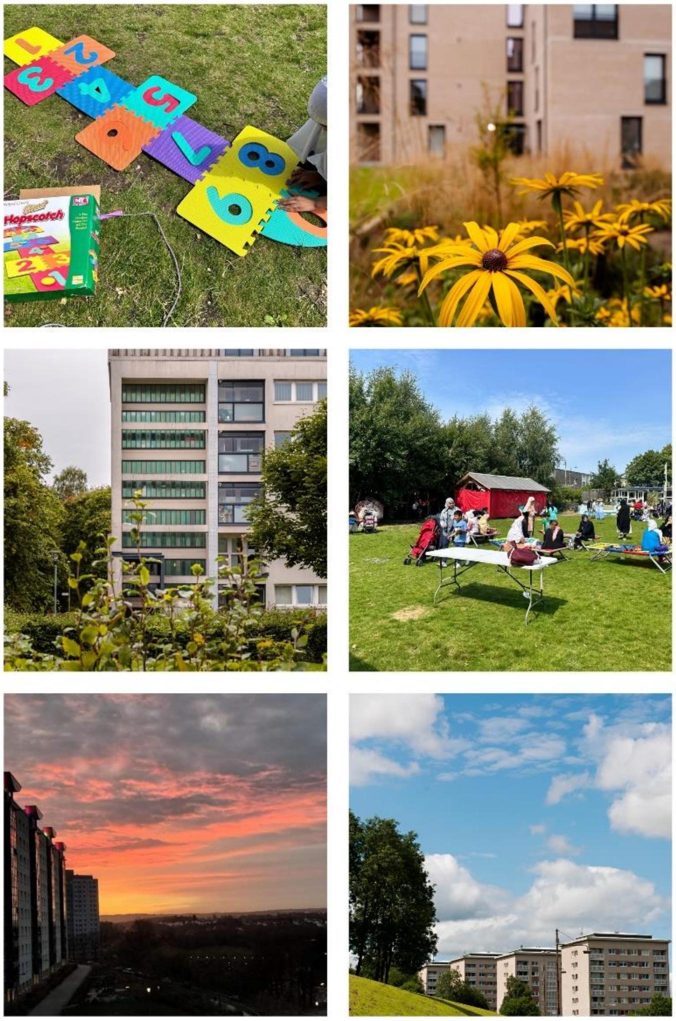


SOUTHSIDE
housing association

SHA IT Policy

Approved by F&CS: 14th November 2024

Next Review Date: every 12 months from issue date

Content

1. Definitions

1.1 Users are anyone who uses a device, software, communication tool, or any other form of IT provided by Southside Housing Association.

1.2 Administrators are those tasked with set up, control of access, email management, Microsoft administration, IT security, password control and so on. Normally these administrators are our IT Team and our Third-Party IT Consultants. From time to time this may be devolved to other people, such as setting up users on software (CPL or Website). Administrator accounts and access will be removed whenever a user no longer requires that access. This will be annually on review of this policy.

1.3 Third-Party IT Consultants are contracted to look after our servers and their security, Microsoft 365 administration, licenses for certain products and support for users. They work in partnership with our IT Team.

1.4 Third-Party Consultants are anyone who has access to our data due to a software contract or access given through Teams.

2. Users and Administrators Roles and Responsibilities

2.1 It is the Users responsibility to ensure that they operate within the protocols, IT Policies and guidance and report any misuse of any device, software, internet or email usage. They will be given training and support to use everything safely and properly. They should never hesitate to ask the IT team or their manager if they are unsure what to do and how to do it. They must ensure they understand the association's Code of Conduct for staff and Data Retention Policy and Data Protection Policy and how these impact on their use of IT.

2.2 It is the Administrators responsibility to keep systems up to date and working within the parameters that keep data safe and secure. They will be responsive to requests from users for support and training and will keep their knowledge and skills sufficiently up to date. They will not use their administrator account to access websites nor download emails. They will work in partnership with other administrators and our Third -Party IT Provider. They will follow all best practice and the requirements necessary to comply with Cyber Essentials Plus and PCI-DSS. They will help to facilitate the good storage of documents and data and will understand the impact of the Associations Data Retention Policy and Data Protection Policy on our IT Policies and Practices.

3. Email, Internet and SharePoint Use

3.1 All users are responsible for using their email, internet and SharePoint access. Everyone should be aware that the use of these communication tools should not be abused.

