Hillhead
HOUSING ASSOCIATION
Building on progress for a brighter Hillhead

HILLHEAD HOUSING ASSOCIATION 2000

ICT SECURITY POLICY

Last reviewed by Management Committee on 7 August 2024

Next review date: August 2025

The information in this document is available in other languages or in large print and also in Braille.
For details contact the Association on 0141 578 0200 or email: admin@hillheadhousing.org

本文件所載資料備有中文 (廣東話) 版本，也可以製作成錄音帶/光碟，以及利用特大字體和凸字印製，以供索取。
欲知有關詳情，請聯絡本協會，電話：0141 578 0200，或向我們發送電郵， 電郵地址：admin@hillheadhousing.org

Tha am fiosrachadh anns an sgrìobhainn seo ri fhaotainn ann an Gàidhlig no air teip/CD, sa chlò mhòr agus cuideachd ann an Clò nan Dall.
Airson tuilleadh fiosrachaidh, cuiribh fios dhan Chomann air 0141 578 0200 no cuiribh post-dealain gu: admin@hillheadhousing.org

इस दस्तावेज़ में दी गई जानकारी हिन्दी में भी या टेप, सी डी, वड़ी छाप और ब्रैल में भी उपलब्ध है। विवरण के लिए ऐसोसिएशन को नम्बर 0141 578 0200 पर या ई-मेल के द्वारा सम्पर्क करें : admin@hillheadhousing.org

ਇਸ ਦਸਤਾਵੇਜ਼ ਵਿਚ ਦਿੱਤੀ ਗਈ ਜਾਣਕਾਰੀ ਪੰਜਾਬੀ ਵਿੱਚ ਵੀ ਜਾਂ ਟੇਪ, ਸੀ ਡੀ, ਵੱਡੀ ਛਪਾਈ ਅਤੇ ਬ੍ਰੈਲ 'ਤੇ ਵੀ ਉਪਲਬਧ ਹੈ। ਵੇਰਵੇ ਲਈ ਐਸੋਸਿਏਸ਼ਨ ਨੂੰ ਨੰਬਰ 0141 578 0200 'ਤੇ ਜਾਂ ਈ-ਮੇਲ ਰਾਹੀਂ ਸੰਪਰਕ ਕਰੋ : admin@hillheadhousing.org

اس دستاویز میں درج معلومات اُردو زبان یاآڈیوٹیپ / سی ڈی، بڑی طباعت اور بریل میں بھی دستیاب ہیں۔
تفصیلات کے لئے ایسوسی ایشن سے ٹیلیفون نمبر **0141 578 0200** یا ای میل **admin@hillheadhousing.org** کے ذریعے رابطہ قائم کریں۔

Table of Contents

Opening Statement

Hillhead Housing Association 2000 is an established user of Information and Communication Technologies (ICT). Since ICT plays such a prominent part in the day to-day activity of the Association, it is essential that controls are in place that protects the Association and all users (Committee Members and Staff), as well as third parties, and suppliers. The Association's objective is to maximise the effectiveness of the equipment and applications provided and to ensure business continuity in the event of any system failures.

The purpose of the policy is to protect the Association's information assets from all threats whether internal or external, deliberate, or accidental. For the purposes of the Policy, information includes data stored in the Cloud, on laptops, iPads, mobile phones, transmitted across networks, printed out on written paper, stored on removeable storage devices, or spoken in conversation and over the telephone.

1. Policy Statement

It is the policy of Hillhead Housing Association to ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured protecting valuable or sensitive information from unauthorised disclosures or intelligible interruption
- Integrity of information will be maintained safeguarding the accuracy and completeness of information by protecting against unauthorised modification
- Business requirements for the availability of information and information systems will be met
- Regulatory and legislative requirements will be met including the needs of the current General Data Protection Regulation and in accordance with our Data Protection Policy
- Business continuity plans will be produced, maintained, and tested to ensure that vital services are available to users when and where they need them
- Information security and cyber security training will be available to all users
- All breaches of information security actual or suspected will be reported to and investigated by the Director
- Procedures will exist to support the Policy. These include device security, passwords, and business continuity
- The Director has direct responsibility for maintaining the Policy and providing advice and guidance on its implementation
- All Managers are directly responsible for implementing the Policy within their section and for adherence by their staff. It is the responsibility of each member of staff to adhere to the Policy.

2. Applicability of the Policy

This policy is applicable to all users.

It is vital that you read this policy carefully. If there is anything that you do not understand, it is your responsibility to ask for an explanation. Queries should be directed to the Senior Systems & Innovation Officer or to a member of the Management Team. Once you have read and understood this Policy, you must sign it on page 40 and photocopy that page.

Return the signed copy to the Head of Corporate Services. Keep a copy for your own reference.

As the use of technology grows, Committee members will have online access to the Associations information such as reports and minutes.

Non-compliance of this policy will be dealt with in accordance with the staff conditions of service disciplinary procedures and for committee members, in line with their code of conduct.

3. Acceptable Use

It is essential to ensure that computers and devices owned or controlled by the Association are used in an appropriate, safe, and secure manner.

Inappropriate or insecure use of Association computers and devices could lead to a malware infection, a breach of data, or damage to our reputation. Acceptable usage is set out in the Acceptable Use Statement (Appendix 1). By following the guidance and instructions given, users will be contributing to the success of the Association as well as developing their own skills and understanding.

4. Cyber Security

The security of information is of paramount importance and therefore it is Association policy to protect business information and systems from all threats, internal and external, deliberate, or accidental. It is equally important to maintain customer, service users and stakeholders' confidence by meeting all obligations under the General Data Protection Regulation and any other relevant information legislation. The Association considers there to be three basic aspects of information security, being confidentiality, integrity, and availability.

To maintain its value, Association information must be available when and where it is needed. Therefore, in order to protect its service users, the Association must protect its own internal systems. Details are set out in the Cyber Security Statement (Appendix 2).

5. Passwords

Passwords are used to protect systems, data, and devices across the business. Appropriate and secure use of passwords is essential for business security. Strong passwords significantly reduce the opportunity for unauthorised access to business information resources, whereas weak passwords heighten risks greatly. Guidance and instructions are set out in the Password Statement and in the Password Construction Guidelines (Appendix 3).

