Hillhead

HOUSING ASSOCIATION

Building on progress for a brighter Hillhead

HILLHEAD HOUSING ASSOCIATION 2000

ICT SECURITY POLICY

Approved/last reviewed by Management Committee: 1 June 2022
Addition of paragraph 3.12 on page 7 approved 22 June 2022

Date due for review: June 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, बड़ी 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 ਸੰਪਕਰ ਕਰੋ :
admin@hillheadhousing.org

اس دستاویز میں درج معلومات اُردو زبان یا آڈیوٹیپ / 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۔

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.

List of Contents

1. Policy Statement

1.1 **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
- Regulatory and legislative requirements will be met including the needs of the general data protection regulations
- 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
- Business requirements for the availability of information and information systems will be met
- The Director has direct responsibility for maintaining the Policy and providing advice and guidance on its implementation.

1.2 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.

1.3 Committee Members have a responsibility to adhere to the policy too.

2. Applicability of the Policy

2.1 The following policy has been prepared. The policy may be amended or revised periodically as the need arises. All sections are applicable to all users.

2.2 It is vital that Staff and Committee Members 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 Systems Support Officer or the Management Team. Once you have read and understood this Policy, you must sign it on page 16 and photocopy that page.

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

2.4 Non-compliance of the ICT Security Policy will be dealt with in accordance with the staff conditions of service disciplinary procedures and for committee in line with their code of conduct.

3. General Information Technology Infrastructure

3.1 This section covers the Association's generic provision of information technology. This section describes these resources and defines acceptable and unacceptable use of them. 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. The Management Team are responsible for ensuring that this policy is complied with.

Current Information Technology Infrastructure

3.2 Hillhead Housing Association 2000 has provided an IT infrastructure which allows for efficient information and resource sharing. This helps facilitate good working relationships with colleagues, business partners and stakeholders alike which, in turn, helps the Association to reach its objectives.

3.3 The following is a description of the IT Infrastructure within the Association.

- The Association's data is held in the cloud in Microsoft Azure with a copy held in a different data centre in a different location.
- The Association's housing management data is held in the cloud in Microsoft Azure with a copy held in the suppliers' secure data centre in a different location.
- The Association uses a number of Microsoft 365 applications for Email, Calendar, Contacts, Teams and SharePoint data.
- Users have access to Microsoft Teams Channels that are relevant to their needs of Data access rights as prescribed by the Head of Corporate Services.
- An internal network is used to connect the laptops to printers and to the internet. Each piece of equipment is connected via a network cable to a wall port. The same infrastructure is used to deliver Telephony service to desks.
- The Association has a high-speed broadband connection for accessing email and our cloud hosted systems and data.
- The Association has a second broadband connection to be used as a backup to the primary connection.
- Users have access to a laptop which will give them access to the software and data required by them.
- The Association will endeavour to install, upgrade or replace hardware and software when required, in order to maintain acceptable performance, subject to budgetary constraints. For new equipment a Business Case must be produced to justify any additional ICT equipment, which should be presented to the Director for consideration.
- All items of ICT Equipment are marked with a unique reference number and name and address of the Association
- The ICT Asset Register is updated regularly and is reconciled annually to actual items held
- Procedures for the safe and secure disposal of redundant ICT equipment are in place and ensure that all confidential data has been removed prior to disposal
- Laptops are replaced every 3 to 5 years.

3.4 Home Working

The Association's ICT infrastructure is capable of supporting remote working and gives employees remote access to all systems and data. Employees are required to have home broadband in place with sufficient speed with appropriate security in place. The Association will, where practical, provide the appropriate equipment and/or software to allow people to work remotely and securely. Further detail can be found in the Home Working Policy.

Security

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

Confidentiality

- All Association information must be protected from unauthorised disclosure. This includes "leaks" of information to a competitor or to the media. It also includes unauthorised access to data and "hacking" into systems from internal or external sources. Access to personal data relating to applicants, tenants, former tenants, committee members, and staff should only be accessed and used for business purposes and as and when required to allow you to carry out your duties.

Integrity

- Data must be protected from unauthorised modification. Only those with the appropriate authority should be able to change data. Data must also be protected from accidental alteration.