3.2 Personal use is acceptable as long as it is minimised, used carefully and in the user's own time.

3.3 Users must not use these tools to access any content that is violent, pornographic, racist, or promoting hatred.

3.4 Communications should be undertaken in a professional manner.

3.5 Users should ensure they are not going to bring the Association into disrepute.

3.6 A Users Guide to using Email, Internet and SharePoint Communications is attached in Appendix 1.

3.7 The administrators do not monitor email, internet or SharePoint usage unless asked to by a Leadership Team Member where there is suspected abuse, or if the user is off on a long-term absence and others require access to continue with Southside business.

3.8 All users are given training on Phishing and the consequences of opening spam emails with links that could allow malicious third parties access to Southside's systems. The user is responsible for completing the training and understanding their role in keeping the Association's systems safe.

4. Passwords

4.1 Access to the user's laptop or chrome book, and a number of software applications requires a unique user identification and password.

4.2 User's passwords for Microsoft based systems will expire if not changed within 60 days

4.3 Most passwords are the responsibility of the user to update timeously when prompted and to be kept safe and secure from others.

4.4 Passwords will not be shared with anyone else.

4.5 Passwords must be at least 8 characters. This includes capital letters, numbers and a special character such as !.

4.6 If you require to store passwords, users should speak to the IT department who can advise on password storage online.

4.7 Duo Authentication is used to confirm the identity of users when they use software when passwords are changed, or a new device is being used.

5. New Starts and Leavers

5.1 New Starts are those who have been recruited to permanent or temporary jobs with the Association, volunteers or Management Committee.

5.2 The IT Officer must be given at least 1 weeks' notice of new starts. The information required is in Appendix 2 and is on a form in the SHA Corporate Services Hub.

5.3 New starts who are new posts, should be given at least 3 weeks' notice as a new laptop, phone and other items may be needed. Also, the manager should discuss this with the Information Systems Project Manager as there may be budget implications.

5.4 Leavers are those no longer to be working for Southside whether in a job, voluntary position or a Management Committee Member.

5.5 As much notice as possible should be given. There are security implications if administrators do not stop access to data and software as soon as the person leaves. Administrators will revoke leavers access to all IT systems at the point of their departure.

5.6 After someone leaves it may be a requirement that IT Department set up access to a manager to see email/SharePoint information. It should be requested in writing (usually email).

6. Use of Devices

6.1 Appendix 3 is the Use of Devices Form and will be signed by any user that receives a device from Southside or who uses their own devices to access Southside resources. The form will be held by the IT department and when new or replacement devices.

6.2 Users are responsible for the work device and should use any protective covering or bags that are given out with the device.

6.3 Users must report any broken or damaged devices immediately to the IT Department.

6.4 The IT Department can shut down devices if they are lost, so please inform them as soon as possible if you lose a device.

7. Security

7.1 Southside is Cyber Essential Plus certified and PCI-DSS compliant.

7.2 Working with our Third-Party IT Consultant we have put in place robust security measures on our servers and systems to prevent malicious hacking or sharing of data.

7.3 The Administrators must ensure that the security settings are changed or adapted in line with our compliances.

7.4 Southside users must not attempt to change or interfere with any system security.

7.5 Part of the security is for users to use their knowledge of phishing and scams to ensure they do not click on malicious links or download software that will compromise the system.

7.6 Our Third-Party IT Consultant will scan for vulnerabilities every 3 months and report to the IT Officer anything of concern or threat.

8. Document Storage

8.1 Southside is moving most of its documents to Teams/Sharepoint/OneDrive. Users and Administrators will monitor permissions to ensure that no data is accessed by users or third-party contractors/consultants who do not have permission.

8.2 Users and administrators must not use USB's to bring in or take away documents without first checking with the IT Department that the device is safe. And in general, this use of transferring documents is not encouraged.

8.3 Devices taken into customer homes must not be left unsupervised nor left open in a way that anyone else to see the content unless the content refers directly to the customer.

8.4 Devices taken home must be securely stored and not access by others.

8.5 The use of Dropbox, We Transfer or other third-party software to transfer documents with any personal information is not allowed.