6. Anti-Malware

It is essential that the Association ensures its systems, data, and devices are secure and free from malware. Malware includes all types of malicious programs, applications and scripts, including but not limited to viruses, trojans, ransomware, spyware and adware. Malware infections can be costly for the Association to deal with, and lead to breach of sensitive data as well as reputational damage to the Association.

It is essential that all users take the anti-malware measures seriously and take all reasonable efforts to protect Association systems, data, and devices.

The Anti-Malware Statement (Appendix 4) sets out responsibilities for users accessing the Association's systems, data, and devices.

7. Cyber Security Awareness Training

The Association acknowledges the threats in a rapidly evolving online world. Keeping up with cyber security is essential for protecting Association and customer data. Without the proper

measures and every user taking up responsibility in securing their devices, services, and networks, data could become compromised.

Exposure of sensitive business information or personal customer details can be highly damaging to the Association. Association devices and the Association network are also at risk from ransomware and malware attacks, which can prove highly costly to deal with. To prevent breaches of data, infection of Association devices or intrusion of the Association network, it is essential that all users are trained in the necessary measures to keep up security. This is set out in the Cyber Security Awareness Training Statement (Appendix 5).

8. Communications

Voice calling is the primary channel used to communicate with customers and business partners. It is therefore, vital that reliable systems are provided and that they are used securely and efficiently.

Wherever possible, voice calling should be via Microsoft Teams. This will ensure calls are recorded.

Email is a widely used form of communication within the Association and it is essential that it is used appropriately and securely so that it cannot compromise the security or integrity of the Association's data or systems. Acceptable use and prohibited use is set out in the Email-Use Statement (Appendix 7)

Communications with customers and applicants should be via the Housing Management System email and text system wherever possible. If not possible, emailing should be via Microsoft Outlook and emails saved to the customer or applicant record.

Texting via work mobile phones is not encouraged and should only be used if the methods above cannot be. If Texting via work mobile is used, screen prints must be taken and saved to the customer record and chats should be deleted when 10 working days old.

WhatsApp use on mobile phones is prohibited. If the methods above cannot be used and WhatsApp use is needed, it must be accessed on your laptop and screen prints must be taken and saved to the customer record and chats should be deleted when 10 working days old.

Wherever possible, internal communications and chat should be done via Microsoft Teams.

9. Internet

While the internet has become essential for many business operations, it also comes with risks. It is essential that the internet is accessed in a secure manner to prevent exposure of Association data or the Association network and is not misused or used to conduct non-business purposes.

Acceptable use and prohibited use is set out in the Internet-Use Statement (Appendix 6).

10. Email

Email is a widely used form of communication within the Association and it is essential that it is used appropriately and securely so that it cannot compromise the security or integrity of the Association's data or systems.

Acceptable use and prohibited use is set out in the Email-Use Statement (Appendix 7).

11. Clear Desk & Clear Screen

To ensure that sensitive and confidential material does not go unaccounted for or become exposed, the Clear Desk & Clear Screen Policy (Appendix 8) requires users to completely clear their desks at the end of their workday, moving items to drawers and disposing of documents that are no longer needed. This protects Association information from unauthorised access as it reduces the amount of information that is available to an unauthorised person who may gain access to the Association's premises.

12. Secure Remote Working

The Association's ICT systems can support remote working and gives employees remote access to all systems and data. Employees are required to have home broadband in place with sufficient speed and appropriate security in place. The Association will provide a laptop with software to allow staff to work remotely and securely. Further detail can be found in the Secure Remote Working Statement (Appendix 9).

13. Mobile Phones

A large part of keeping our systems, data, and devices secure involves knowing what applications are present on all devices. Laptops are protected through policies and malware protection software, but this same protection is not used on mobile devices. To help ensure our mobile devices are secure from malicious apps and software, our guidance and instructions are set out in the Mobile Phone Guidance (Appendix 10).

14. Policy Review

This policy will be reviewed annually or earlier if a change in practice dictates.

Appendix 1 – Acceptable Use Statement

1. Overview

The Association depends on computers and mobile devices as part of our daily business operations. It is essential to ensure that computers and devices owned or controlled by the Association are used in an appropriate, safe and secure manner.

Inappropriate or insecure use of Association computers and devices could lead to a malware infection, a breach of data, or damage to the Association's reputation. This is why an Acceptable Use Statement is essential, as it sets out clear rules on the acceptable use of Association computers and devices.

2. Purpose

The purpose of this statement is to set out rules on the acceptable and secure use of computers and mobile devices owned, leased, or otherwise controlled by the Association.

3. Scope

This statement applies to all users that may use computing devices or network resources owned, leased or controlled by the Association or on behalf of the Association.

4. Statement

4.1. General Use

4.1.1. Association data stored on computing devices owned or controlled by the Association remain the sole property of the Association.

4.1.2. The Association's data must be protected in accordance with the UK General Data Protection Regulation.

4.1.3. Association data must only be accessed, used or shared only to the extent it is necessary for performing your assigned job duties.

4.1.4. Loss, theft or unauthorised disclosure of Association data must be reported immediately to a member of the Management Team and to the Senior Systems & Innovation Officer.

4.2. Prohibited Use

All illegal, immoral, offensive or intolerant behaviour and content are strictly prohibited on the Association computing devices and network.

The following sections form a non-exhaustive list of prohibited activities and content that are expressly prohibited on the Association network and computing devices.

4.2.1. The introduction of malware, viruses, or other malicious programs or applications into Association computing devices or the Association network.

4.2.2. Violation of any copyright, patent, trade secret or other intellectual property.

4.2.3. Using, copying, sharing or accessing copyrighted entertainment, software or other material in an unauthorised manner**.**

4.2.4. Using, creating, transmitting, sharing or accessing material that could be construed to violate sexual harassment or hostile workplace laws, policies or principles.

4.2.5. Posting on any online forum, social media or newsgroup as a representative or associate of the Association without the appropriate permission to do so.

4.2.6. Disclosing any passwords on user or system accounts in the Association's network, devices or systems to any other party.

