, repairing, and further developing those resources. In the normal course of doing their assigned work some individuals, by virtue of their positions within the Association and their specific responsibilities, may have special access privileges to hardware and software and therefore to the content that resides in those resources.

4.4 The Association will strive to protect individual privacy by ensuring that the number of individuals with this level of access is strictly limited and that such individuals are selected for their judgment and ethics, as well as their technical expertise. Such positions, and the individuals who hold them, will be governed through defined responsibilities and procedures. See section 7.0 for "Standards for System Administrators"

4.5 While Southside Housing Association email administrators will not monitor the contents of mail messages as a routine procedure, the Association does reserve the right to inspect, copy, and disclose the contents of electronic mail messages at any time. However, it will do so only when it believes it is appropriate to prevent or correct improper use, satisfy a legal obligation, or ensure proper operation of the electronic mail facilities. Any email administrator or member of staff who believes such actions are necessary must first obtain the approval of the CEO to do so.

5.0 Internet Access and Usage

5.1 The use of the internet is permitted and encouraged where such use promotes the goals and objectives of the association. Staff however must ensure that they use the internet in an acceptable way and do not create unnecessary business risk to the company by their misuse of the internet

5.2 The follow is deemed to be unacceptable use or behavior by staff

- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- Using IT systems to perpetrate any form of fraud, or software, film or music piracy
- Using the internet to send offensive or harassing material to other users
- Downloading software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- Hacking into unauthorised areas
- Publishing defamatory and/or knowingly false material regarding the association, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format
- Revealing confidential information regarding the association in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions
- Introducing any form of malicious software into the corporate network

5.3 The association maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

6.0 Security

6.1 Security, including protection from viruses as well as security of Southside Housing Association’s information, is a concern with both Internet and email use. Access to email and the Internet is restricted to authorised persons. System Users are responsible for the security of their own passwords, which protect against unauthorised access. Regularly changing email passwords is recommended. Refer to **9.0 – use of passwords**

6.2 System Users should keep personal passwords confidential and change passwords on a regular basis. Failure to adhere to this policy jeopardises network security and puts users at risk of potential misuse of the system by other individuals. Network users may be held responsible for all actions taken using their personal network access permissions.

6.3 In a further effort to ensure the security of our systems and the information placed on it by users, the Association has network rules which govern the downloading and uploading of files. Virus detection software is installed on individual workstations and the network and users are responsible for virus checking of downloaded files. If you do not know how to do this or don't fully understand the conventions involved here you should seek advice from your manager or system administrator.

7.0 Standards for system administrators

7.1 System Administrators have specific responsibilities and access capabilities. Because of these special access capabilities they are expected to exercise special care in order to protect the privacy of the individuals whose electronic communications they handle.

7.2 System Administrators shall maintain the following standards:

- Ensure that the postmaster system uses machine headers and machine-generated messages in order to return undeliverable mail.
- Avoid reading message content to the greatest degree possible.
- Inform users of procedures for providing service, and assiduously attempt to respect privacy.
- Inform users and be straightforward if something goes wrong, in order to maintain trust. Keep confidential the content of any message that was inadvertently read in the course of redirecting undeliverable mail.
- Consult with users first if it seems necessary to go beyond machine-generated explanations
- Be informed about and follow the Association policy regarding privacy in electronic communication.
- Advise all users on any restrictions on the size and type of files that may/may not be downloaded

7.3 System administrators have a particular role in determining where on the security versus service continuum their particular mail system resides. They must inform system users of the trade-offs between service and security that exist on their system.

7.4 System administrators will therefore need to take specific actions to ensure, to the greatest degree possible, that the Association policy is followed and that users are informed about the degree of privacy of their communications. The following list of information items will help users be as knowledgeable as possible about the systems that they use. It will also help system administrators manage the issues of email and privacy.

7.5 System Administrators will not routinely examine email content unless there are good reasons to suspect the system is being abused and the rules ignored.

8.0 Protection from viruses and ransomware

8.1 The threat from virus and ransomware is very real and carries a high risk should the association succumb to an attack. The Association will ensure that virus protection software on the network is kept up to date.

8.2 Attacks from viruses and Trojans at best cause a nuisance and at worse can destroy data and systems beyond repair. Ransomware is similar in that it is malicious software which encrypts files and systems until a sum of money has been paid. Given this, it is vital that the Association takes steps to avoid such a problem.

8.3 The main areas where a virus attack would come from are:

- Through the Internet and phishing or spam Email.
- Loading software from e.g. malicious websites, social media, copied software, cloud storage sites
- From using removable media, e.g. USB memory sticks, SD cards

8.4 The only members of staff allowed to install any software are the systems administrators.

8.5 Removable media should ideally be avoided where possible. Removable media should never be plugged into a PC unless you are certain of its source. Hackers while often leave USB drives in car parks or public places which have viruses loaded on to them.

