Acceptable Use Policy

1.0 Introduction

1.1 This Policy covers the security and use of all our information and IT equipment (e.g. use of email, internet, voice, and mobile equipment).

1.2 Everyone has a role to play in keeping our systems and data safe. Although we have centralised controls in place to minimise potential damage to our systems and data, these can only go so far.

1.3 This Policy sets out your responsibilities to help protect Southern Housing when using our network, systems, or equipment issued to you.

1.4 The terms 'you' and 'your' in this Policy refer to all listed in 2.1. The terms 'we', 'our' and 'us' mean Southern Housing.

2.0 Scope

2.1 This Policy applies to:

- Employees (permanent and temporary, work placement candidates)
- Board and Committee members
- Resident Governance members[1]
- Contractual third parties
- Consultants
- Agents (who access our internet services and IT equipment).

2.2 This Policy relates to:

- All information we hold or use
- Any IT equipment used
- The physical environment in which the information or the supporting equipment is used.

2.3 This Policy specifies the management arrangements and key responsibilities. It is supported by more detailed policies covering specific aspects of information security.

[1] As defined in our *Resident Governance Framework*

3.0 Computer access control

3.1 We'll:

- Provide IT equipment, systems, and services to assist you in carrying out your role
- Provide a secure network and system access with passwords
- Monitor how you use our equipment, systems, and services
- Review usage where there is suspected breach of this Policy
- Provide written guidance and advice on the use of our IT services.

3.2 You must:

- Keep your network and system access secure by following the guidance for using our IT services
- Seek appropriate Technology Department authorisation for the use of any internal or external IT systems or equipment
- Protect our business reputation by not making offensive, negative, or damaging statements about us, our clients, suppliers, or any other affiliates or stakeholders
- Lock your screen if you leave your device unattended for any reason in a shared environment
- Only use your username and password to access the IT systems or equipment
- Only download or install software as instructed by the Technology Department. This includes software programs, instant messaging programs, and screensavers.
- Remember when using our network, systems, or internet facility, you are our representative
- Only seek access to restricted areas of the network, or to any password-protected information, where specifically authorised by the Technology Department
- Contact the IT Service Desk if you require access to corporate cloud-based storage
- Only connect to IT systems using IT Security approved devices.

3.3 You must not:

- Perform any changes to the organisation IT equipment or systems (including but not limited to laptops, devices, software, or hardware) without written Technology Department approval. This includes all Technology Department members.
- Delete, destroy, or modify existing systems, programs, information, or data that could have the effect of harming our business or exposing it to risk
- Connect to our IT systems from a public computer (e.g. in an internet café, library, airport etc.) or from any device that does not personally belong to you, or your immediate family
- Store our data or information in the public cloud or download data from the public cloud, unless authorised by the Director of Technology. This includes, but is not limited to, a personal OneDrive, Google account.

- Give or transfer our data or software to any other person or organisation without appropriate data sharing contracts in place and approval from the Technology Department
- Attach unauthorised personal devices or equipment for charging purposes, uploading, or downloading data. This includes any kind of computer, tablet, USB flash drive, MP3 or similar device, PDA, or telephone. It also includes use of the USB port, infra-red connection port, or any other port.
- Allow third party support or access to our devices, in person or via remote access, without prior consent from the IT Service Desk
- Use personal email accounts to move or store our information or data, unless authorised by the Director of Technology.

4.0 Passwords

4.1 We'll enforce password complexity and expiry requirements through software where possible.

4.2 You must:

- Set strong, unique passwords and change them regularly or when requested by someone from the Technology Department
- Keep your passwords confidential (don't share them with anyone)
- Lock your terminal when you leave it unattended and log off when you stop working to prevent unauthorised users accessing the system. You can lock most PCs and laptops by pressing Ctrl + Alt + Delete simultaneously on your keyboard or using the 'Windows' and 'L' keys.
- Report immediately any suspected misuse or compromise of your password to your manager and IT Service Desk
- Change your password for any account you think might have been accessed by an unauthorised person
- Provide your passwords to your line manager along with devices issued by us on termination of your employment with Southern Housing.

4.3 Your passwords need to be difficult to guess. You should set passwords that:

- Are at least 14 characters long
- Contain a non-consecutive mixture of:
    - uppercase letters
    - lowercase letters
    - numbers 0-9
    - symbol ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/
    - you can even use a space.

4.4 Do **not**:

- Use common phrases and names
- Use passwords based on any easily guessable or memorable data such as names, dates of birth, telephone numbers, favourite pet's name, 12345678, Password1, Qwerty, etc.
- Re-use passwords

- Use new passwords that are in a sequence
- Use the same password for organisational work and personal use.

4.5 Passwords must be changed if there is evidence of possible system or password compromise.

4.6 When authorising recording of passwords, the Technology Department will advise how to store them safely and what mechanism to use (i.e. in a sealed envelope stored in a secure cabinet, an authorised password manager e.g. LastPass).