4.2.7. Allowing your user accounts in the Association's network, devices or systems to be used by others.

4.2.8. Port scanning, security scanning or network monitoring.

4.2.9. Circumventing user authentication.

4.2.10. Any form of harassment, abuse, or bullying over email, social networks or in any other form.

4.2.11. Creation or the forwarding of chain letters or multi-level-marketing schemes.

4.2.12. Unauthorised use or forging of email header information.

4.2.13. Unauthorised use of any business email account for purposes not relevant to job duties or for making fraudulent offers or communications.

4.2.14. Engaging in any online activity that may harm or tarnish the image or reputation of the Association.

4.2.15. Personal use of Association computing devices is prohibited.

4.2.16. Personal devices are not to be used by any member of staff for accessing Association data or systems.

4.3. Security

4.3.1. All users must be given minimal access to data and privileges, with only the required access to carry out their role and duties to be given.

4.3.2. All users must set a unique password for each of their accounts.

4.3.3. All computers must be locked or shut down when they are not in use, even for brief periods.

4.3.4. All computing devices must be set to automatically lock after no more than ten minutes of inactivity.

Appendix 2 – Cyber Security Statement

1. Overview

Cyber security is essential for protecting Association data. We are trusted to keep data safe and without the proper measures and every user taking up responsibility in securing their devices, services, and systems, data could become compromised and cause serious damage to the Association and its reputation.

2. Purpose

The purpose of this statement is to inform all users of their obligatory requirements for protecting the Association's technology and information assets from all threats whether internal or external, deliberate or accidental. For the purposes of this statement, information includes data stored, in the Cloud, on laptops, on iPads, on mobile phones, transmitted across networks, printed out on paper or spoken in conversation and over the telephone.

By agreeing to and following this guidance, you are helping ensure that the Association is doing everything it can to keep sensitive and personal data protected and maintain our reputation as a secure operator.

3. What Needs Protecting?

The key assets requiring protection through this statement are:

3.1. Hardware

3.2. Software

3.3. Data

We have broken these assets down into specific business areas which we need to protect – Physical Security, Information Security, and Unauthorised Access.

4. Physical Security

These are the means by which we ensure that premises and documents are kept secure from unauthorised access.

4.1. Protecting the Building

- Intruder alarm, including service notifying designated points of contact and/or security company when triggered
- Key and Fob access to main office doors
- Security cameras
- Staffed reception area to vet and sign in visitors

4.2. Protecting Documents in the Office

Documents are protected from unauthorised access by:

- Locked cabinet for storage of all paper documents
- Locked, fireproof safe for overnight storage of important documents and petty cash
- Clear desk policy to avoid documents left on desks and on view overnight

- Confidential paperwork is placed in secure bags and shredded regularly

5. Information Security

These are the means by which we ensure that any electronically stored information is kept secure from unauthorised access.

5.1. Systems are protected from unauthorised access, viruses and malware by:

- The use of unique usernames and strong passwords
- The use of multi-factor authentication where available
- Information stored in the cloud is encrypted
- Wireless network is secured
- Incoming emails are scanned for threats before they are delivered to the user
- Incoming emails are filtered for spam and quarantined for checking before they are delivered to the user
- Users are prohibited from opening email attachments and clicking on email links that are unexpected
- The use of Association devices for personal use is prohibited
- The use of removable media is prohibited
- Staff are prohibited from using personal devices to access Association systems, services or information
- At least weekly reboot of laptops to ensure security updates are applied
- Laptops have a standard pre-set configuration which should not be changed by the user
- No user has admin access on their laptop. Requests for tasks requiring admin access need to go via the Senior Systems & Innovation Officer. The external IT Support company staff have individual admin accounts for use on the laptops and credentials used are recorded on the support call
- All laptops are installed with remote management and monitoring software (RMM). This product enables our IT Support company to remotely manage devices and schedule important software updates, security patches and third-party software patching
- All laptops are installed with Endpoint Detect and Response (EDR). EDR is designed to prevent, detect, and respond to evolving cyber threats on our devices. EDR uses artificial intelligence to detect unusual behaviour that could indicate malicious activity. This gives users more proactive protection
- All laptops are installed with website DNS protection. This service protects users from visiting known and suspect dangerous websites that are marked as being suspicious

5.2. Use of Personal Devices

Staff are prohibited from using personal devices to access Association systems, services or information.

5.3. Disposal of Hardware

Consideration is given to the disposal of laptops, mobile phones and other hardware devices.

- If a third party is used for the disposal of hardware, the Association will satisfy itself with their security and staff vetting arrangements
- Disposal of a hard drive - the third party will erase all with specialist software and destroyed sufficiently so that information cannot be accessed by an unauthorised person

6. Protecting against Unauthorised Access

These are the additional means by which we ensure that our information is kept secure from unauthorised access.

6.1. Staff

Staff are made aware of their obligations through:

- Staff Handbook/employment contract
- Induction process which covers this and other ICT policies
- Updates to changes on this and other ICT policies
- Regular training on data protection and cyber security

Use of all Association equipment is governed by the ICT Security Policy which ensures that:

- All Association equipment is logged against the user
- Laptops must be locked away and not left in insecure locations (e.g. in cars overnight)
- Files may not be taken home
- The use of personal devices to access Association systems, services or information is prohibited for members of staff
- Users may not use Association devices for personal use
- Users may not email work to personal email accounts
- Users may not leave their devices unattended in a public place
- Users must lock their screen when leaving their device unattended
- Users will not allow any other person to use their device
- Users will reboot their laptop at least weekly to ensure important updates are applied
- Users should only access information that is needed to perform their job duties

6.2. Staff Leavers

The Association is protected from users who leave as all property including IT equipment, ID badge, keys and fobs are to be returned to the Association on leaving. Logins are disabled at the end of the last working day.

6.3. Access Rights

Access to technology and information assets is granted only when necessary, and access may be revoked at any time if the assets are not used in a secure manner or for the purpose for which access was granted. Access to technology and information assets is also determined by the principle of least privilege.