Availability

- To maintain its value, Association data 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. This is achieved by the following:-

  - All users using IT systems will undergo an IT Induction before using any system. This will include logging on and off, passwords, security, applications used, printing, user education & awareness portal and location of the IT procedures. This training will be organised by the Head of Corporate Services.
  - Where third parties have access to the Association's data, such as the housing management supplier and the external IT supplier, Development Agents, Finance Agents, a contract or disclaimer must be obtained that will protect the information held. This should cover any information that the third party may see as a result of their access which should be treated with the strictest confidence. External suppliers and third parties will be required to sign a declaration to confirm acceptance to comply with this Policy
  - Personal use of the Association's systems is prohibited. Any breach will be subject to disciplinary action as laid out in the Employment Conditions for members of staff and the Committee Members' Code of Conduct. The Association has the right to monitor the content of files and data located on any of the Association's IT equipment. Under no circumstances should personal email accounts be accessed on a work device.
  - Users will be responsible for the security of all the Association's information when working remotely or when accessed off site. Under no circumstances should data be copied onto removeable

media, be copied onto a personal device or be uploaded to the internet.

- In order to facilitate recovery in the event of a failure to protect Association information:-

  a) The Director will refer to the current Business Continuity Policy
  b) Data is backed up daily and is held in the Cloud
  c) Further information on IT Recovery can be found within the ICT Disaster Recovery Plan (Appendix 3)

Cyber Security

3.6 The Association acknowledges the threats in a rapidly evolving online world. As a result, all devices 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. Also installed is 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. For Cloud Security we have installed Cisco Umbrella. This service will protect users from visiting known and suspect dangerous websites that are marked as being suspicious. It also protects users from opening email attachments that are suspicious and contain dangerous payloads.

3.7 All laptops should be restarted when prompted that updates await. All mobile phones should be updated when updates are available.

3.8 External devices (HDD, Memory Sticks, mobile phones, personal devices et al) are not allowed to connect to the network in the interest of Data Security.

IT Support

3.9 The Systems Support Officer provides the support service for all IT related issues. Issues can be escalated to the external IT supplier when needed. It is acknowledged that staff also provide a level of support amongst themselves.

3.10 The Systems Support Officer and Director/ Depute Director are responsible for all hardware and software installation, maintenance and development. They will prioritise ICT tasks, basing their decision on the business need. In the event of a hardware or software fault, repairs will be undertaken by either the Systems Support Officer or the external IT supplier.

3.11 Each laptop has a standard pre-set configuration which must not be amended by the user. Users should not install any software unless authorised by the Systems Support Officer, the external IT supplier or Director / Depute Director. Users shall not move, relocate, reassign or otherwise modify hardware. This will ensure that the Association's assets are being managed and tracked effectively.

3.12 Administrator accounts

No user has admin access on their laptop. Requests for tasks requiring admin access need to go via the Systems Support Officer and be recorded on the support call. The external ICT company staff have individual admin accounts for use on the laptops. These accounts are created by Azure policy and the admin user is to be recorded on the call details.

The external ICT company log on to Azure/365 via the Microsoft Partner portal using their individual accounts to manage our Microsoft 365 environment. All of the ICT company staff passwords must be at least 12 characters.

Training

3.13 The Association will recruit staff with the basic skills necessary. Additional training, including on the job training will be provided from the training budget. In addition, training modules on Cyber Security and Microsoft applications are available via the Learning portal.

Passwords

3.14

The Association has set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected. This applies to all users.

Passwords are a critical part of information and network security. Passwords serve to protect user accounts, data and systems, but a poorly chosen password, if compromised, would put the entire network/business at risk.

- Passwords must be changed every 365 days or immediately if a compromise is suspected
- Previous passwords cannot be reused
- Passwords must have a minimum of 12 characters and be strong and memorable
- Passwords have a minimum life of 24 hours
- Users shall have no more than 10 chances to enter their password before they are locked out and they will remain locked out until the Systems Support Officer or the external IT supplier unlocks them
- Device screen will lock after 10 minutes of inactivity
- Users must enter a password to unlock the device when returning from idle state
- All passwords must conform to the guidelines outlined below

Passwords are used to access any number of company systems. Poor or weak passwords are easily cracked either by brute force, guessing or profiling, and put the entire system at risk, thus strong passwords are required.