4.7 You must notify the IT Service Desk immediately if you believe your password has been compromised and someone else has gained access to your account.

5.0 Telephony (voice) and equipment conditions of use

5.1 Use of the organisation's voice equipment is intended for business use. You must not:

- Use the organisation's telephony for conducting private business
- Make hoax or threatening calls to internal or external destinations
- Accept reverse charge calls from domestic or international operators unless there is a legitimate, justifiable business reason for doing so
- Use premium rate numbers without prior authorisation
- Make international calls.

6.0 Clear desk policy, screen savers, and information reproduction

6.1 To reduce the risk of unauthorised access or loss of information, you must:

- Not leave personal, sensitive, or confidential classified business information (in paper or removable storage media format) on desks or in/near reproduction equipment (photocopiers, fax machines, scanners). You must protect and secure this information in line with our security requirements.
- Log off or lock your active computer sessions with a screen locking mechanism controlled by either a password or pin (i.e. not simply turn off the computer screen)
- Dispose of all business-related printed matter using confidential waste bins or shredders; disposal must be appropriate for the classification level
- Only use our reproductive equipment (photocopiers, fax machines, scanners) for work purposes
- Always consult the Communications Team before using our copyright material, logos, brand names, slogans, or other trademarks, or posting any of our confidential or proprietary information.

7.0 Remote working

7.1 Remote working is defined as a work arrangement that permits a colleague to conduct all or some of their work at a non-Southern Housing location.

7.2 We accept staff will take laptops and mobile devices off-site. You must:

- Not leave equipment or removable media (e.g. USB) unattended in public places or in sight in a car
- Carry laptops as hand luggage when travelling
- Protect information against loss or compromise when working remotely by following IT security training and guidance
- Ensure corporate devices are always maintained and kept up to date. Most device updates are automatic, though some require colleague intervention, such as mobile phone system updates. Devices which are not kept up to date may present a security risk and consequently may lose access to corporate systems.
- Not forward corporate emails or information to personal email accounts
- Ensure your device screen is not visible to onlookers when remote working in public environments e.g. public transport, cafés. Be especially careful when working with personal, sensitive, or confidential information.

7.3 When working from home, you must ensure all personal equipment (broadband equipment etc.) is kept up to date and have sufficient protections in place. Protection examples include:

- Wi-Fi encryption uses WPA2 (AES) minimum – please speak to your broadband provider for more information
- Default passwords on routers, wireless networks and personal devices are changed
- Wi-Fi access is only provided to those within your trusted household, i.e., not to persons unknown to the household
- Router firmware is kept up to date
- Under no circumstances must a colleague allow a third-party to remotely access their corporate device for technical support or any other reason. If in doubt, please contact the IT Service Desk.

If you experience any suspicious activity on your device or suspect a cyber incident has occurred report it immediately. Examples of suspicious activity on a device can include, but are not limited to:

- Frequent crashes or unusually slow computer performance
- Unknown programs that start-up when you start your device
- Programs automatically connecting to the internet
- Unusual activities like passwords being changed without your knowledge
- Frequent pop-up windows, especially ones that encourage you to visit unusual sites or download files or other software
- Mass emails being sent from your email account.

8.0 Mobile devices

8.1 We issue mobile devices so you can carry out your role.

8.2 You must:

- Always take care of your device and return it to your line manager when you:
    - move to a role that doesn't require a mobile device
    - leave Southern Housing.

- Protect all mobile devices, including a personal device used for business, with a password in line with the guidance set out in section 4
- Only store our data on devices issued or approved by us
- Only access email on any mobile phone or tablet (whether owned by you or us) via an approved secure application. IT Service Desk will provide access.
- Report the loss or theft of any mobile device immediately to your line manager, the IT Service Desk, and the Data Protection Team
- Not use any unsecured external drive for work purposes If you need to store data externally, the Technology Department can provide an encrypted USB stick.

8.3 Use of personal devices is covered by our Bring your Own Device (BYOD) Policy. Compliance with that Policy, where relevant, is a requirement of this Policy.

9.0 Software

9.1 You must use only Technology Department authorised software on our devices. You must use it in accordance with the software supplier's licensing agreements. This includes free software, shared software, screensavers, toolbars and/or any other programs that might be available.

9.2 You must not:

- Store personal files such as music, video, photographs, or games on IT equipment
- Attempt to disable or over-ride any of the installed software, including anti-malware, software, firewalls, and automatic updating services
- Infringe the copyright of others or us by downloading photos, video clips, and music files. If in any doubt you should ask the IT Service Desk.

10.0 Viruses and malware

10.1 We have implemented centralised, automated virus detection and virus software. All devices have antivirus software installed to detect and remove any virus automatically.

10.2 You must not:

- Remove or disable anti-virus software
- Attempt to remove virus-infected files or clean up an infection, this will be done by IT using approved anti-virus software and procedures.

11.0 Internet and email conditions of use

11.1 We:

- Provide internet access as a business tool
- Allow personal use of the internet and social media if it does not interfere with your duties
- Carry out downloads on your behalf

- Transmit sensitive data securely
- Protect the security of our systems
- Check use of the service is legitimate and in accordance with this Policy
- Investigate suspected wrongful acts and otherwise comply with legal obligations
- May access your internet and social media use on work devices as part of a relevant disciplinary investigation, where there are reasonable grounds to suspect that you have misused our systems.

11.2 You are accountable for:

- Your actions on the internet and email systems
- Keeping personal correspondence to a minimum.

11.3 You must not:

- Use the internet or email for the purposes of harassment or abuse
- Use profanity, obscenities, or derogatory remarks in communications, unless there is a legitimate business reason for doing so, e.g. quoting a tenant's verbal abuse of neighbour
- Access, download, send or receive any data (including images) we consider a breach of our code of conduct or values. This includes but is not limited to sexually explicit, discriminatory, defamatory, or libellous material.
- Use the internet or email to make personal gains or conduct a personal business
- Use the internet or email to gamble
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
- Place any information on the internet (whether using our systems or otherwise) that relate to us, alter any information about it, or express any opinion about us, unless specifically authorised to do so
- Send unprotected personal, sensitive, or confidential classified information externally
- Make official commitments through the internet or email on behalf of the organisation unless authorised to do so
- Download copyrighted material such as music media (MP3) files, film, and video files (not an exhaustive list) without appropriate approval
- In any way infringe any copyright, database rights, trademarks, or other intellectual property
- Download any software that has not been authorised by the IT department
- Connect to the organisation's devices to the internet using non-standard connections e.g. personal VPNs.

12.0 Information classification

12.1 You must ensure all information on your workstation and mobile devices are correctly classified and labelled to prevent incorrect sharing of data.

12.2 You must protect files containing personal or sensitive personal information saved on a group shared drive (e.g. encrypt, password protect, limit access,) and delete them in line with our *Document and Data Retention Policy*.

13.0 Audit and security monitoring

13.1 All data that is created and stored on our computers is our property and there is no provision for colleague data privacy.

13.2 To ensure our systems are used in line with this Policy, we reserve the right to:

- Monitor
- Intercept
- Review
- Record
- Inspect
- Copy your activities using our IT devices, networks, and communications systems.

This includes, but is not limited to, social media postings, emails, text messages, and internet usage.

13.3 The organisation has the right (under certain conditions) to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse.

13.4 Any monitoring will be carried out in accordance with audited, controlled internal processes, in accordance with relevant regulations and law.

14.0 Incident reporting

14.1 You must:

- Respect intellectual property and confidential information
- Report any Cyber Security incidents or suspected Cyber Security incidents to the Technology Department via the Resolve (former SHG staff) / Halo (former Optivo staff) portals
- Report suspicious emails quickly using the Phish Alert Report button in Outlook
- Report any Data Protection incidents or suspected incidents to the Data Protection Team
- Report any lost or stolen mobile devices to the IT Service Desk as soon as it is practicable to do so
- Stolen mobile devices must also be reported to the police and the issued crime number given to the IT Service Desk.

15.0 Revocation and change of access rights

15.1 You must return all equipment and data, for example, laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, to us when you leave Southern Housing.

15.2 All our data or intellectual property developed or gained during the period of employment remains our property. You must not retain it after you leave or reuse it for any other purpose.

15.3 The circumstances when removal and/or change of access rights apply include:

- Change in role
- Failure to comply with this policy
- Failure to comply with mandatory cyber security training
- Temporary suspension from role
- Termination of employment.

16.0 Enforcement

16.1 Internal Audit can, without notice, conduct random assessments to ensure compliance with the principles of this Policy.

16.2 The Information Technology Security Board or Information Governance Group will authorise risk mitigation actions for any system found in violation of this Policy immediately.

17.0 Policy breach

17.1 A security breach is any incident or activity that causes, or may cause, a break down in the availability, confidentiality, or integrity of the physical or electronic information assets of the organisation.

17.2 We'll manage all security breaches via the Information Security Team.

17.3 If you don't keep to the principles in this Policy, it's a disciplinary offence:

- As an employee this may be considered serious/gross misconduct
- As a member of Resident Governance this may be a breach of the Probity Policy and Code of Conduct
- As a contractual third party this would be escalated to the relevant Leadership Team director and could result in action, not excluding termination of contract with us
- As an agent accessing our network and systems this could result in action, not excluding termination of contract with us.

18.0 What have we done to make sure this Policy is fair?

18.1 We've completed an Equality Impact Assessment to consider the positive and negative impacts this Policy may have on people with protected characteristics under the Equality Act 2010.

19.0 Review

19.1 We will review this Policy to address legislative, regulatory, best practice or operational issues.

Policy controls
Version 1.3 – effective 3 June 2024