- Access to laptops and access to systems and data is controlled by notifying our IT Support company using the agreed Staff Changes documents
- Access is granted to information only where required and approved by a member of the Management Team
- Temporary access to data must also be time bound, and privileges revoked after that date or an extension expressly granted by a member of the Management Team
- A register is maintained listing what access rights have been given and to which user. This is maintained and updated by the Senior Systems & Innovation Officer.

7. Requests for and Exchange of Information

7.1. Telephone

All inbound calls from tenants/applicants for the following are subject to verification.

- Change to any contact details
- Request for any copy correspondence previously issued by post
- Request for rent balance
- Any other suspicious requests or requests for information which might reasonably be used for fraud

7.2. Email

All email requests from tenants/applicants for the following are subject to verification by contacting the tenants/applicants by telephone using the number held on the tenants/applicants record.

- Change to any contact details
- Request for any copy correspondence
- Request for rent balance
- Any other suspicious requests or requests for information which might reasonably be used for fraud

All email correspondence sent back to the tenants/applicants containing any personal information, must be sent using the email address held on the tenants/applicants record.

7.3. Letter

All requests by letter from tenants/applicants for the following are subject to verification by contacting the tenants/applicants by telephone using the number held on the tenants/applicants record.

- Change to any contact details
- Request for any copy correspondence

- Request for rent balance or policy information
- Any other suspicious requests or requests for information which might reasonably be used for fraud

All correspondence sent back to the tenant/applicant containing original tenant/applicant documents, must be sent using iMail and to the address held on the tenants/applicants record.

7.4. Request for Information Under the Data Protection Act

Any individual requesting information held on them under the General Data Protection Regulation (GDPR) has a right to such information, subject to certain limitations. All such requests should be forwarded to the Director who is responsible for the processing of such requests. Under no circumstances should staff provide this information without reference to the Director.

8. Security Violations/Data Compromise Reporting

All users are under an obligation to report any incident which you feel violates the information security of the Association by informing a member of the Management Team or the Senior Systems & Innovation Officer. All violations are recorded in the Data Breach Register.

Equally, all users are aware of the need to report any data compromise incidents. These can include:

- Loss of laptop or mobile device
- Loss of tenant/applicant data either in paper form or held electronically
- Unauthorised persons in office area where data is stored
- Tenant/applicant information passed onto an unauthorised third party

All incidents should be reported immediately to a member of the Management Team or to the Senior Systems & Innovation Officer. All violations are recorded in the Data Breach Register.

Appendix 3 - Password Statement & Password Construction Guidelines

1. Overview

Passwords are used to protect systems, data and devices across the business. Appropriate and secure use of passwords is essential for business security. Strong passwords significantly reduce the opportunity for unauthorised access to business information resources, whereas weak passwords heighten risks greatly.

2. Purpose

The purpose of this statement is to protect the Association from the threats stemming from weak passwords and inappropriate use and sharing of passwords. These threats include loss of Association data, tampering of Association devices and systems, cost of recovering data, as well as the potential of regulatory fines.

3. Scope

The scope of this statement includes all users who use the Association systems or devices or access the Association's data or network.

4. Statement

4.1. Password Creation

4.1.1. All passwords must conform to the Password Construction Guidelines.

4.1.2. A separate, unique password must be used for each separate account on the Association’s devices, network or systems.

4.1.3. Passwords may not be reused for other applications within the Association or in personal use.

4.1.4. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges. In addition, users should always use multi-factor authentication when it is available.

4.1.5 Previous passwords cannot be reused until 12 changes have taken place .

4.2. Password Change

4.2.1. Passwords should be changed when prompted and immediately when there is reason to believe that the password has been compromised.

4.2.2. Password cracking or guessing may be performed on a periodic or random basis by IT Support. If a password is guessed or cracked during one of these tests, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3. Password Protection

4.3.1. Passwords must not be shared with anyone, including managers and co-workers. All passwords are to be treated as sensitive, confidential information.

4.3.2. Passwords must not be inserted into email messages, texts or any other form of electronic or non-electronic communication, including over the phone.

4.3.3. Passwords may be stored only in “password managers” that have been specifically approved by IT Support.

4.3.4. Any user suspecting that their password may have been compromised must report the incident to a member of the Management Team and to the Senior Systems & Innovation Officer who will ask IT Support to change their password immediately.

4.3.5. Users shall have no more than 10 attempts to enter their password before they are locked out. They will remain locked out until IT Support unlocks them.

4.3.6 Device screen will lock after 10 minutes of inactivity.

4.3.7 Users must enter a password to unlock the device when returning from idle state.

4.4. Multi-Factor Authentication

Multi-factor authentication should be used whenever available, especially for systems that have access to sensitive data.

5. Admin Accounts

5.1 Users do not have admin access on their accounts on their laptops

5.2 Microsoft 365 admin account has 2FA and is managed by IT Support

5.3 IT Support manage admin access for network access

5.4 Admin accounts are separate from user accounts and IT Support Techs record their use on a call

5.5 All admin passwords are a minimum of 15 characters

6. Cloud Portals

6.1 All user and admin passwords are a minimum of 15 characters

6.2 Multi-factor authentication should be used whenever available

Password Construction Guidelines

1. Overview

Secure passwords are critical to the continued security of Association operations. Passwords are used in many different parts of the Association, for protecting systems, data and devices, and it is essential that passwords are constructed appropriately to ensure that Association operations are not compromised by unauthorised parties.

2. Purpose

The purpose of these guidelines is to provide end users with best practice for the creation of strong passwords.

3. Scope

These guidelines apply to all users who may use passwords to protect data, systems or devices owned by the Association or with access to data owned by the Association.

4. Password Construction

Strong passwords are long, easy to remember but hard to guess. The more characters there are the stronger the password. We highly encourage the use of passphrases, which are passwords made up of multiple words. Examples include “let’s go jumping in the park” or “square-hilarious-cloudy-squirrels”. Passphrases are both easy to remember and type, yet meet the strength requirements. Passwords must have:

- A minimum of 15 characters
- At least three random words

Poor or weak passwords have the following characteristics:

- Contain fifteen characters or less
- Contain personal information such as birthdates, addresses, phone numbers, or names of pets, family members or friends
- Contain work-related information such as the Association name
- Contain common patterns such as 123, qwerty, zxcv or 999.
- Contain common words or phrases such as ‘welcome’ or ‘password’, including variations such as ‘p@zzW0rd456’.

In addition, every work account should have a different, unique password. Users must not use the same password to access multiple systems i.e. do not reuse passwords ever. To enable users to maintain multiple passwords, we highly encourage the use of ‘password manager’ software that is authorised by our IT Support Company and provided by the Association. It's recommended we use the built-in password management service in the Microsoft Edge browser. Only save passwords in Edge when you are signed into your Microsoft 365 account in Edge. Whenever available, enable the use of multi-factor authentication.

Appendix 4 – Anti-Malware Statement

1. Overview

It is essential that the Association ensures its computers and network are secure and free from malware. This statement sets out responsibilities for users accessing the Association's data.

'Malware' as referred to in this statement includes all types of malicious programs, applications and scripts, including but not limited to viruses, trojans, ransomware, spyware and adware. Malware infections can be costly for the Association to deal with, and lead to breach of sensitive data as well as reputational damage to the Association. It is essential that all users take the anti-malware measures set out in this statement seriously and take all reasonable efforts to protect Association devices, network and data.

2. Purpose

The purpose of this statement is to protect Association devices and the Association network from malware by setting out clear rules, guidelines and responsibilities for all users.

3. Scope

The scope of this statement includes all users who may use Association devices or the Association network to access Association data or conduct Association business.

4. Statement

4.1. All computers that are owned or leased by the Association or connect to the Association network must run an approved and up-to-date anti-malware program that continually monitors for malicious software.

4.2. As software updates to anti-malware programs are released, they must be downloaded and installed without undue delay.

4.3. Files, attachments and macros attached to emails which are unexpected should never be opened.

4.4. Report any unexpected, unknown, suspicious or untrustworthy emails and/or attachments you receive to a member of the Management Team and to the Senior Systems & Innovation Officer without undue delay.

4.5. Delete all spam, chain, and other junk email without forwarding, in line with the Association's Acceptable Use Statement.

4.6. Never download files from unknown or suspicious sources or websites.

4.7. Never plug in a USB storage device or other removable device to your computer.

4.8. Always report any unaccounted for or unknown removable devices to a member of the Management Team and to the Senior Systems & Innovation Officer.

4.9. Installation of applications should be carried out by the IT Support company. Applications need to be pre-approved and on our approved apps list with installation from official application stores only. A list of pre-approved apps can be obtained from the Senior Systems & Innovation Officer.

Appendix 5 – Cyber Security Awareness Training

1. Overview

Exposure of sensitive business information or personal customer details can be highly damaging to the Association. Association devices and the Association network are also at risk from ransomware and malware attacks, which can prove highly costly to deal with. To prevent breaches of data, infection of Association devices or intrusion of the Association network, it is essential that all users of the Association network and devices are trained in the necessary measures to keep up security.

2. Purpose

The purpose of this statement is to set out why it is important for all network and device end users within the Association to take up security awareness training, and to clearly outline the expectations of users to engage in their training. This statement will both ensure that users know what is expected of them, and that the Association can take necessary measures to uphold compliance with its data protection regulatory requirements.

3. Scope

This statement applies to all users who have access to the Association's data, the Association's network, or devices owned or controlled by the Association.

4. Statement

All users must be aware of their responsibilities in protecting the data, devices and network of the Association.

The Association will provide training to all users before, and during their use of, the Association network and Association devices. All new users will receive a gap analysis questionnaire that will gauge their current knowledge on security areas. Users will then be trained by individualised programmes that will address their weakest areas first.

Training will be sent out regularly, once every 2 weeks, in the form of online training courses. These courses will be sent out by email and accessed from the Association email inbox.

Users are expected to complete all training courses received by them within no more than 14 working days.

The training will educate users on the risks of, or best practices regarding the use of, the following core information security areas:

- Email and internet use
- Phishing
- Social engineering
- Malware
- Adware and spyware
- Ransomware
- Working remotely
- Physical security

- Cloud security
- Passwords and authentication
- Social media use
- Voice- and text-based phishing

If a user has not received training in their email inbox in more than 3 weeks, or they have trouble accessing or completing their training, they must contact a member of the Management Team or the Senior Systems & Innovation Officer with no undue delay.

Appendix 6 – Internet-Use Statement

1. Overview

While the internet has become essential for many business operations, it also comes with risks. It is essential that the internet is accessed in a secure manner to prevent exposure of Association data or the Association network and is not misused or used to conduct non-business purposes.

2. Purpose

The purpose of this statement is to protect Association systems, services and information from inappropriate and harmful use.

3. Scope

This statement applies to all users who may access the internet through Association issued devices or connect to the internet through the Association network.

4. Statement

4.1. Provision of Internet Access

The provision of internet access to users is entirely at the discretion of the Association and may be reviewed and withdrawn at any time. All users are responsible for ensuring that their use of the internet does not expose Association devices, networks, or data to unauthorised access or damage from malicious software.

4.2. Acceptable Use

Internet privileges are granted to users for the purpose of carrying out the business of the Association, and users are expected to use the Internet for the purpose of carrying out their job functions.

4.3. Prohibited Use

Prohibited use of the Internet on Association issued devices or through the Association's network includes but is not limited to:

- All types of hateful, discriminatory, offensive and violent content.
- Access to Association documents and data that is not within the scope of the users' job duties.
- Unauthorised use, misuse, disclosure, alteration, sharing or access of customer or personnel data or communications.
- Linking of Association web content to Internet sites that contain content that is harmful, hateful, violent or otherwise inconsistent with the culture, values or policies of the Association.
- Any Internet conduct that would constitute or encourage a civil or criminal offense, or otherwise violate any law or regulation in the jurisdiction or jurisdictions in which the Association operates.
- Use, viewing, sharing or duplication of any material that infringes on copyrights, trademarks, trade secrets or patents of any person or organisation.

- Transmission of any confidential, sensitive, personal or proprietary information without the proper authorisation or controls.
- Creation, sharing, transmission, or voluntary receipt of any offensive, libelous, discriminatory or unlawful material including but not limited to material that discriminates on race, sex, gender, sexual orientation, age, disability, religion, national origin or political beliefs.
- Gambling and online gaming.
- Dating and adult content.
- Using the internet for personal use is prohibited.

4.4. Prohibited Activities

The following activities are expressly forbidden:

- Downloading, sharing or installing spyware, viruses, malware or any other type of harmful program or application.
- Playing of any games.
- Use of online dating services.
- Forwarding of chain letters.
- Viewing of pornographic or adult content.

4.5. Software License

Use or reproduction of software in a manner that infringes the vendor's license, copyrights or trademarks is forbidden.

4.6. Expectation of Privacy

4.6.1. The Association reserves the right to monitor all user Internet activity, including Web activity, email contents and file downloads.

4.6.2. The Association cannot guarantee that any activities performed with the Association's Internet access will be private or confidential.

4.7. Maintaining the Association Image and Values

Users must keep in mind that they are representatives of the Association at all times. Whenever employees state an affiliation to the Association, they must clearly indicate that the opinions they may express are those and do not necessarily indicate the opinions or values of the Association.

4.8. Association Materials

Association materials, data and communications may not be shared or posted publicly on the Internet without prior written approval by the employee's line manager.

4.9. Security Violations/Data Compromise

Report any potential security incident immediately to a member of the Management Team or to the Senior Systems & Innovation Officer.

Appendix 7 – Email-Use Statement

1. Overview

Email is a widely used form of communication within the Association and it is essential that it is used appropriately and securely so that it cannot compromise the security or integrity of the Association's data or systems.

2. Purpose

The purpose of this statement is to promote the secure and appropriate use of email within the Association.

3. Scope

This statement applies to all users using email addresses or systems owned by the Association or operated on behalf of the Association.

4. Statement

4.1. All use of email must be compliant with the Association's policies on ethical conduct and security of business data.

4.2. All use of email must be in line with proper business practices and relevant to job duties.

4.3. The Association's email addresses or systems shall not be used for creating, distributing or accessing any offensive or illegal material, including but not limited to material with offensive comments about gender, race, age, sexual orientation or religious beliefs.

4.4. Any offensive material received in email must be reported to a member of the Management Team and to the Senior Systems & Innovation Officer without undue delay.

4.5. Usage of Association owned email addresses and systems for personal use is prohibited.

4.6. Email received to Association email addresses may not be automatically forwarded to email addresses not owned or operated by the Association.

4.7. Individual email addresses may not be forwarded to email addresses not owned or operated by the Association.

4.8. The creation or forwarding of chain or joke letters from Association email addresses or systems is prohibited.

4.9. The Association may monitor and record any and all email messages received or sent by email addresses or systems owned or operated by the Association.

4.10. The Association does not necessarily monitor all email activity but retains the right to do so.

4.11. Wherever possible, communications with customers and applicants should be via the Pyramid Messenger email and text system. If not possible, emailing should be via Microsoft Outlook and emails saved to the customer or applicant record. Email addresses should be used from the customer or applicant record and not typed from scratch.

4.12. Outgoing emails should be checked to ensure that the email address used is the correct recipient for the contents of the email and any attachments. When you click send, the system will prompt you to check before confirming you want to send.

4.13. Users should pay particular attention to incoming emails that they did not expect to receive even if they are from recognised senders. Viruses can use email addresses from an infected PC, making them appear to be from someone you know. Special consideration should be given to emails that contain file attachments or links. If the email is unexpected do not open attachments or click on links before checking if the email is genuine. This should be done by calling the sender. Their phone number should be looked up rather than using a number contained within the email. If in doubt check with the Senior Systems & Innovation Officer or with IT Support company.

4.14. Never send passwords or other credentials over email.

5. Security Violations/Data Compromise

Report any potential security incident immediately to a member of the Management Team or to the Senior Systems & Innovation Officer.

Appendix 8 – Clear Desk & Clear Screen Policy

Introduction

To ensure the security and confidentiality of information, Hillhead Housing Association has adopted a Clear Desk and Clear Screen Policy.

This ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use. This policy will reduce the risk of unauthorized access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended.

A Clear Desk and Clear Screen Policy is an important security and privacy control, and applies to all permanent and temporary members of staff working at Hillhead Housing Association. The policy should also be applied to staff working from home.

Clear Desk

Staff are required to leave their desk/workstation free of any confidential/sensitive data at the end of the working day. This should also apply when staff are away from their workstation for more than a short period of time, namely at lunchtime, when attending meetings and overnight.

All sensitive and confidential paperwork must be removed from the desk and stored securely (where possible, locked in a drawer or filing cabinet).

All wastepaper which contains sensitive or confidential information must be placed in confidential waste sacks. These can be supplied to staff working from home if required. Under no circumstances should such information be placed in regular wastepaper bins.

Documents which are likely to be needed by other members of staff in the office should be stored in shared, locked filing cabinets. Other documents may be locked in other storage types used by individual staff members, e.g. desk pedestals.

Staff should ensure that any documents lying on their desk/workstation are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Sensitive information should be cleared from printers immediately.

Paper records which are left on desks/workstations overnight or for long periods of time are at risk of theft, unauthorised disclosure and damage. By ensuring that staff securely store or lock away confidential papers at the end of the day, when they are away at meetings and over lunch beaks etc. this risk can be reduced.

Printers should be treated with the same care.

Clear Screen

Staff are required to lock their computer screens by using Windows and ‘L’ Key, when leaving their desk for any reason and for any period of time.

Mobile devices should be PIN protected, set to power off after a period of 2 minutes and switched off when left unattended.

Staff should ensure that open documents on their computer screens are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Care must be taken that screens are not sited such that the information displayed on them can be seen by unauthorised persons.

Cameras or other recording devices must not be used to capture confidential/sensitive data.

Policy Review

This policy will be reviewed every 3 years, or earlier if a change in practice dictates.

Appendix 9 – Secure Remote Working Statement

1. Overview

Remote working is commonplace in many organisations. It allows flexibility for both staff and the Association by allowing staff to work from home. It is essential that remote working does not expose the Association systems, data or devices to unauthorised access or to malicious software.

This Secure Remote Working Statement sets out rules and guidelines on remote working, helping users protect Association devices and Association data while working away from the Association premises.

2. Purpose

The purpose of this statement is to help users work securely when away from the Association premises, and to protect the Association systems, devices and data from unauthorised access and malicious software.

3. Scope

This statement covers all users who use the Association's devices or connect to the Association's systems when away from premises owned or controlled by the business.

4. Statement

4.1. Any device accessing Association systems must be provided by the Association.

4.2. Using a personal device to access Association systems is strictly forbidden for members of staff.

4.3. Users working from home must take all reasonable measures to protect the devices from loss, theft, and unauthorised access.

4.4. Any mobile computing devices that contain sensitive or confidential Association data must protect that data with encryption and at least a password.

4.5. Databases and other Association data which resides on the Association network or on Association computers, shall not be downloaded to mobile computing or storage devices.

4.6. Any lost or stolen mobile computing device must be reported to a member of the Management Team and to the Senior Systems & Innovation Officer without any undue delay.

4.7. Any unauthorised access to a mobile computing device or to the data contained within must be reported to a member of the Management Team and to the Senior Systems & Innovation Officer without any undue delay.

4.8. Users should not connect to Public Wi-Fi services as these are insecure.

4.9. Any devices accessing Association systems or data must be protected with antivirus software approved by the Association's IT Support Company.

4.10. Any device accessing Association systems or data must have automatic logout enabled after a period of no more than 10 minutes of inactivity.

4.11. Users should ensure that they access Association systems and data from home only and from no other location.

4.12. If a user needs to work from a location other than the Association office or from home, notice must be given and location approved by their line manager. Access must be gained via a secure dongle provided by the Association.

4.13. Users should ensure their home Wi-Fi is secure and router is regularly kept up to date with updates from their broadband provider.

Appendix 10 – Mobile Phone Guidance

Your work mobile phone is to be used for business purposes only.

Voice calls

Wherever possible, voice calling should be via Microsoft Teams. If not possible, your mobile phone can be used.

Texting

Wherever possible, texting should be via Omniledger Pyramid. If not possible, your mobile phone can be used.

If texting via work mobile phone, screen prints must be taken and saved to the customer record in Pyramid within 10 working days . Once saved to Pyramid, texts and screen prints must be deleted from the mobile phone immediately.

WhatsApp

WhatsApp use on mobile phones is prohibited.

Email

Accessing email or any other parts of our system is prohibited.

Photographs

If used to take photographs these must be transferred to our system within 10 working days. Once done, photographs must be deleted from the mobile phone immediately.

Apps

Downloading of Apps is only allowed when:

1. installation is done by the Senior Systems & Innovation Officer

2. the app is on our approved apps list

3. download is from the official Google or Apple store

Important information

It is essential that your phone is kept up to date at all times with system updates. security updates and application updates. Apply updates within 14 days of being prompted.

If your phone is lost or stolen report this immediately to your manager or to the Senior Systems & Innovation Officer. They will request your phone is erased by Lugo.

Your phone will lock when inactive or when the power button is pressed.

As well as unlocking your phone by using your PIN, you can set up fingerprint recognition and/or face recognition.

If your PIN is entered incorrectly 10 times, all data will be erased.

Power off your phone at the end of each working day.

Connecting to public Wi-Fi hotspots is prohibited as these are insecure.

Appendix 11 - ICT Disaster Recovery Plan

ICT EQUIPMENT & SYSTEMS

1. **Disaster Recovery**

The Association has a comprehensive Disaster Recovery Plan in place which has been developed by its Insurers and which relates to all areas of the Association's business in the event of a serious incident which causes disruption to its operational activities.

This plan sets out the Association's contingency response in relation to specific elements of Information and Communication Technology in the event of such incidents. Implementation of the recovery measures here will be the responsibility of the Head of Corporate Services who will liaise as necessary with the Association's external IT supplier.

The Association's insurance cover allows for replacement of equipment and reinstatement of data.

2. **Backups**

All of the Association's data is stored in the cloud in secure datacentres.

Housing management data is backed up daily by our housing management supplier and is held in Microsoft Azure in different datacentres in different locations in the UK.

Email and all other data is backed up twice daily by our external IT supplier and is held in Microsoft Azure in different datacentres in different locations in the UK.

3. **Disaster Scenarios**

Outlined in Appendix A are foreseeable disaster scenarios which this plan will cover. Timelines are detailed in Appendix B.

4. **Responsibility**

In the event of a serious incident, disaster recovery activities for ICT will be co-ordinated by the Director and Head of Corporate Services in liaison with the Association's Senior Systems & Innovation Officer and our external IT supplier.

Key contacts are noted in Appendix C.

The Director is responsible for ensuring a full test of the ICT Disaster Recovery Plan is undertaken bi-annually.

5. Review

This plan will be reviewed annually by the Senior Systems & Innovation Officer.

.

Last amended July 2024

Appendix A – ICT Disaster Scenarios

Event	Action re IT	Action re Phones
Loss of office	Home working	Home working
No access to office	Home working	Home working
Power cut	Home working	Home working
Hardware fault - Firewall	Contact external IT supplier, troubleshoot and replace if needed	Contact external IT supplier, troubleshoot and replace if needed
Hardware fault - Switch / Data	Contact external IT supplier, troubleshoot and replace if needed	No impact
Hardware fault - Switch / Phones	No impact	Contact external IT supplier, troubleshoot and replace if needed
Hardware fault – Router / Primary internet for data	Contact external broadband supplier for service status updates and contact external IT supplier to switch to backup internet connection	No impact
Hardware fault – Router / Backup internet for data	Contact external IT supplier, troubleshoot and replace if needed	No impact
Hardware fault – Router / Phones internet	No impact	Contact external IT supplier, troubleshoot and replace if needed
Line fault - Internet / Data	Contact external broadband supplier for service status updates	No impact

	and contact external IT supplier to switch to backup internet connection, restart firewall	
Line fault - Internet / Phones	No impact on IT	Contact external IT supplier, troubleshoot
Software fault - No access to Microsoft 365	Contact external IT supplier and await instruction	No impact
Software fault - No access to Housing Management system + data	Contact external housing management supplier and await instruction	No impact
Software fault – No access to phone system	No impact	Contact external IT supplier and await instruction
Data issue - No access to email and to Hillhead data	Contact external IT supplier and await instruction	No impact
Data loss or corruption (ransomware / malware)	Contact external IT supplier or external housing management supplier to restore backup	Contact external IT supplier to restore back up