8.6 The Association has virus protection software on PCs and the network which will automatically scan for viruses. If you receive a warning at any time, you must remove the media and contact a system administrator immediately for advice.

9.0 Use of passwords

9.1 The Association is committed to securing all Association information stored or accessed through SHA computers and networks. Access to computer systems is restricted to those employees and nonemployees authorised for such access, and who have been issued appropriate unique user IDs and passwords. SHA considers passwords to be highly confidential.

9.2 The use of passwords protects the Association from unintentional or deliberate access by unauthorised personnel to the Association's computer network, therefore it is important that staff observe the guidance below.

9.3 All employees and managers are responsible for complying with this policy. Any individual attempting to or requesting someone else to circumvent security or administrative access controls is in violation of this policy.

9.4 There are two main areas where passwords are requested.

- When logging into the computer either in the office or remotely
- When logging into 3rd party software and websites

9.5 In addition, when using word processing or spreadsheet files there is an opportunity to protect these by use of a password created by the user. However, this should be avoided. Preferably, the system administrator can be requested to set up a folder with restricted access. Access must be available to more than one member of staff.

9.6 Access to applications is made possible using a user ID and password. User IDs may include the employee's number, company email address or other approved configurations. Nonemployees will be assigned a unique ID number.

9.7 Access may be revoked if any aspect of this policy is violated. Other actions up to and including termination of employment may also be taken, depending on the violation.

9.8 All users of SHA systems and services are required to adhere to the following rules to use, access, store, process and/or display data acquired from company-owned applications and systems. In addition, contractors and their associated employees and agents must adhere to and agree with the following rules:

- Access to SHA owned applications and systems is granted solely to conduct legitimate business on behalf of the company.
- Access to specific system functions and data resources is consistent with each user's scope of employment and job responsibilities.
- Access requests, including user IDs and passwords, are initiated by written request from company business unit managers who have knowledge about their users' legitimate need to access/change data.
- Access requests for department users must be approved by applicable company department personnel.
- User accounts will remain active until a user's employment relationship either changes or terminates, or a period of nonuse is exceeded.
- All contractors and their associated employees and agents must read, agree and sign the appropriate forms before access to SHA networks and/or systems is permitted, and must adhere to the policies set forth in this document.
- All requests for new access, changes to existing access or termination of access must be submitted to IT with department management approvals and justifications if needed.
- SHA’s managed service provider’s (Tecnica Ltd) helpdesk shall be contacted with all requests for access activities, e.g., user ID and/or password requests and/or changes. The MSP will require authorization from SHA’s internal IT department before making such changes

9.9 All employees and managers are responsible for complying with this policy. Any individual attempting to or requesting someone else to circumvent security or administrative access controls is in violation of this policy.

10.0 Logging into the network

10.1 When user accounts are set up, the Systems Administrator will initially generate the passwords for staff. After this, staff will be asked when they log on, to change their password to one of their choice.

10.2 The new password must be at least 8 characters long, be a combination of alphanumeric characters, numbers and symbols, and should not be easily guessed. Examples of passwords that are not acceptable include user ID, dictionary words, first or last name of user, family member, city, town, street, etc.

10.3 You will be asked to change your password once every 60 days, and a reminder will come up on the screen. SHA will force password changes at least every 60 days on systems accessing sensitive business information.

10.4 You should note that the Administrator will not know your password, only you. The Administrator can only delete your password completely, before allowing you to change to a new one.

10.5 User IDs and passwords or open computer application sessions should not be shared, except on shared workstations.

10.8 Alternate authentication technologies, e.g., biometrics or proximity cards, may be used in place of password protections where applicable

10.9 Users will be locked out of the system after 3 failed login attempts and must contact the system administrator for access resetting. Failed login attempts may be recorded and reviewed for follow-up action.

11.0 Access Control

11.1 All users of SHA systems and services including contractors and their associated employees and agents, are required to adhere to the following rules within the Password and Security policy to use, access, store, process and/or display data acquired from company-owned applications and systems. In summary the Password and Security enforces the following rules:

- Access to SHA owned applications and systems is granted solely to conduct legitimate business on behalf of the company.
- Access to specific system functions and data resources is consistent with each user's scope of employment and job responsibilities.
- Access requests, including user IDs and passwords, are initiated by written request from association managers who have knowledge about their users' legitimate need to access/change data.

11.2 User accounts will remain active until a user's employment relationship either changes or terminates, or a period of nonuse is exceeded. This is usually three months.

11.3 All contractors and their associated employees and agents must read, agree and sign the appropriate forms before access to SHA networks and/or systems is permitted, and must adhere to the policies set forth in this document. **Appendix 3 - Contractor and associated agents IT policy agreement**

11.4 All requests for new access, changes to existing access or termination of access must be submitted to IT with department management approvals and justifications if needed.