9. Compliance Review

9.1 Disaster Recover: we will review and test the Disaster Recovery Plan for IT every 12 months.

9.2 Cyber Essentials Plus: we will review the Cyber Essentials Plus every 12 months.

9.3 PCI-DSS compliance – we will review the PCI-DSS compliance requirements every12 months.

10 Budgets

10.1 A budget will be set every year to ensure that sufficient funds are available to maintain the IT systems, software and hardware.

10.2 Budget overspend must be reported to the Head of Finance & Corporate Services before the money is spent.

11. Use of Artificial Intelligence (AI)

11.1 The Association allows the use of Co-Pilot, Gemini and Chat GPT to create non-policy content or to help to answer queries around use of software, formulas and so on. In using this content, staff must check that it is unique and not plagiarising others work.

11.2 The use of AI should not include the creation of letters or other public facing documents without ensuring that the content is made Southside specific and uses UK spelling, not US spelling.

11.3 The Association has still to establish a set of ground rules for the use of AI in software and how best to direct staff in its use.

11.4 The use of AI must never breach GDPR or Data Protection legislation.

11.5 The use of AI must never supersede any security protocols.

11.6 To back up this policy, staff will develop a Working with AI Policy and guidance for staff.

12. Disposal, recycling and repurposing Hardware

12.1 Hardware can become obsolete. This does not mean it cannot be used by other organisations, it simply means it is not useable with the software we use or perhaps is no longer regarded as secure under our Cyber Essentials Plus accreditation.

12.2 Any hardware that is obsolete will be stored, wiped of information and a decision will be made by the IT Manager, and the CEO if it can be donated to organisations that fit our charitable purposes or with whom we work in the local community. Southside has a Donations Policy and if it is to be donated this should be the reference. If Southside cannot dispose of hardware this way, then any decision to divert from these or our charitable purpose will be brought to the Management Committee for approval.

12.3 Hardware which cannot be repurposed will be recycled and not disposed of in landfill. There are organisations that will strip hardware of its component parts to ensure as much of the item is recycled.

12.4 Only in extremis, will items be disposed of in landfill. All data will be removed as well as software and anything else that might lead to insecurity of the Association's systems or data.

13. Links to relevant Policies

13.1 This policy should be read in conjunction with the following Southside Housing Associations Policies:

- Code of Conduct (SHA Staff and SHA Governing Body Members)
- Privacy Policy
- Retention Policy
- Social Media Policy (not reviewed since 2015)

13.2 In 2025, the Social Media Policy will be reviewed to take into account changing technologies and methods of communication. A new Artificial Intelligence Policy will be created, as will a Digital Policy. We will also create an IT Security Policy encompassing Device Security.

14. Review

14.1 This policy will be reviewed every 12 months to ensure compliance with Cyber Essentials Plus, PCI-DSS and relevant legislation. It will also be updated to current practice.

Appendix 1:

A Users Guide to using Email, Internet and SharePoint Communications

A. Email

Improving your email communication can make a big difference in how effectively you convey your messages and collaborate with others. Here are some tips to help you enhance your email skills:

1. **Craft Clear Subject Lines**

- Be Specific: Use subject lines that clearly indicate the email's purpose (e.g., "Meeting Agenda for Oct 15" instead of "Meeting").
- Use Keywords: Include important keywords to make it easier for recipients to find the email later.

2. **Structure Your Email**

- Opening: Start with a polite greeting and, if necessary, a brief introduction.
- Body: Organise the content logically. Use short paragraphs, bullet points, or numbered lists to break up text.
- Closing: End with a clear call to action or summary of next steps, followed by a courteous closing (e.g., "Best regards").

3. **Be Concise and Direct**

- Stay on Topic: Stick to the main points and avoid unnecessary details.
- Use Simple Language: Avoid jargon and complex sentences. Aim for clarity and simplicity.

4. **Proofread Before Sending**

- Check for Errors: Look for spelling, grammar, and punctuation mistakes.
- Read Aloud: Reading your email aloud can help you catch awkward phrasing or unclear sentences.

5. **Use Professional Tone**

- Be Polite and Respectful: Even if the email is informal, maintain a level of professionalism.

- Avoid Emotions: Be careful with humour and avoid expressing frustration or anger.

6. **Manage Attachments Wisely**

- Relevant Files Only: Attach only necessary documents and ensure they are correctly named.
- Use Links for Large Files: For large attachments, consider using cloud storage links.