Create a password that is easy to remember but hard to guess.

1. Passwords must be at least 12 characters and contain:

   a. three random words
   b. upper case letters [A-Z]
   c. lower case letters [a-z]
   d. numbers [0-9]
   e. special characters [.!"£$%^&*()_+"]:;@'~#<,>.?/'] (a space character is allowable)
2. A new password must not be a modification of an existing password
3. Simple passwords such as 1111 and 1234 cannot be used
4. Picture passwords are not allowed

5. Passwords should not be based on well-known or easily accessible/guessable personal information, or based on family members, friends, pets or car registration numbers
6. Personal information includes logon I.D, name, birthday, address, phone number(s), national insurance number, or any permutations thereof
7. Passwords must not be publicly known or associated with the business/sector
8. Passwords must not be based on the company's name or geographic location

Password Protection Guidelines

1. Passwords should be treated as confidential information
2. No employee is to give, tell, or hint at their password to another person, including IT staff, support companies, superiors, other co-workers, friends, and family members, under any circumstances
3. Users must not transmit passwords electronically over the unprotected Internet, such as via email
4. Users must not use the "Remember Password" feature of applications
5. Users must not use the same password to access multiple systems i.e., do not reuse passwords ever
6. Users must not write down passwords

Additional Protection

Where possible use two-factor authentication i.e., SMS to your mobile, authenticator app etc., where it is available, use it.

Password Managers

Where provisioned by IT/business use password managers to hold your passwords, ensure that the password used to gain access to the password manager is extremely strong (long) and where possible use additional protection as described above.

Clear screen

3.15 Users are required to lock their computer screens by using the Windows and 'L' keys, when leaving their desk for any reason.

Mobile devices through which access to the network can be obtained should be PIN protected, set to lock after a period of 2 minutes and switched off when left unattended.

Users should ensure that open documents on their laptop 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 easily been seen by unauthorised persons.

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

4. Mobile Equipment

4.1 The Association has items of equipment that by their nature are mobile, such as laptops, iPads, mobile phones and digital cameras.

4.2 When in possession of such equipment, users must take care in regard to the security of the equipment and to also comply with any requirements stipulated by the Association insurers. Currently, any equipment carried in a vehicle should be securely locked in the boot, while any equipment kept at home should be made as secure as possible.

5. Email / WhatsApp /Pyramid Messenger

5.1 Email (electronic mail) is a widely used form of communication within the Association and should be primarily used for external communication with third parties. Wherever possible all internal communication should be channelled via Microsoft Teams or via Pyramid Messenger for communications with tenants and applicants. WhatsApp group chats are primarily to be used for general group notifications within staff teams.

Purpose of email

5.2 The objective of this section is to help the Association and its users achieve the maximum benefit, at the lowest risk, from its use. The Association has provided email to facilitate communication among its employees, Committee members and third parties such as business partners and suppliers. The email system is the property of the Association and is intended for business and other Association sanctioned use only. Under no circumstances should personal email accounts be accessed on a work device.

Guidance on legal issues

5.3 Email users should be aware of the following:

- External emails are Association records
- Emails have the same legal status as other mailed documents
- Courts can order that email messages are made available
- Any information held on individuals, including that in the email system, may be subject to the terms of the Association's Data Protection Registration
- If in doubt, ask the Head of Corporate Services for guidance

Privacy

5.4 In order to protect the Association from legal, regulatory or other repercussion, the Association may monitor the content of incoming and outgoing emails through the Association's systems. Users should be aware that this will also cover emails marked or considered private, confidential etc.

Information Confidentiality

5.5 Email is an inherently insecure system (a bit like sending information on a postcard). Emails can be intercepted, and content can be easily copied and forwarded. It should not be used to send any sensitive or confidential information. If such information must be sent via email, then it should be done through an attached file that is password protected, with the password notified to the recipient by a phone call.