11.5 The Association's managed service provider's (Tecnica Ltd) helpdesk shall be contacted with all requests for access activities, e.g., user ID and/or password requests and/or changes. The MSP will require authorisation from SHA's internal IT department before making such changes

Appendix 1

New start IT setup

Personal Details

Start Date	
First Name	
Surname	
Preferred name (if different)	
Personal email address	
Preferred SHA email address	@southside-ha.co.uk

Role

Job Title	
Department	
Copy access from (if applicable)	
Additional Information for email signature (e.g. PT work pattern)	

Server Access

Do they require access to the RDS server?	Yes / No
Mobile number (for Duo MFA)	
Mobile type	Android / IPhone

Equipment required

Laptop / Chromebook	
Tablet	
Mobile Phone	

Additional notes

Manager Approval

Print Name		Date:
Sign		

Email to emacdonal@southside-ha.co.uk

APPENDIX 2

Proper Use Protocol

- Users should be familiar with general housekeeping good practice (e.g. the need to delete Email messages regularly)
- Emails or attachments must not be sent containing personal or association data in line with GDPR laws.
- Users should use appropriate etiquette when writing Email messages; the use of capital letters, for example, is considered to be the equivalent of SHOUTING
- Inappropriate messages are prohibited including those which are sexually harassing or offensive to others on the grounds of age, physical ability, race, religion or gender
- If you are the recipient of such messages you should raise your concerns with your manager immediately
- You also have the right to raise a grievance should you receive offensive Email or be concerned over a colleague’s general use of the Internet/Email resources
- Users should not send potentially defamatory Email messages which criticise other individuals or organisations
- Users should not access or download inappropriate material, such as pornography, from the Internet
- Users should take care not to infringe copyright when downloading material or forwarding it to others
- Users should not email for any Illegal or criminal activates
- Users should not use SHA email accounts for personal shopping or access to online services
- Users should not share access or passwords to their SHA email accounts.
- Passwords should never been written down
- The same password should not be used for different systems
- Users should report any suspicious emails or activity to the IT department

- No email should be sent which could be considered as spam.

  Spam is broadly defined as unsolicited, Email sent to a large number of recipients, and its content is not Southside Housing Association business related. Southside Housing Association's Email accounts are not allowed to be used for the purpose of sending SPAM messages. Not only is this a misuse of Southside Housing Association resources, but it can also result in external sites "black listing" the Southside Housing Association, prohibiting delivery of any future Emails to our location.

Some people will send an angry Email message; one that they would never say in person. Take a minute before you enter an Email message. Be careful about what words you use and how you say them. Remember that messages can be printed or forwarded. Do not say things you will regret later.

Example of improper use

Southside Housing Association provides email facilities to support its communication, learning and service activities and associated administrative functions. Any use of the facilities that interferes with these activities and functions or does not respect the image and reputation of the Southside Housing Association is therefore improper.

In general, policies and regulations that apply to other forms of communications at the Southside Housing Association also apply to email.
In addition, the following specific actions and use of email are improper:

- Alteration of source or destination addresses of Email.
- Use of Email facilities for commercial or private business purposes.
- Use of Email, which unreasonably interferes with or threatens other individuals.
- Use of Email that degrades or demeans other individuals – whether Southside Housing Association employees or others
- Commercial use - any form of commercial use of the Internet is prohibited.
- Solicitation **-** the purchase or sale of personal items through advertising on the Internet is prohibited.
- Harassment **-** the use of the Internet to harass employees, vendors, customers, and others is prohibited.
- Political **-** the use of the Internet for political purposes is prohibited.

- Misinformation/Confidential Information **-** the release of untrue, distorted, or confidential information regarding Southside Housing Association business is prohibited.

- Viewing/Downloading purely entertainment sites or material where there is no benefit to Southside Housing Association in terms of its learning, communication or service aims described earlier.

APPENDIX 3

Contractor and associated agents IT policy agreement

I have read and understood the content and requirements of the Southside Housing Association's IT Policy. I have received a copy of the policy and agree to abide by the policy guidelines as a condition of my further employment or trade with Southside Housing Association.

Please ensure that you have read and fully understood the policy before signing this document.

CONTRACTOR/ AGENT

COMPANY	
PRINTED NAME	
SIGNATURE	
DATE	

SOUTHSIDE HOUSING ASSOCATION, AUTHORISE BY

PRINTED NAME	
SIGNATURE	
DATE	

This form should be scanned and emailed to emacdonald@southside-ha.co.uk

SOUTHSIDE
housing association

Southside housing Association

T: 0141 422 1112
F: 0141 424 3327
E: enquiries@southside-ha.co.uk

A: Southside House, 135 Fifty Pitches Road, G51 4EB