7. **Respond Promptly**

- Timely Replies: Aim to respond to emails within 24 hours, even if it is just to acknowledge receipt and indicate when you will provide a full response.

8. **Use CC and BCC Appropriately**

- CC (Carbon Copy): Use CC to keep others informed without requiring their direct response.
- BCC (Blind Carbon Copy): Use BCC to protect recipients' privacy when emailing a large group.

9. **Use of Southside Signature**

- You should always use your Southside HA signature when starting an email. You do not need to use it in any response to that email.
- The SHA signature should have your name, position, company, and contact details.

10. **Follow Up When Necessary**

- Polite Reminders: If you have not received a response, send a polite follow-up email after a reasonable period.

B. Internet

1. **Reliable Sources**

- Use reputable websites and verify information from multiple sources before sharing.

2. **Privacy**

- Be mindful of privacy settings and avoid sharing sensitive information on public platforms.

3. **Security**

- Use strong passwords and enable two-factor authentication where possible. Be cautious of phishing scams.

4. **Netiquette**

- Follow online etiquette, such as being respectful in forums and avoiding all caps (which can be interpreted as shouting).

C. Posting on Teams channels and Forums

Posting on Teams channels and forums effectively can enhance communication and collaboration within your team. Here are some best practices to follow:

D. Teams Channels

1. **Relevant Channels**:

- Post in the appropriate channel to ensure your message reaches the right audience.

2. Clear and Concise:

- Keep your messages brief and to the point. Use bullet points or numbered lists for clarity.

3. Descriptive Titles:

- Use clear and descriptive titles for your posts to help others understand the topic at a glance.

4. Tagging:

- Use @mentions to tag specific team members or groups to draw their attention to important messages.

5. Threaded Conversations:

- Reply to existing threads instead of starting new ones to keep discussions organised.

6. Files and Links:

- Attach relevant files or links directly in your post for easy access.

7. **Etiquette**:

- Be respectful and professional. Avoid using all caps, which can be interpreted as shouting.

8. **Reactions and Emojis:**

- Use reactions and emojis to acknowledge messages and add a personal touch, but use them sparingly.

E Forums

1. **Search First**:

- Before posting a new question or topic, search the forum to see if it has already been addressed.

2. **Descriptive Titles**:

- Use clear and specific titles to help others understand the content of your post.

3. **Detailed Content:**

- Provide enough detail in your post to help others understand your question or topic. Include relevant context, examples, or screenshots if necessary.

4. **Categories and Tags**:

- Use appropriate categories and tags to make your post easier to find.

5. **Follow Up**:

- Monitor your post for responses and follow up with additional information or thanks as needed.

6. **Be Respectful**:

- Maintain a polite and respectful tone, even if you disagree with others.