Appendix B - ICT Disaster Recovery Action Plan – Timeline

Event/Trigger	Action	Lead	Timescale following plan instigation	Action complete YES/NO
Loss of office	Telephone call/email to ICT support providers	Director or Head of Corporate Services	Immediate	
Loss of office	Message added to Association's website & to Facebook notifying event	Head of Corporate Services	Immediate	
No access to office	Message added to Association's website & to Facebook notifying event	Head of Corporate Services	Immediate	
Power cut	Message added to Association's website and to Facebook notifying event	Head of Corporate Services	Immediate	
Hardware fault - Firewall	Contact external IT supplier, troubleshoot and replace if needed	Senior Systems & Innovation Officer	Immediate	
Hardware fault - Switch / Data	Contact external IT supplier, troubleshoot and replace if needed	Senior Systems & Innovation Officer	Immediate	
Hardware fault - Switch / Phones	Contact external IT supplier, troubleshoot and replace if needed	Senior Systems & Innovation Officer	Immediate	
Hardware fault – Router / Primary internet for data	Contact external broadband supplier,	Senior Systems & Innovation Officer	Immediate	

	troubleshoot and replace if needed			
Hardware fault – Router / Backup internet for data	Contact external IT supplier, troubleshoot and replace if needed	Senior Systems & Innovation Officer	Immediate	
Hardware fault – Router / Phones internet	Contact external IT supplier, troubleshoot and replace if needed	Senior Systems & Innovation Officer	Immediate	
Line fault - Internet / Data	Contact external broadband supplier, troubleshoot and await instruction	Senior Systems & Innovation Officer	Immediate	
Line fault - Internet / Phones	Contact external IT supplier, troubleshoot and await instruction	Senior Systems & Innovation Officer	Immediate	
Software fault - No access to Microsoft 365	Contact external IT supplier, troubleshoot and await instruction	Senior Systems & Innovation Officer	Immediate	
Software fault - No access to Housing Management system + data	Contact external housing management supplier, troubleshoot and await instruction	Senior Systems & Innovation Officer	Immediate	
Software fault – No access to phone system	Contact external IT supplier, troubleshoot and await instruction	Head of Corporate Services or Senior Systems & Innovation Officer	Immediate	

Data issue - No access to email and to Hillhead data	Contact external IT supplier, troubleshoot and await instruction	Senior Systems & Innovation Officer	Immediate	
Data loss or corruption (ransomware / malware)	Contact external IT supplier and/or external housing management supplier, troubleshoot and await instruction	Director or Senior Systems & Innovation Officer	Immediate	

Appendix C – ICT Contacts

Supplier	Support	Contact details
Linten Technologies	uSecure cyber awareness training	0161 503 5050
Lugo IT	Email Hillhead data Backup broadband line Firewall Switches Laptops Microsoft 365 Telephone System	Steven McGuire 07771 777865 steven.mcguire@lugoit.co.uk 03300 242 242 support@lugoit.co.uk 03300 242 999
O2	Mobile phones + iPad	Premium Business End User Customer Services 0800 588 4211 premiumbusiness@o2.com Customer services 08005884210
Omniledger	Housing Management System plus its data	Gary Dempsey 07812 078980 gary.dempsey@omniledger.co.uk 01707 324201 support@omniledger.co.uk https://support.omniledger.co.uk https://www.omniledger.co.uk/

Resource	Standalone phone lines: Alarm Fax	**03451 800 400** networksupport@resourcetelecomgroup.com **www.focusgroup.co.uk**
SoloProtect UK	Lone Worker devices	0114 399 6000 support@soloprotect.com
Virgin Media Business	1. Primary broadband line 2. Freephone number	0800 052 0800

Appendix 12 – Statement for Committee Members

Cyber security is essential for protecting Association data. We are trusted to keep data safe and without the proper measures and everyone taking up responsibility in using a strong password and keeping this secure, data could become compromised and cause damage to the Association and its reputation. Strong passwords significantly reduce the opportunity for unauthorised access to Association information resources, whereas weak passwords heighten risks greatly.

By agreeing to and following this guidance, you are helping ensure that the Association is doing everything it can to protect the Association's information and to maintain our reputation as a secure operator.

You have been given a password which should not be shared or reused in any system or service outwith the Association or in personal use.

If you require a password change to something more memorable for you, please contact the Senior Systems & Innovation Officer who will do this for you.

Your password must be changed immediately when there is reason to believe that the password has been compromised. If you suspect your password may have been compromised, you must report the incident to a member of the Management Team and to the Senior Systems & Innovation Officer who will change your password immediately.

Please leave hard copy papers at the end of a meeting for shredding.

Appendix 13 – Sign-Offs

Employee Agreement

Each employee must confirm that they have read and understood the contents of Hillhead Housing Association 2000's Information and Communication Technology Security Policy as approved by the Committee.

Failure to comply with the rules set out in this Policy

a) may result in legal claims against you and the organisation; and

b) may lead to disciplinary action being taken against you, including dismissal.

I have read and understood the terms of Hillhead Housing Association 2000 Information and Communication Technology Security Policy.

Date: ……...

Signature: ……

Supplier/Third Party Agreement

All external suppliers/third parties engaged by the Association must confirm that they have read and understood the contents of Hillhead Housing Association 2000's Information and Communication Technology Security Policy as approved by the Committee.

Failure to comply with the rules set out in this Policy

a) may result in legal claims against you and your company; and

b) may lead to termination of your company's contract with the Association

I have read and understood the terms of Hillhead Housing Association 2000 Information and Communication Technology Security Policy.

Date: ……...

Signature: ……

Company: ……..……