Drafting of Email

5.6 It is the Association's policy to ensure a consistent standard of email. To that end, users should:

- Draft emails carefully, taking into account discrimination, harassment, Association presentation and defamation issues.
- All users should use suitable email etiquette at all times. See Appendix 2.
- Not attach large files to emails. If internal, these will contribute to the disk space allocated to both the sender and recipient. A link of where the file is stored should be used instead. If the email is external, you should remember that the recipient may have a limit on the maximum message size that can be sent or received through their system.

Virus Threat

5.7 Emails offer a path for hackers to gain access and for viruses to contaminate the Association's systems This is usually through a link in the email itself or an attached file. The email system has protections in place, but users are the first line of defence and are reminded of the dangers, (see Cyber Security above).

5.8 Users should pay particular attention to emails that they did not expect to get even if they are from recognised senders. Many 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.

5.9 If a user is suspicious of an email they have received they should contact the Systems Support Officer immediately. It should be noted that the system may 'filter out' some file attachments that are considered dangerous.

5.10 The Head of Corporate Services will alert staff of any major virus threats that are prevalent at that time. Users should always take heed of any warnings and restart their laptop when prompted that updates have been applied.

Time Management

5.11 While the email system will deliver messages regularly throughout the working day, it is bad practise for users to continually interrupt their work to deal with them. Users and their managers should agree on a suitable strategy for dealing with email messages that restrict the interruptions. Internal communications should be made through Microsoft Teams rather than email.

Personal Use

5.12 Personal use of the email system is not permitted.

Retention Policy

5.13 Most email messages are of temporary value and should be deleted as soon as their immediate purpose is served. However, some messages have content that requires formal handling.

5.14 Retention and deletion of old email messages should be managed by each user bearing in mind data storage levels, archival records, contractual evidence and legal requirements. Unless emails are subject to formal retention guidelines, then they should be deleted as soon as they have been dealt with. Any that include content subject to formal retention should be considered corporate records and be either:

o Saved as a file in the appropriate folder on the Association's cloud storage.

OR

o Printed in hard copy which shall be retained as the "official record"

5.15 Users will be allocated a certain amount of email storage where all the information from their Outlook, including email, will be stored. Users will have to perform regular housekeeping of un-needed messages.

5.16 An email will be sent automatically by the system advising the user that they are nearing their limit. Should this warning be ignored and the limit is reached, the user will not be able to send or receive any emails.

Inappropriate Use

5.17 The Association prohibits the use of Association systems to carry out inappropriate material, in particular:

o The unauthorised distribution (internally or externally) of information known or believed to be confidential
o Representation of personal opinions as that of the Association
o Concealment or misrepresentation of names or affiliations in email messages
o Alteration of source or destination addresses of email
o Use of email facilities for commercial or private business purposes
o Use of email which unreasonably interferes with or threatens other individuals
o The distribution (internally or externally) of chain letters, inappropriate humour, explicit or offensive language or images or any other message which breaches a policy of the Association or creates an intimidating or hostile work environment

5.18 Users must accept the risk that inbound email messages may contain explicit or offensive material that is beyond the control of the Association. If any such material is received then the employee should contact the Head of Corporate Services for advice on what action should be taken.

6. The Internet

6.1 The Internet is offered as a tool to staff because of the opportunities it provides for accessing important information.

Purpose of Internet Access

6.2 The Internet has been recognised as an important, growing source of business information for the Association. Personal use is not encouraged and is viewed as a privilege, not a right. Personal use should not be done during that person's working day. Managers have the right to withdraw this privilege if it is abused. Excessive or inappropriate personal use will be subject to disciplinary action.

6.3 This policy states that:

- Access is available through a Broadband connection to all staff through their laptop being connected to the Association's network or through Wi-Fi. In order not to disrupt work, users should keep on-line to a minimum.
- Normal use is restricted secure sites (https)). Users should consider Internet activity to be public and not reveal confidential information.
- Access to Internet newsgroups and social networking sites is not permitted unless it's the Association's social sites.
- The Internet should be used to access business related information only.
- Users are not permitted to access personal email accounts from work devices.
- The Association has the right to monitor Internet activity, personal or business and to block offensive, illegal and non-business related sites.
- All files downloaded should be subjected to a scan for threats.
- Secure transfer of data/files to third parties e.g. auditors, publishers and solicitors should be carried out by their secure portal or via SharePoint.

Inappropriate Use

6.4 The following use of the Internet is prohibited:

- Visiting Internet sites that contain offensive images or documents. If you inadvertently do so, then disconnect immediately and report the incident to your manager. The Internet should not be used for illegal or unethical purposes.
- Copying or transmitting copyrighted material without explicit permission.
- Sending large volumes of messages to a site with the intention to disable it.
- Unauthorised attempts to access information.
- Commercial use – any form of commercial use of the Internet is prohibited.
- Solicitation – the purchase or sale of personal items through advertising on the Internet is prohibited.
- Harassment – the use of the Internet to harass employees, vendors, customers and others is prohibited.
- Political – the use of the Internet for political purposes is prohibited.
- Misinformation/Confidential Information – the release of untrue, distorted or confidential information regarding the Association's business is prohibited. Viewing/downloading purely entertainment sites or material where there is no benefit to the Association in terms of its learning, communication or service aims described earlier.

Website

6.5 The Association has developed its own website. The site provides information to visitors on services provided by the Association. The Association is continually investigating ways of improving the services that it can offer through the site. The website is owned by a consortium – Scottish Housing Connections – of which the

Association is a Member. The Association's Website is maintained by the Head of Corporate Services. A staff sub group meets periodically to review and update content of the Website.

Virus Threat

6.6 The Internet offers a path for hackers to gain access and for viruses to contaminate the Association's systems primarily by downloading or running infected files. The Association's systems have protections in place but users are the first line of defence and are reminded of the dangers (see Cyber Security above).

6.7 Users should pay particular attention to the types of files available from a website and should only download mainstream files such as PDF. Any downloads should be for business related information only.

6.8 Users should not download or run any files with a file extension '.exe', '.scr', 'pif' etc or if they apparently contain a double file extension e.g. '.doc.exe'. These examples are in no way exhaustive.

6.9 If a member of staff is suspicious of downloading a file they should contact the Systems Support Officer or the external IT supplier.

7. Telecommunications

7.1 Telecommunications 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 efficiently.

Telecommunications Policy

7.2 The Telecommunications Policy is to provide a reliable, flexible system. Each user will be trained in the systems use and should follow the procedures laid down in order to get the most from telecommunications:

- Managers are responsible for ensuring that this policy is complied with
- The Association provides a modern telephone system with the capacity for growth to meet requirements for the foreseeable future
- A Horizon cloud hosted Vo-IP telephony system with Microsoft Teams integration delivers telecommunications to each user laptop using Microsoft Teams and to desks using the company's structured cabling system.
- The telecommunications service is provided for all staff for business and other Association sanctioned use only. Personal use is not encouraged and is viewed as a privilege, not a right. Managers have the right to withdraw this privilege if it is abused. Excessive or inappropriate personal use will be subject to disciplinary action.

8. Committee Members

General

8.1 As the use of technology grows Committee members will have access to the Associations information via ICT, such as reports, minutes etc. This will be via Microsoft 365 on a laptop provided by the Association. This ICT Security Policy applies to all users - staff and committee members.

Appendix 1

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: ………………………………………………

Committee Member Agreement

Each Committee Member 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) will be dealt with in line with the committee member code of conduct.

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: ………………………………………..………

Appendix 2

USE OF EMAIL

The speed and ease with which email messages can be written means that less time and thought goes into an email message than a dictated, typed, printed, signed and sent letter. However, email messages are classified as legal documents.

Courts have the power, in some circumstances, to order that email messages be available for open inspection. Email messages are also subject to Freedom of Information requests and the same standard of care should, therefore, be exercised in the content of an email message as in any other business communication.

As in any communication, the golden rule here is “think before you send”.

Consider the various communications email may replace:

- Telephone messages
- Scribbled notes
- Memos
- Letters

Then remember that your email message constitutes a legal document. So, while perhaps some informality in language may be appropriate for some email messages, the content should conform to the same standards as memos or letters.

Do’s

- Remember your email is a legal document – so be careful what you write
- Use the standard of English that you would normally use for the message if you didn’t have email. If you would have phoned someone, write in spoken English style. For a note, informal English is okay. If you would have sent a letter or a formal memo, then use the same style as you would have used.
- Sign your messages at the bottom with your name and, if required, your job title, direct telephone number. NB – the main telephone as well as the address of the main office is contained in the automatic email footer.
- Write in mixed case. Upper case counts as SHOUTING.
- Use correct spelling and grammar
- Use ‘smileys’ e.g. ☺ to let someone know that what you have just written is meant to be taken lightly or as a joke. It is easy to be misunderstood if you replace face-to-face or telephone communication with an email message so use ☹ ☺ ;-) and the other 101 variants of ‘emotions’ to help express emotion.
- Use an email rather than telephoning if you simply want to give someone a message. It saves disturbing them if they are busy.

Don’ts

- Never send an email message in anger – it will get there very fast and you may regret it!
- Never assume that people have read their email when you next see them
- Do not use capital letters as this can be construed as SHOUTING and is likely to cause offence
- Do not send one long email covering multiple topics. Send several short emails each covering a single topic and then it is easy for people to respond.

Appendix 3

IT DISASTER RECOVERY PLAN
IT 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 policy allows for replacement of equipment and reinstatement of data, the amounts of cover are:

Static computer equipment in the office	£14,850
Equipment at home	£2,000
Portables, including laptops	£32,900
Mobile phones	£4,000
Reinstatement of data	£25,000
Increased cost of working	£12,500

2. Backups

All 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 1 are foreseeable disaster scenarios which this plan will cover. Timelines are detailed in Appendix 2.

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 Systems Support Officer and our external IT supplier.

Key contacts are noted in Appendix 3.

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 Head of Corporate Services.

Last amended June 2022
Stephen Macintyre
DIRECTOR

Appendix 1 – 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 and contact external IT supplier to switch to backup internet connection, restart firewall	No impact
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 2 - 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, Facebook & Twitter notifying event	Head of Corporate Services	Immediate	
No access to office	Message added to Association's website, Facebook & Twitter notifying event	Head of Corporate Services	Immediate	
Power cut	Message added to Association's website, Facebook & Twitter notifying event	Head of Corporate Services	Immediate	
Hardware fault - Firewall	Contact external IT supplier, troubleshoot and replace if needed	Systems Support Officer	Immediate	
Hardware fault - Switch / Data	Contact external IT supplier, troubleshoot and replace if needed	Systems Support Officer	Immediate	
Hardware fault - Switch / Phones	Contact external IT supplier, troubleshoot and replace if needed	Systems Support Officer	Immediate	
Hardware fault – Router / Primary internet for data	Contact external broadband supplier, troubleshoot and replace if needed	Systems Support Officer	Immediate	
Hardware fault – Router / Backup internet for data	Contact external IT supplier, troubleshoot and replace if needed	Systems Support Officer	Immediate	
Hardware fault – Router / Phones internet	Contact external IT supplier, troubleshoot and replace if needed	Systems Support Officer	Immediate	

Line fault - Internet / Data	Contact external broadband supplier, troubleshoot and await instruction	Systems Support Officer	Immediate	
Line fault - Internet / Phones	Contact external IT supplier, troubleshoot and await instruction	Systems Support Officer	Immediate	
Software fault - No access to Microsoft 365	Contact external IT supplier, troubleshoot and await instruction	Systems Support Officer	Immediate	
Software fault - No access to Housing Management system + data	Contact external housing management supplier, troubleshoot and await instruction	Systems Support Officer	Immediate	
Software fault – No access to phone system	Contact external IT supplier, troubleshoot and await instruction	Head of Corporate Services or Systems Support Officer	Immediate	
Data issue - No access to email and to Hillhead data	Contact external IT supplier, troubleshoot and await instruction	Systems Support Officer	Immediate	
Data loss or corruption (ransomware / malware)	Contact external IT supplier and/or external housing management supplier, troubleshoot and await instruction	Director or Systems Support Officer	Immediate	

Appendix 3 – ICT Contacts

Supplier	Support	Contact details
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
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
Virgin Media Business	1. Primary broadband line 2. Mobile phones + iPads 3. Freephone number	0800 052 0800