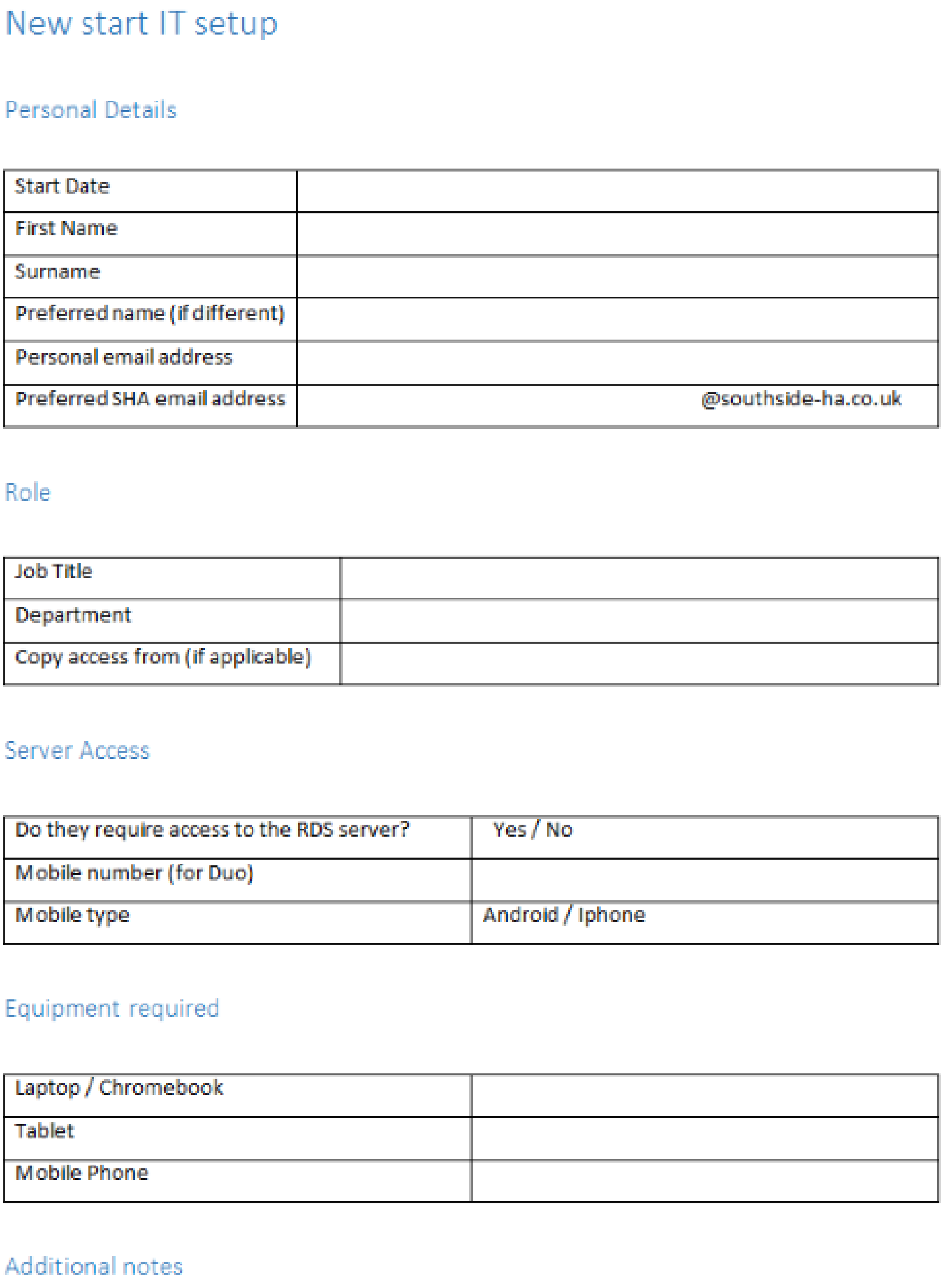
7. **Stay on Topic**:

- Keep discussions focused on the original topic to avoid confusion.

8. **Acknowledge Contributions**:

- Thank those who help you and acknowledge useful contributions by upvoting or marking answers as helpful.

Appendix 2: New Starts Form



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)	

Server Access

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

Equipment required

Laptop / Chromebook	
Tablet	
Mobile Phone	

Additional notes

Appendix 3: Use of Devices Guidelines for signing

Use of Devices Policy

1. Purpose

- This policy outlines the acceptable use of electronic devices within Southside Housing Association. The goal is to ensure that all employees use devices responsibly and securely to protect company data and maintain productivity.

2. Scope

- This policy applies to all employees, contractors, and temporary staff who use association provided or personal devices for work purposes.

3. Acceptable Use of Association Devices

- Devices should be used primarily for work-related activities.
- Personal use should be limited and must not interfere with work responsibilities.
- Employees must comply with all company policies, including those related to data protection and confidentiality.

4. Security Measures

- Devices must be protected with a strong password or biometric authentication.
- Devices are encrypted to protect sensitive data.
- Install and regularly update antivirus software and security patches.
- Avoid connecting to unsecured Wi-Fi networks.
- Use a remote desktop gateway when accessing the association's resources remotely.

5. Prohibited Activities

- Accessing inappropriate or illegal content.
- Downloading unauthorised software or applications.
- Using devices for activities that could harm the company's reputation or security.

6. Monitoring and Privacy

- The association reserves the right to monitor device usage to ensure compliance with this policy.
- Employees should have no expectation of privacy when using company-provided devices.

7. Consequences of Violation

- Violations of this policy may result in disciplinary action, up to and including termination of employment.

8. Policy Review

- This policy will be reviewed annually and updated as necessary.

9. Acknowledgment

- Employees must sign an acknowledgment form confirming they have read and understood this policy.

10. Acknowledgment

- Employees must sign an acknowledgment form confirming they have read and understood these guidelines.

I acknowledge that I have read and understood the Policy on Use of Devices.

Name:

Date:

Signature: